

# Stanislaus County District Attorney's Office

## Policy Manual

---

### **DISTRICT ATTORNEY'S PREFACE**

The mission of the Stanislaus County District Attorney's Office (SCDA) is to promote a strong and safe Stanislaus County by pursuing justice with integrity and respect for the rights of all. SCDA members strive to maintain professional and effective working relationships with our law enforcement partners, promoting efficiency and trust within our community. Together, we work to reduce crime, serve victims, and enhance the quality of life in Stanislaus County.

Serving justice with integrity involves a special trust given to us by the public to uphold and enforce the law. As public servants, we are committed to doing the right thing at all times. While this manual cannot predict every aspect of our jobs or anticipate all potential situations, it establishes a framework of rules, guidelines, and performance expectations for all SCDA members. Each employee plays an essential role in our efforts to serve the community. collectively, we will work to improve public safety, increase public trust, and pursue organizational excellence.

All SCDA members are required to familiarize themselves with the directives in this manual and seek guidance and clarification from a supervisor when necessary. This manual will be updated as needed to reflect changes in the law, personnel responsibilities, and Office goals. As the District Attorney, I am proud of our Office and our members. Every day, our employees demonstrate professionalism and dedication that often goes unnoticed. I am confident that together we can make our Office and community better tomorrow than it is today.

Jeff Laugero, District Attorney

# Stanislaus County District Attorney's Office

## Policy Manual

---

### **MISSION, MOTTO, VALUES, AND GOALS**

#### STANISLAUS COUNTY DISTRICT ATTORNEY'S OFFICE MISSION, MOTTO, VALUES, AND GOALS

##### MISSION STATEMENT:

- Promote a strong and safe Stanislaus County by pursuing justice with integrity and respect for the rights of all.

##### MOTTO:

- Justice with Integrity

##### VALUES: (SERVICE)

- Service: Serve the public interest in our work. Constantly work to earn the public trust.
- Excellence: Be the high performing professional organization the community deserves. Adhere to the highest professional standards and be the uncompromising in our ethics.
- Respect: Treat all people with courtesy and dignity. Value differences in opinions and backgrounds.
- Versatility: Think creatively to provide the best possible outcomes for the community. Adapt to evolve to changing conditions, and demands of the criminal justice system.
- Cooperation: Demonstrate a spirit of teamwork and collaboration. Work together to address the needs of the community.
- Engagement: Foster open and honest communication with the public we serve. Maintain genuine and meaningful relationships with partner agencies.

##### OFFICE GOALS:

- Improve Public Safety
- Increase Public Trust
- Pursue Organizational Excellence

# Stanislaus County District Attorney's Office

## Policy Manual

---

### Table of Contents

<b>District Attorney's Preface.</b>	<b>1</b>
<b>Mission, Motto, Values, and Goals.</b>	<b>2</b>
<b>Chapter 1 - Law Enforcement Role and Authority.</b>	<b>7</b>
100 - Law Enforcement Code of Ethics.	8
101 - Law Enforcement Authority.	9
102 - Chief Executive Officer.	12
103 - Oath of Office.	13
104 - Bureau of Investigation Policy Manual.	14
<b>Chapter 2 - Organization and Administration.</b>	<b>17</b>
200 - Organizational Structure and Responsibility.	18
201 - Interim Directives.	20
202 - Training.	21
202 - Electronic Mail.	23
203 - Retiree Concealed Firearms.	24
<b>Chapter 3 - General Operations.</b>	<b>29</b>
300 - Use of Force.	30
301 - Handcuffing and Restraints.	41
302 - Control Devices and Techniques.	45
303 - Firearms.	48
304 - Foot Pursuits.	58
305 - Investigator Response to Calls.	63
306 - Victim and Witness Assistance.	65
307 - Information Technology Use.	66
308 - Registered Offender Information.	69
309 - Private Persons Arrests.	72
310 - Limited English Proficiency Services.	74
311 - Mandatory Employer Notification.	79
312 - Child and Dependent Adult Safety.	81
313 - Off-Duty Law Enforcement Actions.	85
314 - Bureau of Investigation and Victim Services Unit Mass Victimization Partnership and Response Plan.	87
315 - Drop Charges Request.	89
316 - Bias-Based Policing.	91
317 - Hostage and Barricade Incidents.	94
318 - Hazardous Materials.	99
319 - Response to Bomb Calls.	101
320 - Cite and Release Policy.	106
321 - Medical Marijuana.	110
322 - First Amendment Assemblies.	115
323 - Medical Aid and Response.	123

# Stanislaus County District Attorney's Office

## Policy Manual

---

324 - Body-Worn Cameras. . . . .	128
325 - Vehicle Pursuits. . . . .	137
326 - ADA Compliance. . . . .	148
<b>Chapter 4 - Investigations. . . . .</b>	<b>156</b>
400 - Outside Agency Assistance. . . . .	157
401 - Investigation and Prosecution. . . . .	159
402 - Search and Seizure. . . . .	166
403 - Warrant Service. . . . .	168
404 - Contacts and Temporary Detentions. . . . .	173
405 - Operations Planning and Deconfliction. . . . .	177
406 - Temporary Custody of Juveniles. . . . .	182
407 - On-Call and Call-Out Policy. . . . .	193
408 - Stanislaus County Officer Involved Protocol. . . . .	197
409 - Forensic Genetic Genealogy. . . . .	205
410 - Suspicious Activity Reporting. . . . .	209
411 - Generative Artificial Intelligence Use. . . . .	211
412 - Media Relations. . . . .	215
413 - Criminal Organizations. . . . .	219
414 - Crime and Disaster Scene Integrity. . . . .	224
415 - Domestic Violence. . . . .	226
416 - Gun Violence Restraining Orders. . . . .	234
417 - Hate Crimes. . . . .	238
418 - Foreign Diplomatic and Consular Representatives. . . . .	245
419 - Sexual Assault Investigations. . . . .	249
420 - Child Abuse. . . . .	255
421 - Immigration Violations. . . . .	263
422 - Missing Persons. . . . .	269
423 - Mental Illness Commitments. . . . .	271
424 - Public Recording of Law Enforcement Activity. . . . .	276
425 - Informants. . . . .	279
426 - Senior and Disability Victimization. . . . .	284
427 - Eyewitness Identification. . . . .	299
428 - Brady Material Disclosure. . . . .	303
429 - Public Alerts. . . . .	305
430 - Unmanned Aerial System. . . . .	312
431 - California Witness Relocation and Assistance Program (Cal-WRAP). . . . .	315
432 - Restoration of Rights and Application for Pardon Investigations. . . . .	320
<b>Chapter 5 - Equipment. . . . .</b>	<b>322</b>
500 - Bureau Owned and Personal Property. . . . .	323
501 - Personal Communication Devices. . . . .	325
502 - Vehicle Use. . . . .	328
503 - Military Equipment. . . . .	334
<b>Chapter 6 - Support Services. . . . .</b>	<b>337</b>
600 - Property and Evidence. . . . .	338



# Stanislaus County District Attorney's Office

## Policy Manual

---

601 - Protected Information. . . . .	347
<b>Chapter 7 - Custody. . . . .</b>	<b>351</b>
700 - Temporary Custody of Adults. . . . .	352
701 - Transporting Persons in Custody. . . . .	365
<b>Chapter 8 - Personnel. . . . .</b>	<b>370</b>
800 - Standards of Conduct. . . . .	371
801 - Evaluation of Employees. . . . .	378
803 - Recruitment and Selection. . . . .	381
804 - Pre-employment Background Investigation. . . . .	387
805 - Special Assignments and Promotions. . . . .	389
806 - Grievance Procedure. . . . .	391
807 - Anti-Retaliation. . . . .	392
808 - Reporting of Arrests, Convictions, and Court Orders. . . . .	396
809 - Drug- and Alcohol-Free Workplace. . . . .	399
810 - Sick Leave. . . . .	402
811 - Communicable Diseases. . . . .	404
813 - Personnel Complaints. . . . .	408
814 - Seat Belts. . . . .	419
815 - Body Armor. . . . .	421
816 - Personnel Records. . . . .	423
819 - Lactation Breaks. . . . .	431
821 - Overtime Compensation Requests. . . . .	433
822 - Outside Employment. . . . .	435
824 - Personal Appearance Standards. . . . .	440
825 - Uniform Regulations. . . . .	442
826 - Nepotism and Conflicting Relationships. . . . .	447
827 - Bureau Badges. . . . .	450
828 - Temporary Modified-Duty Assignments. . . . .	452
830 - Employee Speech, Expression and Social Networking. . . . .	456
832 - Line-of-Duty Deaths. . . . .	460
833 - Wellness Program. . . . .	471
<b>Chapter 9 - Traffic Operations. . . . .</b>	<b>475</b>
900 - Impaired Driving. . . . .	476
<b>Attachments. . . . .</b>	<b>482</b>
Statutes and Legal Requirements.pdf. . . . .	483
epo001.pdf. . . . .	484
Addendum B_Countywide Strangulation Form.pdf. . . . .	485
MedicalReleaseFormInv .pdf. . . . .	486
Addendum A_Countywide DV Form.pdf. . . . .	487
Personnel Manual TAB 8 Drug Free Workplace Policy.pdf. . . . .	488
Supplemental Hate Crime Report.pdf. . . . .	489
Complaint and Greivance Procedure.pdf. . . . .	490
CJIS Security Policy v5_5_20160601 (2) (1).pdf. . . . .	491

# Stanislaus County District Attorney's Office

## Policy Manual

---

Background Procedures 2025 nrt.pdf. . . . .	492
DA Office Op Plan Template.pdf. . . . .	493
DA Office Op Plan Template.pdf. . . . .	494
Bail increase affidavit and order 2023B Template-Final.pdf. . . . .	495
Bail increase affidavit and order 2023B Template.pdf. . . . .	496
Driver Authorization and Performance Policy Employee Training Standards.pdf. . . . .	497
Stanislaus County Motor Vehicle Accident Report.pdf. . . . .	498
Application for Authorization to Drive on Official County Business Form.pdf. . . . .	499
Photo Lineup Advisement.pdf. . . . .	500
SCDA Risk Assessment Matrix.pdf. . . . .	501
Live Line Up and In Field Show Up Advisement Form.pdf. . . . .	502
UOF Review Blank Example.pdf. . . . .	503
Hate Crime Checklist.pdf. . . . .	504
SCDA Ops Plan.pdf. . . . .	505
Military Equipment Attachment.pdf. . . . .	506
Questionnaire from LA Cty CertificateRehabandPardonPacket.pdf. . . . .	507
2022-10-03 Military Equipment Attachment.pdf. . . . .	508
2020-05-11 SCDA Ops Plan.pdf. . . . .	509
2022-01-06 UOF Review blank.pdf. . . . .	510
2022-01-06 Pursuit Review blank.pdf. . . . .	511
Supplemental Hate Crime Report-Agency.pdf. . . . .	512

## **Chapter 1 - Law Enforcement Role and Authority**

# Law Enforcement Code of Ethics

## 100.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that all peace officers are aware of their individual responsibilities to maintain their integrity and that of their bureau at all times.

## 100.2 POLICY

The Law Enforcement Code of Ethics shall be administered to all peace officer trainees during the Basic Academy course and to all other persons at the time of appointment (11 CCR 1013).

## 100.3 LAW ENFORCEMENT CODE OF ETHICS

AS A LAW ENFORCEMENT OFFICER, my fundamental duty is to serve; to safeguard lives and property; to protect the innocent against deception, the weak against oppression or intimidation, and the peaceful against abuse or disorder; and to respect the constitutional rights of all to liberty, equality and justice.

I WILL keep my private life unsullied as an example to all; maintain courageous calm in the face of danger, scorn, or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed in both my personal and official life, I will be exemplary in obeying the laws of the land and the regulations of my bureau. Whatever I see or hear of a confidential nature or that is confided to me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

I WILL never act officiously or permit personal feelings, prejudices, animosities or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately without fear or favor, malice or ill will, never employing unnecessary force or violence and never accepting gratuities.

I RECOGNIZE the badge of my office as a symbol of public faith, and I accept it as a public trust to be held so long as I am true to the ethics of the police service. I will constantly strive to achieve these objectives and ideals, dedicating myself before god to my chosen profession... law enforcement.

### 100.3.1 OBJECTION TO RELIGIOUS AFFIRMATION

Reference to religious affirmation in the Law Enforcement Code of Ethics may be omitted where objected to by the investigator.

## Law Enforcement Authority

### 101.1 PURPOSE AND SCOPE

The purpose of this policy is to affirm the authority of the members of the Stanislaus County District Attorney's Office to perform their functions based on established legal authority.

### 101.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to limit its members to only exercise the authority granted to them by law.

While this bureau recognizes the power of peace officers to make arrests and take other enforcement action, investigators are encouraged to use sound discretion in the enforcement of the law. This bureau does not tolerate the abuse of law enforcement authority.

### 101.3 PEACE OFFICER POWERS

Sworn members of this bureau are authorized to exercise peace officer powers pursuant to applicable state law (Penal Code § 830.1 et seq.).

#### 101.3.1 ARREST AUTHORITY INSIDE THE JURISDICTION OF THE STANISLAUS COUNTY DISTRICT ATTORNEY'S OFFICE

The arrest authority within the jurisdiction of the Stanislaus County District Attorney's Office includes (Penal Code § 830.1; Penal Code § 836):

- (a) When the investigator has probable cause to believe the person has committed a felony, whether or not committed in the presence of the investigator.
- (b) When the investigator has probable cause to believe the person has committed a misdemeanor in this jurisdiction and in the presence of the investigator.
- (c) When the investigator has probable cause to believe the person has committed a public offense outside this jurisdiction, in the presence of the investigator and the investigator reasonably believes there is an immediate danger to person or property, or of escape.
- (d) When the investigator has probable cause to believe the person has committed a misdemeanor for which an arrest is authorized or required by statute even though the offense has not been committed in the presence of the investigator such as certain domestic violence offenses.
- (e) In compliance with an arrest warrant.

#### 101.3.2 ARREST AUTHORITY OUTSIDE THE JURISDICTION OF THE STANISLAUS COUNTY DISTRICT ATTORNEY'S OFFICE

The arrest authority outside the jurisdiction of the Stanislaus County District Attorney's Office includes (Penal Code § 830.1; Penal Code § 836):

- (a) When the investigator has probable cause to believe the person committed a felony.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Law Enforcement Authority*

---

- (b) When the investigator has probable cause to believe the person has committed a misdemeanor in the presence of the investigator and the investigator reasonably believes there is immediate danger to person or property or of escape.
- (c) When the investigator has probable cause to believe the person has committed a misdemeanor for which an arrest is authorized even if not committed in the presence of the investigator such as certain domestic violence offenses and there is immediate danger to person or property or of escape or the arrest is mandated by statute.
- (d) When authorized by a cross jurisdictional agreement with the jurisdiction in which the arrest is made.
- (e) In compliance with an arrest warrant.

On-duty arrests will not generally be made outside the jurisdiction of this bureau except in cases of hot or fresh pursuit, while following up on crimes committed within the County, or while assisting another agency.

On-duty investigators who discover criminal activity outside the jurisdiction of the County should when circumstances permit, consider contacting the agency having primary jurisdiction before attempting an arrest.

#### 101.3.3 DELIVERY TO NEAREST MAGISTRATE

When an investigator makes an arrest pursuant to a warrant with bail set, and the warrant was issued in a county other than where the person was arrested, the investigator shall inform the person in writing of the right to be taken before a magistrate in the county where the arrest occurred (Penal Code § 821; Penal Code § 822).

#### 101.3.4 TIME OF MISDEMEANOR ARRESTS

Investigators shall not arrest a person for a misdemeanor between the hours of 10:00 p.m. of any day and 6:00 a.m. of the next day unless (Penal Code § 840):

- (a) The arrest is made without a warrant pursuant to Penal Code § 836 which includes:
  - 1. A misdemeanor committed in the presence of the investigator.
  - 2. Misdemeanor domestic violence offenses (See the Domestic Violence Policy).
- (b) The arrest is made in a public place.
- (c) The arrest is made with the person in custody pursuant to another lawful arrest.
- (d) The arrest is made pursuant to a warrant which, for good cause shown, directs that it may be served at any time of the day or night.

#### 101.3.5 OREGON AUTHORITY

Sworn members of this bureau who enter the state of Oregon in order to provide or attempt to provide law enforcement assistance have Oregon peace officer authority within 50 miles from the California-Oregon border (ORS 133.405). Such authority shall only apply when investigators are acting:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Law Enforcement Authority*

---

- (a) In response to a request for law enforcement assistance initiated by an Oregon sheriff, constable, marshal, municipal police officer or member of the Oregon State Police.
- (b) In response to a reasonable belief that emergency law enforcement assistance is necessary to preserve life, and circumstances make it impractical for Oregon law enforcement officials to formally request assistance.
- (c) For the purpose of assisting Oregon law enforcement officials with emergency assistance in response to criminal activity, traffic accidents, emergency incidents or other similar public safety situations, regardless of whether an Oregon law enforcement official is present at the scene of the incident.

Stanislaus County District Attorney's Office investigators have no authority to enforce Oregon traffic or motor vehicle laws.

Whenever practicable, investigators should seek permission from a bureau supervisor before entering Oregon to provide law enforcement services. As soon as practicable, investigators exercising law enforcement authority in Oregon shall submit any appropriate written reports concerning the incident to the Oregon agency having primary jurisdiction over the area in which the incident occurred.

#### **101.4 INTERSTATE PEACE OFFICER POWERS**

Peace officer powers may be extended to other states:

- (a) As applicable under interstate compacts, memorandums of understanding or mutual aid agreements in compliance with the laws of each state.
- (b) When an investigator enters an adjoining state in close or fresh pursuit of a person believed to have committed a felony (ARS § 13-3832; NRS 171.158; ORS 133.430).

The person arrested out of state must be taken without unnecessary delay before a magistrate of the county in which the arrest was made (ARS § 13-3833; NRS 171.158; ORS 133.440).

#### **101.5 CONSTITUTIONAL REQUIREMENTS**

All members shall observe and comply with every person's clearly established rights under the United States and California Constitutions.

# Chief Executive Officer

## 102.1 PURPOSE AND SCOPE

The California Commission on Peace Officer Standards and Training (POST) has mandated that all sworn officers and dispatchers employed within the State of California shall receive certification by POST within prescribed time periods.

### 102.1.1 CHIEF EXECUTIVE OFFICER REQUIREMENTS

Any sworn member of this bureau appointed after January 1, 1999, shall, as a condition of continued employment, complete the course of training prescribed by POST and obtain the Basic Certificate by POST within two years of appointment (Penal Code § 832.4).



## Oath of Office

### **103.1 PURPOSE AND SCOPE**

The purpose of this policy is to ensure that oaths, when appropriate, are administered to Stanislaus District Attorney members.

### **103.2 POLICY**

It is the policy of the Stanislaus County District Attorney's Office that, when appropriate, members affirm the oath of their office as an expression of commitment to the constitutional rights of those served, and the dedication of its members to their duties.

### **103.3 OATH OF OFFICE**

All members, when appropriate, shall take and subscribe to the oaths or affirmations applicable to their positions. All sworn members shall be required to affirm the oath of office expressing commitment and intent to respect constitutional rights in discharging the duties of a law enforcement officer (Cal. Const. Art. 20, § 3; Government Code § 3102). The oath shall be as follows:

"I, (employee name), do solemnly swear (or affirm) that I will support and defend the Constitution of the United States and the Constitution of the State of California against all enemies, foreign and domestic; that I will bear true faith and allegiance to the Constitution of the United States and the Constitution of the State of California; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties upon which I am about to enter."

### **103.4 MAINTENANCE OF RECORDS**

The oath of office shall be filed as prescribed by law (Government Code § 3105).

# Bureau of Investigation Policy Manual

## 104.1 PURPOSE AND SCOPE

The manual of the Stanislaus County District Attorney's Office is hereby established and shall be referred to as the Policy Manual or the manual. The manual is a statement of the current policies, rules and guidelines of this bureau. All members are to conform to the provisions of this manual.

All prior and existing manuals, orders and regulations that are in conflict with this manual are rescinded, except to the extent that portions of existing manuals, procedures, orders and other regulations that have not been included herein shall remain in effect, provided that they do not conflict with the provisions of this manual.

## 104.2 POLICY

Except where otherwise expressly stated, the provisions of this manual shall be considered as guidelines. It is recognized that the work of law enforcement is not always predictable and circumstances may arise which warrant departure from these guidelines. It is the intent of this manual to be viewed from an objective standard, taking into consideration the sound discretion entrusted to members of this bureau under the circumstances reasonably available at the time of any incident.

### 104.2.1 DISCLAIMER

The provisions contained in the Policy Manual are not intended to create an employment contract nor any employment rights or entitlements. The policies contained within this manual are for the internal use of the Stanislaus County District Attorney's Office and shall not be construed to create a higher standard or duty of care for civil or criminal liability against the County, its officials or members. Violations of any provision of any policy contained within this manual shall only form the basis for bureau administrative action, training or discipline. The Stanislaus County District Attorney's Office reserves the right to revise any policy content, in whole or in part.

## 104.3 AUTHORITY

The Chief of Investigations shall be considered the ultimate authority for the content and adoption of the provisions of this manual and shall ensure compliance with all applicable federal, state and local laws. The Chief of Investigations or the authorized designee is authorized to issue Interim Directives, which shall modify those provisions of the manual to which they pertain. Interim Directives shall remain in effect until such time as they may be permanently incorporated into the manual.

## 104.4 DEFINITIONS

The following words and terms shall have these assigned meanings throughout the Policy Manual, unless it is apparent from the content that they have a different meaning:

**Adult** - Any person 18 years of age or older.

**CCR** - California Code of Regulations (Example: 15 CCR 1151).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Bureau of Investigation Policy Manual*

---

**CHP**- The California Highway Patrol.

**CFR** - Code of Federal Regulations.

**County** - The County of Stanislaus.

**Non-sworn** - Employees and volunteers who are not sworn peace officers.

**Bureau/SCDA** - The Stanislaus County District Attorney's Office.

**DMV** - The Department of Motor Vehicles.

**Employee** - Any person employed by the Bureau.

**Juvenile**- Any person under the age of 18 years.

**Manual** - The Stanislaus County District Attorney's Office Policy Manual.

**May** - Indicates a permissive, discretionary or conditional action.

**Member** - Any person employed or appointed by the Stanislaus County District Attorney's Office, including:

- Full- and part-time employees
- Sworn peace officers
- Interns
- Non-sworn employees
- Volunteers.

**Investigator** - Those employees, regardless of rank, who are sworn peace officers of the Stanislaus County District Attorney's Office.

**On-duty** - A member's status during the period when he/she is actually engaged in the performance of his/her assigned duties.

**Order** - A written or verbal instruction issued by a superior.

**POST** - The California Commission on Peace Officer Standards and Training.

**Rank** - The title of the classification held by an investigator.

**Shall or will** - Indicates a mandatory action.

**Should** - Indicates a generally required or expected action, absent a rational basis for failing to conform.

**Supervisor** - A person in a position of authority that may include responsibility for hiring, transfer, suspension, promotion, discharge, assignment, reward or discipline of other bureau members, directing the work of other members or having the authority to adjust grievances. The supervisory exercise of authority may not be merely routine or clerical in nature but requires the use of independent judgment.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Bureau of Investigation Policy Manual*

---

The term "supervisor" may also include any person (e.g., investigator-in-charge, lead or senior worker) given responsibility for the direction of the work of others without regard to a formal job title, rank or compensation.

When there is only one bureau member on-duty, that person may also be the supervisor, except when circumstances reasonably require the notification or involvement of the member's off-duty supervisor or an on-call supervisor.

**USC** - United States Code.

#### **104.5 ISSUING THE POLICY MANUAL**

An electronic version of the Policy Manual will be made available to all members on the bureau network for viewing and printing. No changes shall be made to the manual without authorization from the Chief of Investigations or the authorized designee.

Each member shall acknowledge that he/she has been provided access to, and has had the opportunity to review the Policy Manual and Interim Directives. Members shall seek clarification as needed from an appropriate supervisor for any provisions that they do not fully understand.

#### **104.6 PERIODIC REVIEW OF THE POLICY MANUAL**

The Chief of Investigations will ensure that the Policy Manual is periodically reviewed and updated as necessary.

#### **104.7 REVISIONS TO POLICIES**

All revisions to the Policy Manual will be provided to each member on or before the date the policy becomes effective. Each member will be required to acknowledge that he/she has reviewed the revisions and shall seek clarification from an appropriate supervisor as needed.

Members are responsible for keeping abreast of all Policy Manual revisions.

Each Lieutenant will ensure that members under his/her command are aware of any Policy Manual revision.

All bureau members suggesting revision of the contents of the Policy Manual shall forward their written suggestions to their Lieutenants, who will consider the recommendations and forward them to the command staff as appropriate.

## **Chapter 2 - Organization and Administration**

# Organizational Structure and Responsibility

## 200.1 PURPOSE AND SCOPE

The organizational structure of this bureau is designed to create an efficient means to accomplish our mission and goals and to provide for the best possible service to the citizens of our community.

## 200.2 SUCCESSION OF COMMAND

The District Attorney is the elected executive officer and department head for the Stanislaus County District Attorney's Office. The Chief of Investigations exercises command over personnel in the District Attorney's Bureau of Investigation. During planned absences, the Chief Investigator may designate a Lieutenant to serve as the acting Chief of Investigations. The Bureau's command authority is as follows:

- (a) Chief Investigator
- (b) Lieutenant
- (c) Lieutenant

Both Bureau Lieutenants supervise and manage many aspects of the Bureau including the activities of the Criminal Investigators who are assigned to one of two Units within the Bureau. The Lieutenants' primary responsibility is to provide general management, direction and control of the Bureau.

## 200.3 BUREAU UNITS

There are 2 units in the Investigations Bureau. They are as follows:

- (a) General Investigation Unit
  1. Criminal Investigators assigned to the General Crimes Unit are assigned to conduct investigations related to cases that are not specific to a vertical unit.
  2. Criminal Investigators are often assigned to assist Deputy District Attorneys with follow up investigations and preparing cases for trial.
- (b) Special Investigation Unit
  1. Criminal Investigators assigned to the Special Investigation Unit are responsible for conducting investigations into crimes related to vertical units.
  2. Criminal Investigators will also assist Deputy District Attorneys with follow up and preparing cases for trial.
  3. Criminal Investigators in the Special Investigation Unit are assigned to a variety of Countywide task forces assisting other local peace officers with investigations.
- (c) Support Staff
  1. Legal Clerks who staff the HUB and Investigative Aide positions.
  2. Paralegals who provide support with all homicide prosecutions.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Organizational Structure and Responsibility*

---

#### **200.4 UNITY OF COMMAND**

The principles of unity of command ensure efficient supervision and control within the Bureau. Generally, each employee shall be accountable to one supervisor at any time for a given assignment or responsibility. Except where specifically delegated authority may exist by policy or special assignment (e.g. SIU, FIU, STANCATT, FBI, CVGIT) any supervisor may temporarily direct any subordinate if an operational necessity exists.

#### **200.5 ORDERS**

Members shall respond to and make a good faith and reasonable effort to comply with the lawful order of a superior having proper authority.

# Interim Directives

## **201.1 PURPOSE AND SCOPE**

Interim Directives establish an interdepartmental communication that may be used by the Chief of Investigations to make immediate changes to policy and procedure consistent with the current Memorandum of Understanding and as permitted by Government Code § 3500 et seq. Interim Directives will immediately modify or change and supersede sections of this manual to which they pertain.

### **201.1.1 INTERIM DIRECTIVE PROTOCOL**

Interim Directives will be incorporated into the manual as required upon approval of the Chief Investigator. Interim Directives will modify existing policies or create a new policy as appropriate and will be rescinded upon incorporation into the manual.

All existing Interim Directives have now been incorporated in the updated Policy Manual as of the below revision date.

Any Interim Directives issued after publication of the manual shall be numbered consecutively starting with the last two digits of the year, followed by the number 01. For example, 12-01 signifies the first Interim Directive for the year 2012.

## **201.2 RESPONSIBILITIES**

### **201.2.1 STAFF**

The staff shall review and approve revisions of the Policy Manual, which will incorporate changes originally made by a Interim Directive.

### **201.2.2 CHIEF OF INVESTIGATIONS**

The Chief of Investigations shall issue all Interim Directives.

## **201.3 ACCEPTANCE OF INTERIM DIRECTIVES**

All employees are required to read and obtain any necessary clarification of all Interim Directives. All employees are required to acknowledge in writing the receipt and review of any new Interim Directive. Signed acknowledgement forms and/or e-mail receipts showing an employee's acknowledgement will be maintained by the Lieutenant.



# Training

## 202.1 PURPOSE AND SCOPE

It is the policy of this bureau to administer a training program that will provide for the professional growth and continued development of its personnel. By doing so, the Bureau will ensure its personnel possess the knowledge and skills necessary to provide a professional level of service that meets the needs of the community.

## 202.2 PHILOSOPHY

The bureau seeks to provide ongoing training and encourages all personnel to participate in advanced training and formal education on a continual basis. Training is provided within the confines of funding, requirements of a given assignment, staffing levels, and legal mandates. Whenever possible, the bureau will use courses certified by the California Commission on Peace Officer Standards and Training (POST).

## 202.3 OBJECTIVES

The objectives of the Training Program are to:

- (a) Enhance the level of law enforcement service to the public.
- (b) Increase the technical expertise and overall effectiveness of our personnel.
- (c) Provide for continued professional development of bureau personnel.
- (d) Ensure compliance with POST rules and regulations concerning law enforcement training.

## 202.4 TRAINING PLAN

A training plan will be developed and maintained by the training manager Lieutenant. It is the responsibility of the training manager to maintain, review, and update the training plan on an annual basis. The plan will address the following areas:

POST required training to include: cultural diversity, legislative mandated training, perishable skills training and refresher training as required.

## 202.5 TRAINING PROCEDURES

- (a) All employees assigned to attend training shall attend as scheduled unless previously excused by their immediate supervisor. Excused absences from mandatory training should be limited to the following:
  - 1. Court appearances
  - 2. Approved vacation
  - 3. Sick leave
  - 4. Physical limitations (injury) preventing the employee's participation.
  - 5. Emergency situations

# Stanislaus County District Attorney's Office

## Policy Manual

### *Training*

---

- (b) When an employee is unable to attend mandatory training, that employee shall:
  - 1. Notify his/her supervisor as soon as possible but no later than one hour prior to the start of training.
  - 2. Document his/her absence in a memorandum to his/her supervisor.
  - 3. Make arrangements through his/her supervisor and the training managerLieutenant to attend the required training on an alternate date.

#### **202.6 DAILY TRAINING BULLETINS**

The Lexipol Daily Training Bulletins (DTBs) is a web-accessed system that provides training on the Stanislaus County District Attorney's Office Policy Manual and other important topics. Generally, one training bulletin is available for each day of the month. However, the number of DTBs may be adjusted by the Lieutenant.

Personnel assigned to participate in DTBs should only use the password and login name assigned to them by the Lieutenant. Personnel should not share their password with others and should frequently change their password to protect the security of the system. After each session, employees should log off the system to prevent unauthorized access. The content of the DTBs is copyrighted material and shall not be shared with others outside of the Bureau.

Employees who are assigned to participate in the DTB program should complete each DTB at the beginning of their shift or as otherwise directed by their supervisor. Employees should not allow uncompleted DTBs to build up over time. Personnel may be required to complete DTBs missed during extended absences (e.g., vacation, medical leave) upon returning to duty. Although the DTB system can be accessed from any Internet active computer, employees shall only take DTBs as part of their on-duty assignment unless directed otherwise by a supervisor.

Supervisors will be responsible for monitoring the progress of personnel under their command to ensure compliance with this policy.

#### **202.7 POLICY**

The Bureau shall administer a training program that will meet the standards of federal, state, local, and POST training requirements. It is a priority of this bureau to provide continuing education and training for the professional growth and development of its members.

#### **202.8 LIEUTENANT**

The Chief of Investigations shall designate a Lieutenant who is responsible for developing, reviewing, updating, and maintaining the bureau training plan so that required training is completed. The Lieutenant should review the training plan annually.

##### **202.8.1 TRAINING RESTRICTION**

The Lieutenant is responsible for establishing a process to identify investigators who are restricted from training other investigators for the time period specified by law because of a sustained use of force complaint (Government Code § 7286(b)).

## Electronic Mail

### 202.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper use and application of the Stanislaus County District Attorney's (SCDA) electronic mail (email) system by employees of this bureau. Email is a communication tool available to employees to enhance efficiency in the performance of job duties and is to be used in accordance with generally accepted business practices and current law (e.g., California Public Records Act). Messages transmitted over the email system must only be those that involve official business activities or contain information essential to employees for the accomplishment of business-related tasks and/or communication directly related to the business, administration, or practices of the Bureau and SCDA.

### 202.2 EMAIL RIGHT OF PRIVACY

All email messages, including any attachments, that are transmitted over SCDA networks are considered SCDA records and therefore are SCDA property. The SCDA reserves the right to access, audit or disclose, for any lawful reason, any message including any attachment that is transmitted over its email system or that is stored on any SCDA system.

The email system is not a confidential system since all communications transmitted on, to or from the system are the property of the SCDA. Therefore, the email system is not appropriate for confidential communications. If a communication must be private, an alternative method to communicate the message should be used instead of email. Employees using the SCDA email system shall have no expectation of privacy concerning communications utilizing the system.

Employees should not use personal accounts to exchange email or other information that is related to the official business of the Bureau or SCDA.

### 202.3 PROHIBITED USE OF EMAIL

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive and harassing or any other inappropriate messages on the email system is prohibited and may result in discipline.

Bureau members are not permitted to send emails to DA\_AllStaff@standa.org unless there is prior approval from a supervisor. This email group includes everyone at the SCDA office and should be used sparingly. There are email groups for DA\_Investigations, DA\_Investigators and DA\_INVassistant that bureau members and clerks should use. Likewise, email messages addressed to the entire bureau are only to be used for official business related items that are of particular interest to bureau members.

It is a violation of this policy to transmit a message under another user's name. Users are strongly encouraged to log off the network when their computer is unattended. This added security measure would minimize the misuse of an individual's email, name and/or password by others.

## Retiree Concealed Firearms

### 203.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the issuance, denial, suspension or revocation of Stanislaus County District Attorney's Office identification cards under the Law Enforcement Officers' Safety Act (LEOSA) and California law (18 USC § 926C; Penal Code § 25455).

### 203.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to provide identification cards to qualified former or retired investigators as provided in this policy.

### 203.3 LEOSA

The Chief of Investigations may issue an identification card for LEOSA purposes to any qualified former investigator of this bureau who (18 USC § 926C(c)):

- (a) Separated from service in good standing from this bureau as an investigator.
- (b) Before such separation, had regular employment as a law enforcement officer for an aggregate of 10 years or more or, if employed as a law enforcement officer for less than 10 years, separated from service after completing any applicable probationary period due to a service-connected disability as determined by this bureau.
- (c) Has not been disqualified for reasons related to mental health.
- (d) Has not entered into an agreement with this bureau where the investigator acknowledges that he/she is not qualified to receive a firearm qualification certificate for reasons related to mental health.
- (e) Is not prohibited by federal law from receiving or possessing a firearm.

#### 203.3.1 LEOSA IDENTIFICATION CARD FORMAT

The LEOSA identification card should contain a photograph of the former investigator and identify him/her as having been employed as an investigator.

If the Stanislaus County District Attorney's Office qualifies the former investigator, the LEOSA identification card or separate certification should indicate the date the former investigator was tested or otherwise found by the Bureau to meet the active duty standards for qualification to carry a firearm.

#### 203.3.2 AUTHORIZATION

Any qualified former law enforcement officer, including a former investigator of this bureau, may carry a concealed firearm under 18 USC § 926C when he/she is:

- (a) In possession of photographic identification that identifies him/her as having been employed as a law enforcement officer, and one of the following:
  - 1. An indication from the person's former law enforcement agency that he/she has, within the past year, been tested or otherwise found by the law enforcement

# Stanislaus County District Attorney's Office

## Policy Manual

### *Retiree Concealed Firearms*

---

agency to meet agency-established active duty standards for qualification in firearms training to carry a firearm of the same type as the concealed firearm.

2. A certification, issued by either the state in which the person resides or by a certified firearms instructor who is qualified to conduct a firearms qualification test for active duty law enforcement officers within that state, indicating that the person has, within the past year, been tested or otherwise found to meet the standards established by the state or, if not applicable, the standards of any agency in that state.
- (b) Not under the influence of alcohol or another intoxicating or hallucinatory drug or substance.
- (c) Not prohibited by federal law from receiving a firearm.
- (d) Not in a location prohibited by California law or by a private person or entity on his/her property if such prohibition is permitted by California law.

#### **203.4 CALIFORNIA IDENTIFICATION CARD ISSUANCE**

Any full-time sworn investigator of this bureau who was authorized to, and did, carry a concealed firearm during the course and scope of his/her employment shall be issued an identification card with a Carrying Concealed Weapon endorsement, "CCW Approved," upon honorable retirement (Penal Code § 25455).

- (a) For the purpose of this policy, honorably retired includes all peace officers who have qualified for, and accepted, a service or disability retirement. It shall not include any investigator who retires in lieu of termination.
- (b) No CCW Approved endorsement shall be issued to any investigator retiring because of a psychological disability (Penal Code § 26305).

##### **203.4.1 CALIFORNIA IDENTIFICATION CARD FORMAT**

The identification card issued to any qualified and honorably retired investigator shall be 2 inches by 3 inches, and minimally contain (Penal Code § 25460):

- (a) A photograph of the retiree.
- (b) The retiree's name and date of birth.
- (c) The date of retirement.
- (d) The name and address of this bureau.
- (e) A stamped CCW Approved endorsement along with the date by which the endorsement must be renewed (not more than one year). If a CCW endorsement has been denied or revoked, the identification card shall be stamped "No CCW Privilege."

#### **203.5 FORMER INVESTIGATOR RESPONSIBILITIES**

A former investigator with a card issued under this policy shall immediately notify the Lieutenant of his/her arrest or conviction in any jurisdiction, or that he/she is the subject of a court order, in accordance with the Reporting of Employee Convictions policy.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Retiree Concealed Firearms*

---

#### 203.5.1 RESPONSIBILITIES UNDER LEOSA

In order to obtain or retain a LEOSA identification card, the former investigator shall:

- (a) Sign a waiver of liability of the Bureau for all acts taken related to carrying a concealed firearm, acknowledging both his/her personal responsibility as a private person for all acts taken when carrying a concealed firearm as permitted by LEOSA and also that these acts were not taken as an employee or former employee of the Bureau.
- (b) Remain subject to all applicable bureau policies and federal, state and local laws.
- (c) Demonstrate good judgment and character commensurate with carrying a loaded and concealed firearm.
- (d) Successfully pass an annual criminal history background check indicating that he/she is not prohibited by law from receiving or possessing a firearm.

#### 203.5.2 MAINTAINING A CALIFORNIA IDENTIFICATION CARD CCW ENDORSEMENT

In order to maintain a CCW Approved endorsement on an identification card issued under California law, the retired investigator shall (Penal Code § 26305):

- (a) Qualify annually with the authorized firearm at a course approved by this bureau at the retired investigator's expense.
- (b) Remain subject to all applicable bureau policies and federal, state and local laws.
- (c) Not engage in conduct that compromises public safety.
- (d) Only be authorized to carry a concealed firearm inspected and approved by the Bureau.

#### **203.6 DENIAL, SUSPENSION, OR REVOCATION OF A LEOSA IDENTIFICATION CARD**

A LEOSA identification card may be denied or revoked upon a showing of good cause as determined by the Bureau. In the event that an identification card is denied, suspended, or revoked, the former investigator may request a review by the Chief of Investigations. The decision of the Chief of Investigations is final.

#### **203.7 DENIAL, SUSPENSION, OR REVOCATION OF A CALIFORNIA CCW ENDORSEMENT CARD**

A CCW endorsement for any investigator retired from this bureau may be denied or revoked only upon a showing of good cause. The CCW endorsement may be immediately and temporarily revoked by the Lieutenant when the conduct of a retired peace officer compromises public safety (Penal Code § 25470).

- (a) In the event that a CCW endorsement is initially denied, the retired investigator shall have 15 days from the date of denial to request a formal hearing. The failure to submit a timely written request for a hearing shall be deemed a waiver of such right. The hearing, absent written agreement between the parties, shall be held no later than 120 days after the request is received.
- (b) Prior to revocation of any CCW endorsement, the Bureau shall provide the affected retiree with written notice of a hearing by either personal service or first class mail,

# Stanislaus County District Attorney's Office

## Policy Manual

### *Retiree Concealed Firearms*

---

postage prepaid, return receipt requested to the retiree's last known address (Penal Code § 26315).

1. The retiree shall have 15 days from the date of service to file a written request for a hearing.
  2. The hearing, absent written agreement between the parties, shall be held no later than 120 days after the request is received (Penal Code § 26315).
  3. The failure to submit a timely written request for a hearing shall be deemed a waiver of such right.
- (c) A hearing for the denial or revocation of any CCW endorsement shall be conducted before a hearing board composed of three members, one selected by the Bureau, one selected by the retiree or his/her employee organization, and one selected jointly (Penal Code § 26320).
1. The decision of such hearing board shall be binding on the Bureau and the retiree.
  2. Any retiree who waives the right to a hearing or whose CCW endorsement has been revoked at a hearing shall immediately surrender his/her identification card. The Bureau will then reissue a new identification card which shall be stamped "No CCW Privilege."
- (d) Members who have reason to suspect the conduct of a retiree has compromised public safety shall notify the Lieutenant as soon as practicable. The Lieutenant should promptly take appropriate steps to look into the matter and, if warranted, contact the retiree in person and advise him/her of the temporary suspension and hearing information listed below.
1. Notification of the temporary suspension should also be promptly mailed to the retiree via first class mail, postage prepaid, return receipt requested (Penal Code § 26312).
  2. The Lieutenant should document the investigation, the actions taken and, if applicable, any notification made to the retiree. The memo should be forwarded to the Chief of Investigations.
  3. The personal and written notification should be as follows:
    - (a) The retiree's CCW endorsement is immediately and temporarily suspended.
    - (b) The retiree has 15 days to request a hearing to determine whether the temporary suspension should become permanent revocation.
    - (c) The retiree will forfeit his/her right to a hearing and the CCW endorsement will be permanently revoked if the retiree fails to respond to the notice of hearing within the 15-day period.
  4. In the event that personal contact with the retiree cannot be reasonably achieved in a timely manner, the Lieutenant should attempt to make the above notice of temporary suspension through another law enforcement officer. For example, if a retiree was arrested or detained by a distant agency, the Lieutenant may

# Stanislaus County District Attorney's Office

## Policy Manual

### *Retiree Concealed Firearms*

---

request that a law enforcement officer from that agency act as the agent of the Bureau to deliver the written notification.

#### **203.8 FIREARM QUALIFICATIONS**

The Rangemaster may provide former investigators from this bureau an opportunity to qualify. Written evidence of the qualification and the weapons used will be provided and will contain the date of the qualification. The Rangemaster will maintain a record of the qualifications and weapons used.



## **Chapter 3 - General Operations**

# Use of Force

## 300.1 PURPOSE AND SCOPE

This policy provides guidelines on the reasonable use of force. While there is no way to specify the exact amount or type of reasonable force to be applied in any situation, every member of this bureau is expected to use these guidelines to make such decisions in a professional, impartial, and reasonable manner (Government Code § 7286).

In addition to those methods, techniques, and tools set forth below, the guidelines for the reasonable application of force contained in this policy shall apply to all policies addressing the potential use of force, including but not limited to the Control Devices and Techniques and Conducted Energy Device policies.

Retaliation prohibitions for reporting suspected violations are addressed in the Anti-Retaliation Policy.

### 300.1.1 DEFINITIONS

Definitions related to this policy include:

**Deadly force** - Any use of force that creates a substantial risk of causing death or serious bodily injury, including but not limited to the discharge of a firearm (Penal Code § 835a).

**Feasible** - Reasonably capable of being done or carried out under the circumstances to successfully achieve the arrest or lawful objective without increasing risk to the investigator or another person (Government Code § 7286(a)).

**Force** - The application of physical techniques or tactics, chemical agents, or weapons to another person. It is not a use of force when a person allows him/herself to be searched, escorted, handcuffed, or restrained.

**Serious bodily injury** - A serious impairment of physical condition, including but not limited to the following: loss of consciousness; concussion; bone fracture; protracted loss or impairment of function of any bodily member or organ; a wound requiring extensive suturing; and serious disfigurement (Penal Code § 243(f)(4)).

**Totality of the circumstances** - All facts known to the investigator at the time, including the conduct of the officer and the subject leading up to the use of force (Penal Code § 835a).

## 300.2 POLICY

The use of force by law enforcement personnel is a matter of critical concern, both to the public and to the law enforcement community. Investigators are involved on a daily basis in numerous and varied interactions and, when warranted, may use reasonable force in carrying out their duties.

Investigators must have an understanding of, and true appreciation for, their authority and limitations. This is especially true with respect to overcoming resistance while engaged in the performance of law enforcement duties.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Use of Force*

---

The Bureau recognizes and respects the value of all human life and dignity without prejudice to anyone. Vesting investigators with the authority to use reasonable force and to protect the public welfare requires monitoring, evaluation and a careful balancing of all interests.

#### **300.2.1 DUTY TO INTERCEDE**

Any investigator present and observing another law enforcement officer or an employee using force that is clearly beyond that which is necessary, as determined by an objectively reasonable investigator under the circumstances, shall, when in a position to do so, intercede (as defined by Government Code § 7286) to prevent the use of unreasonable force.

When observing force used by a law enforcement officer, each investigator should take into account the totality of the circumstances and the possibility that other law enforcement officers may have additional information regarding the threat posed by the subject (Government Code § 7286(b)).

#### **300.2.2 FAIR AND UNBIASED USE OF FORCE**

Investigators are expected to carry out their duties, including the use of force, in a manner that is fair and unbiased (Government Code § 7286(b)). See the Bias-Based Policing Policy for additional guidance.

#### **300.2.3 DUTY TO REPORT EXCESSIVE FORCE**

Any investigator who observes a law enforcement officer or an employee use force that potentially exceeds what the investigator reasonably believes to be necessary shall immediately report these observations to a supervisor (Government Code § 7286(b)).

As used in this subsection, "immediately" means as soon as it is safe and feasible to do so.

#### **300.2.4 FAILURE TO INTERCEDE**

An investigator who has received the required training on the duty to intercede and then fails to act to intercede when required by law, may be disciplined in the same manner as the investigator who used force beyond that which is necessary (Government Code § 7286(b)).

### **300.3 USE OF FORCE**

Investigators shall use only that amount of force that reasonably appears necessary given the facts and totality of the circumstances known to or perceived by the investigator at the time of the event to accomplish a legitimate law enforcement purpose (Penal Code § 835a).

The reasonableness of force will be judged from the perspective of a reasonable investigator on the scene at the time of the incident. Any evaluation of reasonableness must allow for the fact that investigators are often forced to make split-second decisions about the amount of force that reasonably appears necessary in a particular situation, with limited information and in circumstances that are tense, uncertain, and rapidly evolving.

Given that no policy can realistically predict every possible situation an investigator might encounter, investigators are entrusted to use well-reasoned discretion in determining the appropriate use of force in each incident. Investigators may only use a level of force that they

# Stanislaus County District Attorney's Office

## Policy Manual

### *Use of Force*

---

reasonably believe is proportional to the seriousness of the suspected offense or the reasonably perceived level of actual or threatened resistance (Government Code § 7286(b)).

It is also recognized that circumstances may arise in which investigators reasonably believe that it would be impractical or ineffective to use any of the approved or authorized tools, weapons, or methods provided by the Bureau. Investigators may find it more effective or reasonable to improvise their response to rapidly unfolding conditions that they are confronting. In such circumstances, the use of any improvised device or method must nonetheless be objectively reasonable and utilized only to the degree that reasonably appears necessary to accomplish a legitimate law enforcement purpose.

While the ultimate objective of every law enforcement encounter is to avoid or minimize injury, nothing in this policy requires an investigator to retreat or be exposed to possible physical injury before applying reasonable force.

#### 300.3.1 USE OF FORCE TO EFFECT AN ARREST

Any peace officer may use objectively reasonable force to effect an arrest, to prevent escape, or to overcome resistance. A peace officer who makes or attempts to make an arrest need not retreat or desist from his/her efforts by reason of resistance or threatened resistance on the part of the person being arrested; nor shall an investigator be deemed the aggressor or lose his/her right to self-defense by the use of reasonable force to effect the arrest, prevent escape, or to overcome resistance. Retreat does not mean tactical repositioning or other de-escalation techniques (Penal Code § 835a).

#### 300.3.2 FACTORS USED TO DETERMINE THE REASONABLENESS OF FORCE

When determining whether to apply force and evaluating whether an investigator has used reasonable force, a number of factors should be taken into consideration, as time and circumstances permit (Government Code § 7286(b)). These factors include but are not limited to:

- (a) The apparent immediacy and severity of the threat to investigators or others (Penal Code § 835a).
- (b) The conduct of the individual being confronted, as reasonably perceived by the investigator at the time (Penal Code § 835a).
- (c) Investigator/subject factors (age, size, relative strength, skill level, injuries sustained, level of exhaustion or fatigue, the number of investigators available vs. subjects).
- (d) The conduct of the involved investigator leading up to the use of force (Penal Code § 835a).
- (e) The effects of suspected drugs or alcohol.
- (f) The individual's apparent mental state or capacity (Penal Code § 835a).
- (g) The individual's apparent ability to understand and comply with investigator commands (Penal Code § 835a).
- (h) Proximity of weapons or dangerous improvised devices.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Use of Force*

---

- (i) The degree to which the subject has been effectively restrained and his/her ability to resist despite being restrained.
- (j) The availability of other reasonable and feasible options and their possible effectiveness (Penal Code § 835a).
- (k) Seriousness of the suspected offense or reason for contact with the individual prior to and at the time force is used.
- (l) Training and experience of the investigator.
- (m) Potential for injury to investigators, suspects, bystanders, and others.
- (n) Whether the person appears to be resisting, attempting to evade arrest by flight, or is attacking the investigator.
- (o) The risk and reasonably foreseeable consequences of escape.
- (p) The apparent need for immediate control of the subject or a prompt resolution of the situation.
- (q) Whether the conduct of the individual being confronted no longer reasonably appears to pose an imminent threat to the investigator or others.
- (r) Prior contacts with the subject or awareness of any propensity for violence.
- (s) Any other exigent circumstances.

#### 300.3.3 PAIN COMPLIANCE TECHNIQUES

Pain compliance techniques may be effective in controlling a physically or actively resisting individual. Investigators may only apply those pain compliance techniques for which they have successfully completed bureau-approved training. Investigators utilizing any pain compliance technique should consider:

- (a) The degree to which the application of the technique may be controlled given the level of resistance.
- (b) Whether the person can comply with the direction or orders of the investigator.
- (c) Whether the person has been given sufficient opportunity to comply.

The application of any pain compliance technique shall be discontinued once the investigator determines that compliance has been achieved.

#### 300.3.4 CAROTID CONTROL HOLD

On June 5, 2020, Governor Gavin Newsom ordered the California Commission on Peace Officer Training and Standards (P.O.S.T.) to stop teaching the technique and remove it from P.O.S.T. arrest and control training curriculums. As a result, sworn investigators will no longer receive on going training on this force option.

Apart from an immediate and necessary need to prevent serious bodily injury or death to an investigator or citizen, and where no other force options are available, investigators of this Bureau are not authorized to use a carotid control hold. Investigators should understand that the use of teh carotid control hold will be viewed upon as a use of deadly force and will be investigated as such.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Use of Force*

---

A carotid restraint means a vascular neck restraint or any similar restraint, hold, or other defensive tactic in which pressure is applied to the sides of a person's neck that involves a substantial risk of restricting blood flow and may render the person unconscious in order to subdue or control the person (Government Code § 7286.5).

#### 300.3.5 USE OF FORCE TO SEIZE EVIDENCE

In general, investigators may use reasonable force to lawfully seize evidence and to prevent the destruction of evidence. However, investigators are discouraged from using force solely to prevent a person from swallowing evidence or contraband. In the instance when force is used, investigators should not intentionally use any technique that restricts blood flow to the head, restricts respiration or which creates a reasonable likelihood that blood flow to the head or respiration would be restricted. Investigators are encouraged to use techniques and methods taught by the Stanislaus County District Attorney's Office for this specific purpose.

#### 300.3.6 ALTERNATIVE TACTICS - DE-ESCALATION

As time and circumstances reasonably permit, and when community and officer safety would not be compromised, investigators should consider actions that may increase investigator safety and may decrease the need for using force:

- (a) Summoning additional resources that are able to respond in a reasonably timely manner.
- (b) Formulating a plan with responding investigators before entering an unstable situation that does not reasonably appear to require immediate intervention.
- (c) Employing other tactics that do not unreasonably increase investigator jeopardy.

In addition, when reasonable, investigators should evaluate the totality of circumstances presented at the time in each situation and, when feasible, consider and utilize reasonably available alternative tactics and techniques that may persuade an individual to voluntarily comply or may mitigate the need to use a higher level of force to resolve the situation before applying force (Government Code § 7286(b)). Such alternatives may include but are not limited to:

- (a) Attempts to de-escalate a situation.
- (b) If reasonably available, the use of crisis intervention techniques by properly trained personnel.

#### 300.3.7 RESTRICTIONS ON THE USE OF A CHOKE HOLD

Investigators of this bureau are not authorized to use a choke hold. A choke hold means any defensive tactic or force option in which direct pressure is applied to a person's trachea or windpipe (Government Code § 7286.5).

#### 300.3.8 ADDITIONAL RESTRICTIONS

Terms such as "positional asphyxia," "restraint asphyxia," and "excited delirium" continue to remain the subject of debate among experts and medical professionals, are not universally recognized medical conditions, and frequently involve other collateral or controlling factors such

# Stanislaus County District Attorney's Office

## Policy Manual

### *Use of Force*

---

as narcotics or alcohol influence or pre-existing medical conditions. While it is impractical to restrict an investigator's use of reasonable control methods when attempting to restrain a combative individual, investigators are not authorized to use any restraint or transportation method which might unreasonably impair an individual's breathing or respiratory capacity for a period beyond the point when the individual has been adequately and safely controlled. Once the individual is safely secured, investigators should promptly check and continuously monitor the individual's condition for signs of medical distress (Government Code § 7286.5).

#### **300.4 DEADLY FORCE APPLICATIONS**

Where feasible, the investigator shall, prior to the use of deadly force, make reasonable efforts to identify themselves as a peace officer and to warn that deadly force may be used, unless the investigator has objectively reasonable grounds to believe the person is aware of those facts (Penal Code § 835a).

If an objectively reasonable investigator would consider it safe and feasible to do so under the totality of the circumstances, investigators shall evaluate and use other reasonably available resources and techniques when determining whether to use deadly force. To the extent that it is reasonably practical, investigators should consider their surroundings and any potential risks to bystanders prior to discharging a firearm (Government Code § 7286(b)).

The use of deadly force is only justified when the investigator reasonably believes it is necessary in the following circumstances (Penal Code § 835a):

- (a) An investigator may use deadly force to protect themselves or others from what the investigator reasonably believes is an imminent threat of death or serious bodily injury to the investigator or another person.
- (b) An investigator may use deadly force to apprehend a fleeing person for any felony that threatened or resulted in death or serious bodily injury, if the investigator reasonably believes that the person will cause death or serious bodily injury to another unless immediately apprehended.

Investigators shall not use deadly force against a person based on the danger that person poses to themselves, if an objectively reasonable investigator would believe the person does not pose an imminent threat of death or serious bodily injury to the investigator or to another person (Penal Code § 835a).

Additionally, an investigator shall not use deadly force against a person whose actions are a threat solely to property unless the person poses an imminent danger of death or serious physical injury to the investigator or others in close proximity.

An "imminent" threat of death or serious bodily injury exists when, based on the totality of the circumstances, a reasonable investigator in the same situation would believe that a person has the present ability, opportunity, and apparent intent to immediately cause death or serious bodily injury to the investigator or another person. An investigator's subjective fear of future harm alone is insufficient as an imminent threat. An imminent threat is one that from appearances is reasonably believed to require instant attention (Penal Code § 835a).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Use of Force*

---

#### **300.4.1 SHOOTING AT OR FROM MOVING VEHICLES**

Shots fired at or from a moving vehicle are rarely effective and involve considerations and risks in addition to the justification for the use of deadly force. When feasible, investigators should take reasonable steps to move out of the path of an approaching vehicle instead of discharging their firearm at the vehicle or any of its occupants. An investigator should only discharge a firearm at a moving vehicle or its occupants when the investigator reasonably believes there are no other reasonable means available to avert the imminent threat of the vehicle, or if deadly force other than the vehicle is directed at the investigator or others (Government Code § 7286(b)).

Investigators should not shoot at any part of a vehicle in an attempt to disable the vehicle.

#### **300.4.2 DISPLAYING OF FIREARMS**

Given that individuals might perceive the display of a firearm as a potential application of force, investigators should carefully evaluate each tactical situation and use sound discretion when drawing a firearm in public by considering the following guidelines (Government Code § 7286(b)):

- (a) If the investigator does not initially perceive a threat but reasonably believes that the potential for such threat exists, firearms should generally be kept in the low-ready or other position not directed toward an individual.
- (b) If the investigator reasonably believes that a threat exists based on the totality of circumstances presented at the time (e.g., high-risk stop, tactical entry, armed encounter), firearms may be directed toward such threat until the investigator no longer perceives such threat.

Once it is reasonably safe to do so, investigators should carefully secure all firearms.

### **300.5 REPORTING THE USE OF FORCE**

Any use of force by a member of this bureau shall be documented promptly, completely, and accurately in an appropriate report, depending on the nature of the incident. The investigator should articulate the factors perceived and why he/she believed the use of force was reasonable under the circumstances. To collect data for purposes of training, resource allocation, analysis, and related purposes, the Bureau may require the completion of additional report forms, as specified in bureau policy, procedure, or law. See the Report Preparation Policy for additional circumstances that may require documentation.

#### **300.5.1 NOTIFICATION TO SUPERVISORS**

Any use of force by an investigator shall be reported immediately to a supervisor, including but not limited to the following circumstances (Penal Code § 832.13):

- (a) The application caused a visible injury.
- (b) The application would lead a reasonable investigator to conclude that the individual may have experienced more than momentary discomfort.
- (c) The individual subjected to the force complained of injury or continuing pain.
- (d) The individual indicates intent to pursue litigation.
- (e) Any application of a conducted energy device or control device.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Use of Force*

---

- (f) Any application of a restraint device other than handcuffs, shackles, or belly chains.
- (g) The individual subjected to the force was rendered unconscious.
- (h) An individual was struck or kicked.
- (i) An individual alleges unreasonable force was used or that any of the above has occurred.

As used in this subsection, "immediately" means as soon as it is safe and feasible to do so.

#### **300.5.2 REPORTING TO CALIFORNIA DEPARTMENT OF JUSTICE**

Statistical data regarding all officer-involved shootings and incidents involving use of force resulting in serious bodily injury is to be reported to the California Department of Justice as required by Government Code § 12525.2. See the Records Bureau Policy.

#### **300.5.3 REPORT RESTRICTIONS**

Investigators shall not use the term "excited delirium" to describe an individual in an incident report. Investigators may describe the characteristics of an individual's conduct, but shall not generally describe the individual's demeanor, conduct, or physical and mental condition at issue as "excited delirium" (Health and Safety Code § 24402).

#### **300.6 MEDICAL CONSIDERATIONS**

Once it is reasonably safe to do so, properly trained investigators should promptly provide or procure medical assistance for any person injured or claiming to have been injured in a use of force incident (Government Code § 7286(b)).

Prior to booking or release, medical assistance shall be obtained for any person who exhibits signs of physical distress, who has sustained visible injury, expresses a complaint of injury or continuing pain, or who was rendered unconscious. Any individual exhibiting signs of physical distress after an encounter should be continuously monitored until the individual can be medically assessed.

Based upon the investigator's initial assessment of the nature and extent of the subject's injuries, medical assistance may consist of examination by fire personnel, paramedics, hospital staff, or medical staff at the jail. If any such individual refuses medical attention, such a refusal shall be fully documented in related reports and, whenever practicable, should be witnessed by another investigator and/or medical personnel. If a recording is made of the contact or an interview with the individual, any refusal should be included in the recording, if possible.

The on-scene supervisor or, if the on-scene supervisor is not available, the primary handling investigator shall ensure that any person providing medical care or receiving custody of a person following any use of force is informed that the person was subjected to force. This notification shall include a description of the force used and any other circumstances the investigator reasonably believes would be potential safety or medical risks to the subject (e.g., prolonged struggle, extreme agitation, impaired respiration).

Persons who exhibit extreme agitation, violent irrational behavior accompanied by profuse sweating, extraordinary strength beyond their physical characteristics and imperviousness to pain,

# Stanislaus County District Attorney's Office

## Policy Manual

### *Use of Force*

---

or who require a protracted physical encounter with multiple investigators to be brought under control, may be at an increased risk of sudden death. Calls involving these persons should be considered medical emergencies. Investigators who reasonably suspect a medical emergency should request medical assistance as soon as practicable and have medical personnel stage away if appropriate.

See the Medical Aid and Response Policy for additional guidelines.

#### **300.7 LIEUTENANT RESPONSIBILITY**

A Lieutenant should respond to any reported use of force, if reasonably available. The responding Lieutenant is expected to (Government Code § 7286(b)):

- (a) Obtain the basic facts from the involved investigators. Absent an allegation of misconduct or excessive force, this will be considered a routine contact in the normal course of duties.
- (b) Ensure that any injured parties are examined and treated.
- (c) When possible, separately obtain a recorded interview with the subject upon whom force was applied. If this interview is conducted without the person having voluntarily waived his/her *Miranda* rights, the following shall apply:
  - 1. The content of the interview should not be summarized or included in any related criminal charges.
  - 2. The fact that a recorded interview was conducted should be documented in the Lieutenants use of force review report.
  - 3. The recording of the interview should be distinctly marked for retention until all potential for civil litigation has expired.
- (d) Once any initial medical assessment has been completed or first aid has been rendered, ensure that photographs have been taken of any areas involving visible injury or complaint of pain, as well as overall photographs of uninjured areas. These photographs should be retained until all potential for civil litigation has expired.
- (e) Identify any witnesses not already included in related reports.
- (f) Review and approve all related reports.
- (g) Determine if there is any indication that the subject may pursue civil litigation.
  - 1. If there is an indication of potential civil litigation, the supervisor should complete and route a notification of a potential claim through the appropriate channels.
- (h) Evaluate the circumstances surrounding the incident and initiate an administrative investigation if there is a question of policy non-compliance or if for any reason further investigation may be appropriate.
- (i) Once all pertinent information is gathered, complete a use of force review that is forwarded to the Chief Investigator.

See attachment: [2022-01-06 UOF Review blank.pdf](#)

# Stanislaus County District Attorney's Office

## Policy Manual

### *Use of Force*

---

In the event that a Lieutenant is unable to respond to the scene of an incident involving the reported application of force, the Lieutenant is still expected to complete as many of the above items as circumstances permit.

#### **300.8 TRAINING**

Sworn Bureau members will receive annual training on this policy and demonstrate their knowledge and understanding (Government Code § 7286(b)).

##### **300.8.1 TRAINING REQUIREMENTS**

Required annual training should include:

- (a) Legal updates.
- (b) De-escalation tactics, including alternatives to force.
- (c) The duty to intercede.
- (d) The duty to request and/or render medical aid.
- (e) Warning shots (see the Firearms Policy).
- (f) All other subjects covered in this policy (e.g., use of deadly force, chokeholds and carotid holds, discharge of a firearm at or from a moving vehicle, verbal warnings).
- (g) Training courses required by and consistent with POST guidelines set forth in Penal Code § 13519.10.

See the Training Policy for restrictions relating to investigators who are the subject of a sustained use of force complaint.

##### **300.8.2 STATE-SPECIFIC TRAINING REQUIREMENTS**

Required state-specific training shall include guidelines regarding vulnerable populations, including but not limited to children, elderly persons, pregnant individuals, and individuals with physical, mental, and developmental disabilities (Government Code § 7286(b)).

#### **300.9 USE OF FORCE COMPLAINTS**

The receipt, processing, and investigation of civilian complaints involving use of force incidents should be handled in accordance with the Personnel Complaints Policy (Government Code § 7286(b)).

#### **300.10 POLICY REVIEW**

The Chief of Investigations or the authorized designee should regularly review and update this policy to reflect developing practices and procedures (Government Code § 7286(b)).

#### **300.11 POLICY AVAILABILITY**

The Chief of Investigations or the authorized designee should ensure this policy is accessible to the public (Government Code § 7286(c)).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Use of Force*

---

#### **300.12 PUBLIC RECORDS REQUESTS**

Requests for public records involving an investigator's personnel records shall be processed in accordance with Penal Code § 832.7 and the Personnel Records and Records Maintenance and Release policies (Government Code § 7286(b)).

# Handcuffing and Restraints

## 301.1 PURPOSE AND SCOPE

This policy provides guidelines for the use of handcuffs and other restraints during detentions and arrests.

## 301.2 POLICY

The Stanislaus County District Attorney's Office authorizes the use of restraint devices in accordance with this policy, the Use of Force Policy, the Transporting Persons in Custody Policy, and bureau training. Restraint devices shall not be used to punish, to display authority, or as a show of force.

## 301.3 USE OF RESTRAINTS

Only members who have successfully completed Stanislaus County District Attorney's Office-approved training on the use of restraint devices described in this policy are authorized to use these devices.

When deciding whether to use any restraint, investigators should carefully balance officer safety concerns with factors that include but are not limited to:

- The circumstances or crime leading to the arrest.
- The demeanor and behavior of the arrested person.
- The age and health of the person.
- Whether the person is known to be pregnant.
- Whether the person has a hearing or speaking disability. In such cases, consideration should be given, safety permitting, to handcuffing to the front in order to allow the person to sign or write notes.
- Whether the person has any other apparent disability.

### 301.3.1 RESTRAINT OF DETAINEES

Situations may arise where it may be reasonable to restrain a person who may, after brief investigation, be released without arrest. Unless arrested, the use of restraints on detainees should continue only for as long as is reasonably necessary to ensure the safety of investigators and others. When deciding whether to remove restraints from a detainee, investigators should continuously weigh the safety interests at hand against the continuing intrusion upon the detainee.

### 301.3.2 RESTRAINT OF PREGNANT PERSONS

Persons who are known to be pregnant should be restrained in the least restrictive manner that is effective for officer safety. Leg restraints, waist chains, or handcuffs behind the body should not be used unless the investigator has a reasonable suspicion that the person may resist, attempt escape, injure themselves or others, or damage property.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Handcuffing and Restraints*

---

No person who is in labor, delivery, or recovery after delivery shall be handcuffed or restrained except in extraordinary circumstances, and only when a supervisor makes an individualized determination that such restraints are necessary for the safety of the detainee, investigators, or others (Penal Code § 3407; Penal Code § 6030). See the Transporting Persons in Custody Policy for guidelines relating to transporting pregnant persons.

#### **301.3.3 RESTRAINT OF JUVENILES**

A juvenile under 14 years of age should not be restrained unless he/she is suspected of a dangerous felony or when the investigator has a reasonable suspicion that the juvenile may resist, attempt escape, injure him/herself, injure the investigator, or damage property.

#### **301.4 APPLICATION OF HANDCUFFS OR PLASTIC CUFFS**

Handcuffs, including temporary nylon or plastic cuffs, may be used only to restrain a person's hands to ensure officer safety.

Although recommended for most arrest situations, handcuffing is discretionary and not an absolute requirement of the Bureau. Investigators should consider handcuffing any person they reasonably believe warrants that degree of restraint. However, investigators should not conclude that in order to avoid risk every person should be handcuffed, regardless of the circumstances.

In most situations, handcuffs should be applied with the hands behind the person's back. When feasible, handcuffs should be double-locked to prevent tightening, which may cause undue discomfort or injury to the hands or wrists.

In situations where one pair of handcuffs does not appear sufficient to restrain the person or may cause unreasonable discomfort due to the person's size, investigators should consider alternatives, such as using an additional set of handcuffs or multiple plastic cuffs.

Handcuffs should be removed as soon as it is reasonable or after the person has been searched and is safely confined within a detention facility.

#### **301.5 APPLICATION OF SPIT HOODS**

Spit hoods are temporary protective devices designed to prevent the wearer from biting and/or transferring or transmitting fluids (saliva and mucous) to others.

Spit hoods may be placed upon persons in custody when the investigator reasonably believes the person will bite or spit, either on a person or in an inappropriate place. They are generally used during application of a physical restraint, while the person is restrained, or during or after transport.

Investigators utilizing spit hoods should ensure that the spit hood is fastened properly to allow for adequate ventilation and so that the restrained person can breathe normally. Investigators should provide assistance during the movement of a restrained person due to the potential for impairing or distorting that person's vision. Investigators should avoid comingling those wearing spit hoods with other detainees.

Spit hoods should not be used in situations where the restrained person is bleeding profusely from the area around the mouth or nose, or if there are indications that the person has a medical

### *Handcuffing and Restraints*

---

condition, such as difficulty breathing or vomiting. In such cases, prompt medical care should be obtained. If the person vomits while wearing a spit hood, the spit hood should be promptly removed and discarded. Persons who have been sprayed with oleoresin capsicum (OC) spray should be thoroughly decontaminated, including hair, head, and clothing, prior to application of a spit hood.

Those who have been placed in a spit hood should be continually monitored and shall not be left unattended until the spit hood is removed. Spit hoods shall be discarded after each use.

#### **301.6 APPLICATION OF AUXILIARY RESTRAINT DEVICES**

Auxiliary restraint devices include transport belts, waist or belly chains, transportation chains, leg restraints, and other similar devices. Auxiliary restraint devices are intended for use during long-term restraint or transportation. They provide additional security and safety without impeding breathing, while permitting adequate movement, comfort, and mobility.

Only bureau-authorized devices may be used. Any person in auxiliary restraints should be monitored as reasonably appears necessary.

#### **301.7 APPLICATION OF LEG RESTRAINT DEVICES**

Leg restraints may be used to restrain the legs of a violent or potentially violent person when it is reasonable to do so during the course of detention, arrest, or transportation. Only restraint devices approved by the Bureau shall be used.

In determining whether to use the leg restraint, investigators should consider:

- (a) Whether the investigator or others could be exposed to injury due to the assaultive or resistant behavior of a person.
- (b) Whether it is reasonably necessary to protect the person from his/her own actions (e.g., hitting his/her head against the interior of the patrol vehicle, running away from the arresting investigator while handcuffed, kicking at objects or investigators).
- (c) Whether it is reasonably necessary to avoid damage to property (e.g., kicking at windows of the patrol vehicle).

##### **301.7.1 GUIDELINES FOR USE OF LEG RESTRAINTS**

When applying leg restraints, the following guidelines should be followed:

- (a) If practicable, investigators should notify a supervisor of the intent to apply the leg restraint device. In all cases, a supervisor shall be notified as soon as practicable after the application of the leg restraint device.
- (b) Once applied, absent a medical or other emergency, restraints should remain in place until the investigator arrives at the jail or other facility or the person no longer reasonably appears to pose a threat.
- (c) Once secured, the person should be placed in a seated or upright position, secured with a seat belt, and shall not be placed on their stomach for an extended period, as this could reduce the person's ability to breathe.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Handcuffing and Restraints*

---

- (d) The restrained person should be continually monitored by an investigator while in the leg restraint. The investigator should ensure that the person does not roll onto and remain on their stomach.
- (e) The investigator should look for signs of labored breathing and take appropriate steps to relieve and minimize any obvious factors contributing to this condition.

#### **301.8 REQUIRED DOCUMENTATION**

If a person is restrained and released without an arrest, the investigator shall document the details of the detention and the need for handcuffs or other restraints.

If a person is arrested, the use of handcuffs or other restraints shall be documented in the related report.

Investigators should document the following information in reports, as appropriate, when restraints other than handcuffs are used on a person:

- (a) The factors that led to the decision to use restraints.
- (b) Supervisor notification and approval of restraint use.
- (c) The types of restraint used.
- (d) The amount of time the person was restrained.
- (e) How the person was transported and the position of the person during transport.
- (f) Observations of the person's behavior and any signs of physiological problems.
- (g) Any known or suspected drug use or other medical problems.

#### **301.9 TRAINING**

The Lieutenant should ensure that investigators receive periodic training on the proper use of handcuffs and other restraints, including:

- (a) Proper placement and fit of handcuffs and other restraint devices approved for use by the Bureau.
- (b) Response to complaints of pain by restrained persons.
- (c) Options for restraining those who may be pregnant without the use of leg restraints, waist chains, or handcuffs behind the body.
- (d) Options for restraining amputees or those with medical conditions or other physical conditions that may be aggravated by being restrained.
- (e) Proper placement of safely secured persons into an upright or seated position to avoid placement on the stomach for an extended period, as this could reduce the person's ability to breathe.



## Control Devices and Techniques

### 302.1 PURPOSE AND SCOPE

This policy provides guidelines for the use and maintenance of control devices that are described in this policy.

### 302.2 POLICY

In order to control subjects who are violent or who demonstrate the intent to be violent, the Stanislaus County District Attorney's Office authorizes investigators to use control devices in accordance with the guidelines in this policy and the Use of Force Policy.

### 302.3 ISSUING, CARRYING AND USING CONTROL DEVICES

Control devices described in this policy may be carried and used by members of this bureau only if the device has been issued by the Bureau or approved by the Chief of Investigations or the authorized designee.

Only investigators who have successfully completed bureau-approved training in the use of any control device are authorized to carry and use the device.

Control devices may be used when a decision has been made to control, restrain or arrest a subject who is violent or who demonstrates the intent to be violent, and the use of the device appears reasonable under the circumstances. When reasonable, a verbal warning and opportunity to comply should precede the use of these devices.

When using control devices, investigators should carefully consider potential impact areas in order to minimize injuries and unintentional targets.

### 302.4 BATON GUIDELINES

The need to immediately control a suspect must be weighed against the risk of causing serious injury. The head, neck, throat, spine, heart, kidneys and groin should not be intentionally targeted except when the investigator reasonably believes the suspect poses an imminent threat of serious bodily injury or death to the investigator or others.

When carrying a baton, investigators shall carry the baton in its authorized holder on their belt.

### 302.5 OLEORESIN CAPSICUM (OC) GUIDELINES

As with other control devices, oleoresin capsicum (OC) spray and pepper projectiles may be considered for use to bring under control an individual or groups of individuals who are engaging in, or are about to engage in violent behavior. Pepper projectiles and OC spray should not, however, be used against individuals or groups who merely fail to disperse or do not reasonably appear to present a risk to the safety of officers or the public.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Control Devices and Techniques*

---

#### **302.5.1 TREATMENT FOR OC SPRAY EXPOSURE**

Persons who have been sprayed with or otherwise affected by the use of OC should be promptly provided with clean water to cleanse the affected areas. Those persons who complain of further severe effects shall be examined by appropriate medical personnel.

#### **302.6 BEAN BAG SHOTGUN**

The need to immediately control a suspect must be weighted against the risk of causing serious injury. The head, neck, throat, spine, heart, kidneys and groin should not be intentionally targeted except when the officer reasonably believes the suspect poses an imminent threat of serious bodily injury or death to the officer or others. The 12 gauge bean bag should never be deployed against a woman who is known to be or visibly pregnant.

12 gauge drag stabilized bean bag rounds have an optimal range of 5 to 20 yards. At a distance of less than 5 yards, a bean bag round should not be used as an impact munition.

The bean bag shotgun should be maintained in an empty condition meaning, no bean bag rounds shall be loaded into the shotgun chamber or magazine until the bean bag shotgun is deployed and intended to be used to subdue a suspect. Only Office issued 12 gauge bean bag munitions will be carried on or deployed with the bean bag shotgun. No other 12 gauge munitions shall be loaded into a bean bag shotgun or attached to the weapon.

In circumstances permitting and when tactically feasible, the officer deploying the bean bag should call or yell out "BEAN BAG" at least once, loud enough for other peace officers to hear, prior to firing and engaging a suspect.

#### **302.7 POST-APPLICATION NOTICE**

Whenever OC has been introduced into a residence, building interior, vehicle or other enclosed area, investigators should provide the owners or available occupants with notice of the possible presence of residue that could result in irritation or injury if the area is not properly cleaned. Such notice should include advisement that clean up will be at the owner's expense. Information regarding the method of notice and the individuals notified should be included in related reports.

#### **302.8 TRAINING FOR CONTROL DEVICES**

The Lieutenant shall ensure that all personnel who are authorized to carry a control device have been properly trained and certified to carry the specific control device and are retrained or recertified as necessary.

- (a) Proficiency training shall be monitored and documented by a certified, control-device weapons or tactics instructor.
- (b) All training and proficiency for control devices will be documented in the investigator's training file.
- (c) Investigators who fail to demonstrate proficiency with the control device or knowledge of this agency's Use of Force Policy will be provided remedial training. If an investigator cannot demonstrate proficiency with a control device or knowledge of this agency's

# Stanislaus County District Attorney's Office

## Policy Manual

### *Control Devices and Techniques*

---

Use of Force Policy after remedial training, the investigator will be restricted from carrying the control device and may be subject to discipline.

#### **302.9 REPORTING USE OF CONTROL DEVICES AND TECHNIQUES**

Any application of a control device or technique listed in this policy shall be documented in the related incident report and reported pursuant to the Use of Force Policy.

## Firearms

### **303.1 PURPOSE AND SCOPE**

This policy provides guidelines for issuing firearms, the safe and legal carrying of firearms, firearms maintenance and firearms training.

This policy does not apply to issues related to the use of firearms that are addressed in the Use of Force or Officer-Involved Shootings and Deaths policies.

This policy only applies to those members who are authorized to carry firearms.

### **303.2 POLICY**

The Stanislaus County District Attorney's Office will equip its members with firearms to address the risks posed to the public and bureau members by violent and sometimes well-armed persons. The Bureau will ensure firearms are appropriate and in good working order and that relevant training is provided as resources allow.

### **303.3 AUTHORIZED FIREARMS, AMMUNITION AND OTHER WEAPONS**

Members shall only use firearms that are issued or approved by the Bureau and have been thoroughly inspected by the Rangemaster. Except in an emergency or as directed by a supervisor, no firearm shall be carried by a member who has not qualified with that firearm at an authorized bureau range.

All other weapons not provided by the Bureau, including but not limited to edged weapons, chemical or electronic weapons, impact weapons or any weapon prohibited or restricted by law or that is not covered elsewhere by bureau policy, may not be carried by members in the performance of their official duties without the express written authorization of the member's Lieutenant. This exclusion does not apply to the carrying of a single folding pocketknife that is not otherwise prohibited by law.

#### **303.3.1 HANDGUNS**

The authorized bureau-issued handgun is the Glock Gen 5, 19, 9mm. The bureau allows members to carry other approved handguns at the members own expense. The approved duty calibers are 9mm, 40 cal and 45 ACP. Within the approved calibers, any reputable handgun manufacturer can be utilized by the member as long as the member can qualify with the handgun and is approved by the Range Lieutenant and Chief Investigator. Any personally owned handgun utilized for duty use must be inspected by a Rangemaster prior to its use.

#### **303.3.2 SHOTGUNS**

The authorized bureau-issued shotgun is the Remington 870 12 gauge. The bureau allows members to carry other approved 12 gauge shotguns at the members own expense. Any reputable 12 gauge shotgun manufacturer can be utilized by the member as long as the member can qualify with the shotgun and have the approval of the Range Lieutenant and Chief Investigator. Any

# Stanislaus County District Attorney's Office

## Policy Manual

### *Firearms*

---

personally owned shotguns utilized for duty use must be inspected by a Rangemaster prior to its use.

When not deployed, the shotgun shall be properly secured consistent with bureau training in a locking weapons rack in the investigators vehicle.

#### 303.3.3 PATROL RIFLES

The authorized bureau-issued patrol rifle is the Colt AR-15 .223. The bureau allows members to carry other approved patrol rifles purchased at the members own expense. Any reputable rifle manufacturer can be utilized by the member as long as the member can qualify with the patrol rifle and it is approved by the Range Lieutenant and Chief Investigator. Any personally owned patrol rifles utilized for duty use must be inspected by a Rangemaster prior to its use.

Members may deploy the patrol rifle in any circumstance where the member can articulate a reasonable expectation that the rifle may be needed. Examples of some general guidelines for deploying the patrol rifle may include but are not limited to:

- (a) Situations where the member reasonably anticipates an armed encounter.
- (b) When a member is faced with a situation that may require accurate and effective fire at long range.
- (c) Situations where a member reasonably expects the need to meet or exceed a suspect's firepower.
- (d) When a member reasonably believes that there may be a need to fire on a barricaded person or a person with a hostage.
- (e) When a member reasonably believes that a suspect may be wearing body armor.
- (f) When authorized or requested by a supervisor.
- (g) When needed to euthanize an animal.

When not deployed, the patrol rifle shall be properly secured consistent with bureau training in a locking weapons rack in the Investigators vehicle.

#### 303.3.4 PERSONALLY OWNED DUTY FIREARMS

Members desiring to carry an authorized but personally owned duty firearm must receive approval from the Range Lieutenant and Chief of Investigations. Once approved, personally owned duty firearms are subject to the following restrictions:

- (a) The firearm shall be in good working order and made by a reputable firearm manufacturer.
- (b) The firearm shall be inspected by a Rangemaster prior to being carried and thereafter shall be subject to inspection whenever it is deemed necessary.
- (c) Prior to carrying the firearm, members shall qualify under range supervision and thereafter shall qualify in accordance with the bureau qualification schedule. Members must demonstrate proficiency and safe handling, and that the firearm functions properly.

# Stanislaus County District Attorney's Office

## Policy Manual

### Firearms

---

- (d) Members shall provide written notice of the make, model, color, serial number and caliber of the firearm to the Rangemaster, who will maintain a list of the information.

#### 303.3.5 AUTHORIZED SECONDARY HANDGUN

Members desiring to carry bureau or personally owned secondary handguns are subject to the following restrictions:

- (a) The handgun shall be in good working order and made by a reputable firearm manufacturer.
- (b) Only one secondary handgun may be carried at a time.
- (c) The purchase of the handgun and ammunition shall be the responsibility of the member unless the handgun and ammunition are provided by the Bureau.
- (d) The handgun shall be carried concealed at all times and in such a manner as to prevent unintentional cocking, discharge or loss of physical control.
- (e) The handgun shall be inspected by the Rangemaster prior to being carried and thereafter shall be subject to inspection whenever it is deemed necessary.
- (f) Ammunition shall be the same as bureau issue. If the caliber of the handgun is other than bureau issue, the Range Lieutenant and Chief Investigator shall approve the ammunition.
- (g) Prior to carrying the secondary handgun, members shall qualify under range supervision and thereafter shall qualify in accordance with the bureau qualification schedule. Members must demonstrate proficiency and safe handling, and that the handgun functions properly.
- (h) Members shall provide written notice of the make, model, color, serial number and caliber of a secondary handgun to the Rangemaster, who will maintain a list of the information.

#### 303.3.6 AUTHORIZED OFF-DUTY FIREARMS

The carrying of firearms by members while off-duty is permitted by the Chief of Investigations but may be rescinded should circumstances dictate (e.g., administrative leave). Members who choose to carry a firearm while off-duty, based on their authority as peace officers, will be required to meet the following guidelines:

- (a) The member may use his/her duty firearm or may use a personally owned firearm that is carried and inspected in accordance with the Personally Owned Duty Firearms requirements in this policy. A member carrying his/her duty firearm will be deemed to have complied with (c), (d) and (e) of this section.
  - 1. The purchase of the personally owned firearm and ammunition shall be the responsibility of the member.
- (b) The firearm shall be carried concealed at all times and in such a manner as to prevent accidental unintentional cocking, discharge or loss of physical control.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Firearms*

---

- (c) It will be the responsibility of the member to submit the firearm to the Rangemaster for inspection prior to being personally carried. Thereafter the firearm shall be subject to periodic inspection by the Rangemaster.
- (d) Prior to carrying any off-duty firearm, the member shall demonstrate to the Rangemaster that he/she is proficient in handling and firing the firearm and that it will be carried in a safe manner.
- (e) The member will successfully qualify with the firearm prior to it being carried.
- (f) Members shall provide written notice of the make, model, color, serial number and caliber of the firearm to the Rangemaster, who will maintain a list of the information.
- (g) If a member desires to use more than one firearm while off-duty, he/she may do so, as long as all requirements set forth in this policy for each firearm are met.
- (h) Members shall only carry bureau-authorized ammunition.
- (i) When armed, investigators shall carry their issued flat badge and/or their Stanislaus County District Attorney's Office identification cards under circumstances requiring possession of such identification.

#### **303.3.7 AMMUNITION**

Members shall carry only bureau-authorized ammunition. At the direction of a Rangemaster, members shall be issued fresh duty ammunition in the specified quantity for all bureau-issued firearms during the member's firearms qualification. Replacements for unserviceable or depleted ammunition issued by the Bureau shall be dispensed by the Rangemaster when needed, in accordance with established policy.

Members carrying personally owned authorized firearms of a caliber differing from bureau-issued firearms shall be responsible for obtaining fresh duty ammunition in accordance with the above, at their own expense.

#### **303.4 EQUIPMENT**

Firearms carried on or off-duty shall be maintained in a clean, serviceable condition. Maintenance and repair of authorized personally owned firearms are the responsibility of the individual member.

##### **303.4.1 REPAIRS OR MODIFICATIONS**

Each member shall be responsible for promptly reporting any damage or malfunction of an assigned firearm to a supervisor or the Rangemaster.

Firearms that are the property of the Bureau or personally owned firearms that are approved for bureau use may be repaired or modified only by a person who is bureau-approved and certified as an armorer or gunsmith in the repair of the specific firearm. Such modification or repair must be authorized in advance by the Rangemaster.

Any repairs or modifications to the member's personally owned firearm shall be done at his/her expense and must be approved by the Rangemaster.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Firearms*

---

Modular weapon systems are permitted for use as long as the system is from a reputable firearms manufacturer and approved/inspected by Department Range Staff. If the modular system utilizes more than one serial number for identification, both serial numbers will be recorded by Range Staff.

#### **303.4.2 HOLSTERS**

Only bureau-approved holsters shall be used and worn by members. Members shall periodically inspect their holsters to make sure they are serviceable and provide the proper security and retention of the handgun.

#### **303.4.3 TACTICAL LIGHTS**

Tactical lights may only be installed on a firearm carried on or off-duty after they have been examined and approved by the Rangemaster.

#### **303.4.4 OPTICS OR LASER SIGHTS**

Optics or laser sights may only be installed on a firearm carried on or off-duty after they have been examined and approved by the Rangemaster. Any approved sight shall only be installed in strict accordance with manufacturer specifications. Once approved sights have been properly installed on any firearm, the member shall qualify with the firearm to ensure proper functionality and sighting of the firearm prior to carrying it.

### **303.5 SAFE HANDLING, INSPECTION AND STORAGE**

Members shall maintain the highest level of safety when handling firearms and shall consider the following:

- (a) Members shall not unnecessarily display or handle any firearm.
- (b) Members shall be governed by all rules and regulations pertaining to the use of the range and shall obey all orders issued by the Rangemaster. Members shall not dry fire or practice quick draws except as instructed by the Rangemaster or other firearms training staff.
- (c) Members shall not clean, repair, load or unload a firearm anywhere in the Bureau, except where clearing barrels are present.
- (d) Shotguns or rifles removed from vehicles or the equipment storage room shall be loaded and unloaded in the parking lot and outside of the vehicle, using clearing barrels when available. In all other cases, due care should be directed at keeping the muzzle pointed in a safe direction while loading and unloading.
- (e) Members shall not place or store any firearm or other weapon on bureau premises except where the place of storage is locked. No one shall carry firearms into the jail section or any part thereof when securing or processing an arrestee, but shall place all firearms in a secured location. Members providing access to the jail section to persons from outside agencies are responsible for ensuring firearms are not brought into the jail section.
- (f) Members shall not use any automatic firearm, heavy caliber rifle, gas or other type of chemical weapon or firearm from the armory, except with approval of a supervisor.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Firearms*

---

- (g) Any firearm authorized by the Bureau to be carried on or off-duty that is determined by a member to be malfunctioning or in need of service or repair shall not be carried. It shall be promptly presented to the Bureau or a Rangemaster approved by the Bureau for inspection and repair. Any firearm deemed in need of repair or service by the Rangemaster will be immediately removed from service. If the firearm is the member's primary duty firearm, a replacement firearm will be issued to the member until the duty firearm is serviceable.

#### 303.5.1 INSPECTION AND STORAGE

Member issued and personally owned duty firearms shall be inspected regularly and upon access or possession by another person. The member shall ensure that the firearm is carried in the proper condition and loaded with approved ammunition. Inspection of the shotgun and rifle shall be done while standing outside of the Investigators vehicle. All firearms shall be pointed in a safe direction or into clearing barrels.

All non-issued firearms, ammunition and related firearms equipment will be safely stored in the bureau armory.

#### 303.5.2 STORAGE AT HOME

Members shall ensure that all firearms and ammunition are locked and secured while in their homes, vehicles or any other area under their control, and in a manner that will keep them inaccessible to children and others who should not have access. Members shall not permit bureau-issued firearms to be handled by anyone not authorized by the Bureau to do so. Members should be aware that negligent storage of a firearm could result in civil and criminal liability (Penal Code § 25100).

#### 303.5.3 STORAGE IN VEHICLES

When leaving a handgun in an unattended vehicle, members shall ensure that it is locked in the trunk, or in a locked container that is placed out of view, or in a locked container that is permanently affixed to the vehicle's interior and not in plain view, or in a locked toolbox or utility box permanently affixed to the vehicle (Penal Code § 25140; Penal Code § 25452).

If the vehicle does not have a trunk or a locked container, then the firearm should be locked within the center utility console that can be locked with a padlock, keylock, combination lock, or other similar locking device (Penal Code § 25140).

Investigators are exempt from these requirements during circumstances requiring immediate aid or action in the course of official duties (Penal Code § 25140).

#### 303.5.4 ALCOHOL AND DRUGS

Firearms shall not be carried by any member, either on or off-duty, who has consumed an amount of an alcoholic beverage, taken any drugs or medication, or has taken any combination thereof that would tend to adversely affect the member's senses or judgment.

### *Firearms*

---

#### **303.6 FIREARMS TRAINING AND QUALIFICATIONS**

All members who carry a firearm while on or off-duty are required to successfully complete monthly firearms training. Members shall successfully qualify with their duty, secondary and off-duty firearms every six months. Training and qualifications must be on an approved range course. Members must seek approval from their immediate supervisor prior to being absent from firearms training. In addition to practical firearms training at an approved range, training can include any of the following: roll call training, training videos, case studies/debriefs, policy review, and force options simulators.

At least annually, all members carrying a firearm should receive practical training designed to simulate field situations including low-light shooting.

##### **303.6.1 NON-CERTIFICATION OR NON-QUALIFICATION**

If any member fails to meet minimum standards for firearms training or qualification for any reason, including injury, illness, duty status or scheduling conflict, that member shall submit a memorandum to his/her immediate supervisor prior to the end of the required training or qualification period.

Those who fail to meet minimum standards or qualify on their first shooting attempt shall be provided remedial training and will be subject to the following requirements:

- (a) Additional range assignments may be scheduled to assist the member in demonstrating consistent firearm proficiency.
- (b) Members shall be given credit for a range training or qualification when obtaining a qualifying score or meeting standards after remedial training.
- (c) No range credit will be given for the following:
  - 1. Unauthorized range make-up
  - 2. Failure to meet minimum standards or qualify after remedial training

Members who repeatedly fail to meet minimum standards will be removed from field assignment and may be subject to disciplinary action.

#### **303.7 FIREARM DISCHARGE**

Except during training or recreational use, any member who discharges a firearm intentionally or unintentionally, on or off-duty, shall make a verbal report to his/her supervisor as soon as circumstances permit. If the discharge results in injury or death to another person, additional statements and reports shall be made in accordance with the Officer-Involved Shootings and Deaths Policy. If a firearm was discharged as a use of force, the involved member shall adhere to the additional reporting requirements set forth in the Use of Force Policy.

In all other cases, written reports shall be made as follows:

- (a) If on-duty at the time of the incident, the member shall file a written report with his/her Lieutenant or provide a recorded statement to investigators prior to the end of shift, unless otherwise directed.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Firearms*

---

- (b) If off-duty at the time of the incident, the member shall file a written report or provide a recorded statement no later than the end of the next regularly scheduled shift, unless otherwise directed by a supervisor.

#### **303.7.1 DESTRUCTION OF ANIMALS**

Members are authorized to use firearms to stop an animal in circumstances where the animal reasonably appears to pose an imminent threat to human safety and alternative methods are not reasonably available or would likely be ineffective.

In circumstances where there is sufficient advance notice that a potentially dangerous animal may be encountered, bureau members should develop reasonable contingency plans for dealing with the animal (e.g., fire extinguisher, conducted energy device, oleoresin capicum (OC) spray, animal control officer). Nothing in this policy shall prohibit any member from shooting a dangerous animal if circumstances reasonably dictate that a contingency plan has failed, becomes impractical, or if the animal reasonably appears to pose an imminent threat to human safety.

#### **303.7.2 INJURED ANIMALS**

With the approval of a supervisor, a member may euthanize an animal that is so badly injured that human compassion requires its removal from further suffering and where other dispositions are impractical.

Stray or abandoned injured animals that may be moved or taken to an available veterinarian should not be euthanized. With supervisor approval, abandoned injured animals (with the exception of dogs and cats) may only be euthanized after a reasonable search to locate the owner has been made. Injured dogs and cats found without their owners shall be taken to an appropriate veterinarian for determination of whether they should be treated or humanely destroyed (Penal Code § 597.1).

#### **303.7.3 WARNING AND OTHER SHOTS**

Generally, shots fired for the purpose of summoning aid are discouraged and may not be discharged unless the member reasonably believes that they appear necessary, effective, and reasonably safe.

Warning shots shall not be used.

### **303.8 RANGEMASTER DUTIES**

The range will be under the exclusive control of the Rangemaster. All members attending will follow the directions of the Rangemaster. The Rangemaster will maintain a roster of all members attending the range and will submit the roster to the RangeLieutenant after each range date.

The range shall remain operational and accessible to bureau members during hours established by the Bureau.

The Rangemaster has the responsibility of making periodic inspection, at least once a year, of all duty firearms carried by members of this bureau to verify proper operation. The Rangemaster has the authority to deem any bureau-issued or personally owned firearm unfit for service. The

# Stanislaus County District Attorney's Office

## Policy Manual

### *Firearms*

---

member will be responsible for all repairs to his/her personally owned firearm and it will not be returned to service until inspected by the Rangemaster.

The Rangemaster has the responsibility for ensuring each member meets the minimum requirements during training shoots and, on at least a yearly basis, can demonstrate proficiency in the care, cleaning and safety of all firearms the member is authorized to carry.

The Rangemaster shall complete and submit to the Range and Training Lieutenant documentation of the training courses provided. Documentation shall include the qualifications of each instructor who provides the training, a description of the training provided and, on a form that has been approved by the Bureau, a list of each member who completes the training. The Rangemaster should keep accurate records of all training shoots, qualifications, repairs, maintenance or other records as directed by the Range Lieutenant.

#### **303.9 FLYING WHILE ARMED**

The Transportation Security Administration (TSA) has imposed rules governing law enforcement officers flying armed on commercial aircraft. The following requirements apply to investigators who intend to be armed while flying on a commercial air carrier or flights where screening is conducted (49 CFR 1544.219):

- (a) Investigators wishing to fly while armed must be flying in an official capacity, not for vacation or pleasure, and must have a need to have the firearm accessible, as determined by the Bureau based on the law and published TSA rules.
- (b) Investigators must carry their Stanislaus County District Attorney's Office identification card and badge, bearing the investigator's name, a full-face photograph, identification number, the investigator's signature and the signature of the Chief of Investigations or the official seal of the Bureau and must present this identification to airline officials when requested. The investigator should also carry the standard photo identification needed for passenger screening by airline and TSA officials (e.g., driver license, passport).
- (c) The Stanislaus County District Attorney's Office must submit a National Law Enforcement Telecommunications System (NLETS) message prior to the investigator's travel. If approved, TSA will send the Stanislaus County District Attorney's Office an NLETS message containing a unique alphanumeric identifier. The investigator must present the message on the day of travel to airport personnel as authorization to travel while armed.
- (d) An official letter signed by the Chief of Investigations authorizing armed travel may also accompany the investigator. The letter should outline the investigator's need to fly armed, detail his/her itinerary, and include that the investigator has completed the mandatory TSA training for a law enforcement officer flying while armed.
- (e) Investigators must have completed the mandated TSA security training covering investigators flying while armed. The training shall be given by the bureau-appointed instructor.

# Stanislaus County District Attorney's Office

## Policy Manual

### Firearms

---

- (f) It is the investigator's responsibility to notify the air carrier in advance of the intended armed travel. This notification should be accomplished by early check-in at the carrier's check-in counter.
- (g) Any investigator flying while armed should discreetly contact the flight crew prior to take-off and notify them of his/her assigned seat.
- (h) Discretion must be used to avoid alarming passengers or crew by displaying a firearm. The investigator must keep the firearm concealed on his/her person at all times. Firearms are not permitted in carry-on luggage and may not be stored in an overhead compartment.
- (i) Investigators should try to resolve any problems associated with flying armed through the flight captain, ground security manager, TSA representative or other management representative of the air carrier.
- (j) Investigators shall not consume alcoholic beverages while aboard an aircraft, or within eight hours prior to boarding an aircraft.

#### **303.10 CARRYING FIREARMS OUT OF STATE**

Qualified, active, full-time investigators of this bureau are authorized to carry a concealed firearm in all other states subject to the following conditions (18 USC § 926B):

- (a) The investigator shall carry his/her Stanislaus County District Attorney's Office identification card and badge whenever carrying such firearm.
- (b) The investigator is not the subject of any current disciplinary action.
- (c) The investigator may not be under the influence of alcohol or any other intoxicating or hallucinatory drug.
- (d) The investigator will remain subject to this and all other bureau policies (including qualifying and training).

Investigators are cautioned that individual states may enact local regulations that permit private persons or entities to prohibit or restrict the possession of concealed firearms on their property, or that prohibit or restrict the possession of firearms on any state or local government property, installation, building, base or park. Federal authority may not shield an investigator from arrest and prosecution in such locally restricted areas.

Active law enforcement officers from other states are subject to all requirements set forth in 18 USC § 926B.

## Foot Pursuits

### 304.1 PURPOSE AND SCOPE

This policy provides guidelines to assist investigators in making the decision to initiate or continue the pursuit of suspects on foot.

### 304.2 POLICY

It is the policy of this bureau that investigators, when deciding to initiate or continue a foot pursuit, continuously balance the objective of apprehending the suspect with the risk and potential for injury to bureau members, the public or the suspect.

Investigators are expected to act reasonably, based on the totality of the circumstances.

### 304.3 DECISION TO PURSUE

The safety of bureau members and the public should be the primary consideration when determining whether a foot pursuit should be initiated or continued. Investigators must be mindful that immediate apprehension of a suspect is rarely more important than the safety of the public and bureau members.

Investigators may be justified in initiating a foot pursuit of any individual the investigator reasonably believes is about to engage in, is engaging in or has engaged in criminal activity. The decision to initiate or continue such a foot pursuit, however, must be continuously re-evaluated in light of the circumstances presented at the time.

Mere flight by a person who is not suspected of criminal activity shall not serve as justification for engaging in an extended foot pursuit without the development of reasonable suspicion regarding the individual's involvement in criminal activity or being wanted by law enforcement.

Deciding to initiate or continue a foot pursuit is a decision that an investigator must make quickly and under unpredictable and dynamic circumstances. It is recognized that foot pursuits may place bureau members and the public at significant risk. Therefore, no investigator or supervisor shall be criticized or disciplined for deciding not to engage in a foot pursuit because of the perceived risk involved.

If circumstances permit, surveillance and containment are generally the safest tactics for apprehending fleeing persons. In deciding whether to initiate or continue a foot pursuit, an investigator should continuously consider reasonable alternatives to a foot pursuit based upon the circumstances and resources available, such as:

- (a) Containment of the area.
- (b) Saturation of the area with law enforcement personnel, including assistance from other agencies.
- (c) A canine search.
- (d) Thermal imaging or other sensing technology.

### *Foot Pursuits*

---

- (e) Air support.
- (f) Apprehension at another time when the identity of the suspect is known or there is information available that would likely allow for later apprehension, and the need to immediately apprehend the suspect does not reasonably appear to outweigh the risk of continuing the foot pursuit.

#### **304.4 GENERAL GUIDELINES**

When reasonably practicable, investigators should consider alternatives to engaging in or continuing a foot pursuit when:

- (a) Directed by a supervisor to terminate the foot pursuit; such an order shall be considered mandatory
- (b) The investigator is acting alone.
- (c) Two or more investigators become separated, lose visual contact with one another, or obstacles separate them to the degree that they cannot immediately assist each other should a confrontation take place. In such circumstances, it is generally recommended that a single investigator keep the suspect in sight from a safe distance and coordinate the containment effort.
- (d) The investigator is unsure of his/her location and direction of travel.
- (e) The investigator is pursuing multiple suspects and it is not reasonable to believe that the investigator would be able to control the suspect should a confrontation occur.
- (f) The physical condition of the investigator renders him/her incapable of controlling the suspect if apprehended.
- (g) The investigator loses radio contact with the dispatcher or with assisting or backup investigators.
- (h) The suspect enters a building, structure, confined space, isolated area or dense or difficult terrain, and there are insufficient investigators to provide backup and containment. The primary investigator should consider discontinuing the foot pursuit and coordinating containment pending the arrival of sufficient resources.
- (i) The investigator becomes aware of unanticipated or unforeseen circumstances that unreasonably increase the risk to investigators or the public.
- (j) The investigator reasonably believes that the danger to the pursuing investigators or public outweighs the objective of immediate apprehension.
- (k) The investigator loses possession of his/her firearm or other essential equipment.
- (l) The investigator or a third party is injured during the pursuit, requiring immediate assistance, and there are no other emergency personnel available to render assistance.

### *Foot Pursuits*

---

- (m) The suspect's location is no longer definitely known.
- (n) The identity of the suspect is established or other information exists that will allow for the suspect's apprehension at a later time, and it reasonably appears that there is no immediate threat to bureau members or the public if the suspect is not immediately apprehended.
- (o) The investigator's ability to safely continue the pursuit is impaired by inclement weather, darkness or other environmental conditions.

### **304.5 RESPONSIBILITIES IN FOOT PURSUITS**

#### **304.5.1 INITIATING INVESTIGATOR RESPONSIBILITIES**

Unless relieved by another investigator or a supervisor, the initiating investigator shall be responsible for coordinating the progress of the pursuit. When acting alone and when practicable, the initiating investigator should not attempt to overtake and confront the suspect but should attempt to keep the suspect in sight until sufficient investigators are present to safely apprehend the suspect.

Early communication of available information from the involved investigators is essential so that adequate resources can be coordinated and deployed to bring a foot pursuit to a safe conclusion. Investigators initiating a foot pursuit should, at a minimum, broadcast the following information as soon as it becomes practicable and available:

- (a) Location and direction of travel
- (b) Call sign identifier
- (c) Reason for the foot pursuit, such as the crime classification
- (d) Number of suspects and description, to include name if known
- (e) Whether the suspect is known or believed to be armed with a dangerous weapon

Investigators should be mindful that radio transmissions made while running may be difficult to understand and may need to be repeated.

Absent extenuating circumstances, any investigator unable to promptly and effectively broadcast this information should terminate the foot pursuit. If the foot pursuit is discontinued for any reason, immediate efforts for containment should be established and alternatives considered based upon the circumstances and available resources.

When a foot pursuit terminates, the investigator will notify the dispatcher of his/her location and the status of the pursuit termination (e.g., suspect in custody, lost sight of suspect), and will direct further actions as reasonably appear necessary, to include requesting medical aid as needed for investigators, suspects or members of the public.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Foot Pursuits*

---

#### **304.5.2 ASSISTING INVESTIGATOR RESPONSIBILITIES**

Whenever any investigator announces that he/she is engaged in a foot pursuit, all other investigators should minimize non-essential radio traffic to permit the involved investigators maximum access to the radio frequency.

#### **304.5.3 SUPERVISOR RESPONSIBILITIES**

Upon becoming aware of a foot pursuit, the supervisor shall make every reasonable effort to ascertain sufficient information to direct responding resources and to take command, control and coordination of the foot pursuit. The supervisor should respond to the area whenever possible; the supervisor does not, however, need not be physically present to exercise control over the foot pursuit. The supervisor shall continuously assess the situation in order to ensure the foot pursuit is conducted within established bureau guidelines.

The supervisor shall terminate the foot pursuit when the danger to pursuing investigators or the public appears to unreasonably outweigh the objective of immediate apprehension of the suspect.

Upon apprehension of the suspect, the supervisor shall promptly proceed to the termination point to direct the post-foot pursuit activity.

#### **304.5.4 SR 911 RESPONSIBILITIES**

Upon notification or becoming aware that a foot pursuit is in progress, the dispatcher is responsible for:

- (a) Clearing the radio channel of non-emergency traffic.
- (b) Coordinating pursuit communications of the involved investigators.
- (c) Broadcasting pursuit updates as well as other pertinent information as necessary.
- (d) Ensuring that a field supervisor is notified of the foot pursuit.
- (e) Notifying and coordinating with other involved or affected agencies as practicable.
- (f) Notifying the Lieutenant as soon as practicable.
- (g) Assigning an incident number and logging all pursuit activities.

#### **304.6 REPORTING REQUIREMENTS**

The initiating investigator shall complete appropriate crime/arrest reports documenting, at minimum:

- (a) Date and time of the foot pursuit.
- (b) Initial reason and circumstances surrounding the foot pursuit.
- (c) Course and approximate distance of the foot pursuit.
- (d) Alleged offenses.
- (e) Involved vehicles and investigators.
- (f) Whether a suspect was apprehended as well as the means and methods used.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Foot Pursuits*

---

1. Any use of force shall be reported and documented in compliance with the Use of Force Policy.
  - (g) Arrestee information, if applicable.
  - (h) Any injuries and/or medical treatment.
  - (i) Any property or equipment damage.
  - (j) Name of the supervisor at the scene or who handled the incident.

Assisting investigators taking an active role in the apprehension of the suspect shall complete supplemental reports as necessary or as directed.

The supervisor reviewing the report will make a preliminary determination that the pursuit appears to be in compliance with this policy or that additional review and/or follow-up is warranted.

In any case in which a suspect is not apprehended and there is insufficient information to support further investigation, a supervisor may authorize that the initiating investigator need not complete a formal report.

# Investigator Response to Calls

## 305.1 PURPOSE AND SCOPE

This policy provides for the safe and appropriate response to emergency and non-emergency situations whether dispatched or self-initiated.

## 305.2 RESPONSE TO CALLS

Investigators dispatched "Code-3" shall consider the call an emergency response and proceed immediately. Investigators responding Code-3 shall continuously operate emergency lighting equipment, including at minimum a steady forward facing red light, and shall sound the siren as reasonably necessary pursuant to Vehicle Code § 21055.

Responding with emergency light(s) and siren does not relieve the investigator of the duty to continue to drive with due regard for the safety of all persons. The use of any other warning equipment without a red light and siren does not provide any exemption from the Vehicle Code.

Investigators should only respond Code-3 when so dispatched or when circumstances reasonably indicate an emergency response is required. Investigators not authorized to respond Code-3 shall observe all traffic laws and proceed without the use of emergency lights and siren.

## 305.3 REQUESTING EMERGENCY ASSISTANCE

Requests for emergency assistance should be limited to those situations where the involved personnel reasonably believe that there is an immediate threat to the safety of investigators, or assistance is needed to prevent imminent serious harm to a citizen. In any event, where a situation has stabilized and emergency response is not required, the requesting investigator shall immediately notify SR 911.

If circumstances permit, the requesting investigator should give the following information:

- The unit number
- The location
- The reason for the request and type of emergency
- The number of units required

## 305.4 INITIATING CODE 3 RESPONSE

If an investigator believes a Code-3 response to any call is appropriate, the investigator shall immediately notify SR 911 that they are responding Code-3 and the location they are responding from. When the emergency situation has resolved or there is not immediate need to continue to respond Code-3, the investigator shall proceed without the use of emergency lights and siren and observe all traffic laws.

### *Investigator Response to Calls*

---

#### **305.5 RESPONSIBILITIES OF RESPONDING INVESTIGATORS**

Investigators shall exercise sound judgment and care with due regard for life and property when responding to an emergency call. Investigators shall reduce speed at all street intersections to such a degree that they shall have complete control of the vehicle.

The decision to continue a Code-3 response is at the discretion of the investigator. If, in the investigator's judgment, the roadway conditions or traffic congestion does not permit such a response without unreasonable risk, the investigator may elect to respond to the call without the use of red lights and siren at the legal speed limit. In such an event, the investigator should immediately notify SR 911 they are not responding Code-3. An investigator shall also discontinue the Code-3 response when directed by a supervisor.

#### **305.6 COMMUNICATIONS RESPONSIBILITIES**

A dispatcher shall assign a Code-3 response when an investigator requests emergency assistance or available information reasonably indicates that the public is threatened with serious injury or death and immediate police response is needed. The dispatcher shall:

- (a) Attempt to assign the closest available unit to the location requiring assistance
- (b) Confirm the location from which the unit is responding
- (c) Notify and coordinate allied emergency services (e.g., fire and ambulance)
- (d) Continue to obtain and broadcast information as necessary concerning the response and monitor the situation until it is stabilized or terminated
- (e) Control all radio communications during the emergency and coordinate assistance as necessary until the situation is stabilized.

#### **305.7 FAILURE OF EMERGENCY EQUIPMENT**

If the emergency equipment on the vehicle should fail to operate, the investigator must terminate the Code-3 response and respond accordingly. In all cases, the investigator shall notify the Lieutenant, field supervisor, or SR 911 of the equipment failure so that another unit may be assigned to the emergency response.

## Victim and Witness Assistance

### **306.1 PURPOSE AND SCOPE**

The purpose of this policy is to ensure that crime victims and witnesses receive appropriate assistance, that they are provided with information from government and private resources, and that the agency meets all related legal mandates.

### **306.2 POLICY**

The Stanislaus County District Attorney's Office is committed to providing guidance and assistance to the victims and witnesses of crime. The members of the Stanislaus County District Attorney's Office will show compassion and understanding for victims and witnesses and will make reasonable efforts to provide the support and information identified in this policy.

### **306.3 CRIME VICTIM LIAISON**

The Chief of Investigations shall refer victims of crime seeking assistance to the Victim Services Unit Coordinator. The Victim Services crime victim liaison will be the point of contact for individuals requiring further assistance or information from the Stanislaus County District Attorney's Office regarding benefits from crime victim resources. This person shall also be responsible for maintaining compliance with all legal mandates related to crime victims and/or witnesses.

### **306.4 CRIME VICTIMS**

Investigators should never guarantee a victim's safety from future harm but may make practical safety suggestions to victims who express fear of future harm or retaliation. Investigators should never guarantee that a person qualifies as a victim for the purpose of compensation or restitution but may direct him/her to the proper written bureau material or available victim resources.

#### **306.4.1 VICTIMS OF HUMAN TRAFFICKING**

Investigators investigating or receiving a report involving a victim of human trafficking shall inform the victim, or the victim's parent or guardian if the victim is a minor, that upon the request of the victim the names and images of the victim and his/her immediate family members may be withheld from becoming a matter of public record until the conclusion of the investigation or prosecution (Penal Code § 293).

### **306.5 WITNESSES**

Investigators should never guarantee a witness' safety from future harm or that his/her identity will always remain confidential. Investigators may make practical safety suggestions to witnesses who express fear of future harm or retaliation.

Investigators should investigate allegations of witness intimidation and take enforcement action when lawful and reasonable.

# Information Technology Use

## 307.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of bureau information technology resources, including computers, electronic devices, hardware, software and systems.

### 307.1.1 DEFINITIONS

Definitions related to this policy include:

**Computer system** - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented, or licensed by the Stanislaus County District Attorney's Office that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Bureau or bureau funding.

**Hardware** - Includes but is not limited to computers, computer terminals, network equipment, electronic devices, telephones (including cellular and satellite), modems, or any other tangible computer device generally understood to comprise hardware.

**Software** - Includes but is not limited to all computer programs, systems, and applications, including shareware and firmware. This does not include files created by the individual user.

**Temporary file, permanent file, or file** - Any electronic document, information, or data residing or located, in whole or in part, on the system including but not limited to spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs, or videos.

## 307.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Bureau in a professional manner and in accordance with this policy.

## 307.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts, or anything published, shared, transmitted, or maintained through file-sharing software or any internet site that is accessed, transmitted, received, or reviewed on any bureau computer system.

The Bureau reserves the right to access, audit, and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received, or reviewed over any technology that is issued or maintained by the Bureau, including the bureau email system, computer network, and/or any information placed into storage on any bureau system or device. This includes records of all keystrokes or Web-browsing history made at any bureau computer or over any bureau network. The fact that access to a database, service, or website requires a username or password will not create an expectation of privacy if it is accessed through bureau computers, electronic devices, or networks.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Information Technology Use*

---

The Bureau shall not require a member to disclose a personal username or password for accessing personal social media or to open a personal social website; however, the Bureau may request access when it is reasonably believed to be relevant to the investigation of allegations of work-related misconduct (Labor Code § 980).

#### **307.4 RESTRICTED USE**

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to their supervisors or Lieutenants.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

##### **307.4.1 SOFTWARE**

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any bureau computer. Members shall not install personal copies of any software onto any bureau computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the information systems technology (IT) staff and with the authorization of the Chief of Investigations or the authorized designee.

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Bureau while on bureau premises, computer systems or electronic devices. Such unauthorized use of software exposes the Bureau and involved members to severe civil and criminal penalties.

Introduction of software by members should only occur as part of the automated maintenance or update process of bureau- or County-approved or installed programs by the original manufacturer, producer or developer of the software.

Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

##### **307.4.2 HARDWARE**

Access to technology resources provided by or through the Bureau shall be strictly limited to bureau-related activities. Data stored on or available through bureau computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or bureau-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Information Technology Use*

---

#### **307.4.3 INTERNET USE**

Internet access provided by or through the Bureau shall be strictly limited to bureau-related activities. Internet sites containing information that is not appropriate or applicable to bureau use and which shall not be intentionally accessed include but are not limited to adult forums, pornography, gambling, chat rooms, and similar or related internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member's assignment.

Downloaded information from the internet shall be limited to messages, mail, and data files.

#### **307.5 PROTECTION OF AGENCY SYSTEMS AND FILES**

All members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care, and maintenance of the computer system.

Members shall ensure bureau computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, logon information, and other individual security data, protocols, and procedures are confidential information and are not to be shared. Password length, format, structure, and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the internet) to a supervisor.

#### **307.6 INSPECTION OR REVIEW**

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Bureau involving one of its members or a member's duties, an alleged or suspected violation of any bureau policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the bureau computer system when requested by a supervisor or during the course of regular duties that require such information.



## Registered Offender Information

### 308.1 PURPOSE AND SCOPE

This policy establishes guidelines by which the Stanislaus County District Attorney's Office will address issues associated with certain offenders who are residing in the jurisdiction and how the Bureau will disseminate information and respond to public inquiries for information about registered sex, arson and drug offenders.

### 308.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to identify and monitor registered offenders living within this jurisdiction and to take reasonable steps to address the risks those persons may pose.

### 308.3 REGISTRATION

The Investigative Bureau supervisor shall establish a process to reasonably accommodate registration of certain offenders. The process should rebut any allegation on the part of the offender that the registration process was too confusing, burdensome, or difficult for compliance. If it is reasonable to do so, an investigator assigned to related investigations should conduct the registration in order to best evaluate any threat the person may pose to the community. Those assigned to register offenders should receive appropriate training regarding the registration process.

Upon conclusion of the registration process, the investigator shall ensure that the registration information is provided to the California Department of Justice (DOJ) in accordance with applicable law (Penal Code § 457.1; Penal Code § 290 et seq.).

The refusal of a registrant to provide any of the required information or complete the process should initiate a criminal investigation for failure to register.

#### 308.3.1 CONTENTS OF REGISTRATION

The information collected from the registering offenders shall include a signed statement as required by the California DOJ, fingerprints and a photograph, and any other information required by applicable law (Penal Code § 457.1; Penal Code § 290 et seq.).

### 308.4 MONITORING OF REGISTERED OFFENDERS

The Investigative Bureau supervisor should establish a system to periodically, and at least once annually, verify that a registrant remains in compliance with his/her registration requirements after the initial registration. This verification should include:

- (a) Efforts to confirm residence using an unobtrusive method, such as an internet search or drive-by of the declared residence.
- (b) Review of information on the California DOJ website for sex offenders.
- (c) Contact with a registrant's parole or probation officer.

Any discrepancies should be reported to the California DOJ.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Registered Offender Information*

---

The Investigative Bureau supervisor should also establish a procedure to routinely disseminate information regarding registered offenders to Stanislaus County District Attorney's Office personnel, including timely updates regarding new or relocated registrants.

#### **308.5 DISSEMINATION OF PUBLIC INFORMATION**

Members will not unilaterally make a public notification advising the community of a particular registrant's presence in the community. Members who identify a significant risk or other public safety issue associated with a registrant should promptly advise their supervisor. The supervisor should evaluate the request and forward the information to the Chief of Investigations if warranted. A determination will be made by the Chief of Investigations, with the assistance of legal counsel as necessary, whether such a public alert should be made.

Members of the public requesting information on sex registrants should be provided the Megan's Law website or the Stanislaus County District Attorney's Office's website. Information on sex registrants placed on the Stanislaus County District Attorney's Office's website shall comply with the requirements of Penal Code § 290.46.

The Records Manager may release local registered offender information to residents only in accordance with applicable law and in compliance with a California Public Records Act request (Government Code § 7920.000 et seq.; Penal Code § 290.45; Penal Code § 290.46; Penal Code § 457.1).

##### **308.5.1 LIMITED RELEASE WITHIN COLLEGE CAMPUS COMMUNITY**

California law allows the following additional information regarding a registered sex offender on campus, whose information is not available to the public via the internet website, to be released to a campus community (Penal Code § 290.01(d)):

- (a) The offender's full name
- (b) The offender's known aliases
- (c) The offender's sex
- (d) The offender's race
- (e) The offender's physical description
- (f) The offender's photograph
- (g) The offender's date of birth
- (h) Crimes resulting in the registration of the offender under Penal Code § 290
- (i) The date of last registration

For purposes of this section, campus community shall be defined as those persons present at or regularly frequenting any place constituting campus property, satellite facilities, laboratories, public areas contiguous to the campus and other areas set forth in Penal Code § 290.01(d).

##### **308.5.2 RELEASE NOTIFICATIONS**

Registrant information that is released should include notification that:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Registered Offender Information*

---

- (a) The offender registry includes only those persons who have been required by law to register and who are in compliance with the offender registration laws.
- (b) The information is provided as a public service and may not be current or accurate.
- (c) Persons should not rely solely on the offender registry as a safeguard against offenses in their communities.
- (d) The crime for which a person is convicted may not accurately reflect the level of risk.
- (e) Anyone who uses information contained in the registry to harass registrants or commit any crime may be subject to criminal prosecution.
- (f) The purpose of the release of information is to allow members of the public to protect themselves and their children from sex offenders (Penal Code 290.45).

## Private Persons Arrests

### 309.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the handling of private person's arrests made pursuant to Penal Code § 837.

### 309.2 ADVISING PRIVATE PERSONS OF THE ARREST PROCESS

Penal Code § 836(b) expressly mandates that all investigators shall advise victims of domestic violence of the right to make a private person's arrest, including advice on how to safely execute such an arrest. In all other situations, investigators should use sound discretion in determining whether or not to advise an individual of the arrest process.

- (a) When advising any individual regarding the right to make a private person's arrest, investigators should refrain from encouraging or dissuading any individual from making such an arrest and should instead limit advice to the legal requirements for such an arrest as listed below.
- (b) Private individuals should be discouraged from using force to effect a private person's arrest, and absent immediate threat to their own safety or the safety of others, private individuals should be encouraged to refer matters to law enforcement officials for further investigation or arrest.

### 309.3 ARRESTS BY PRIVATE PERSONS

Penal Code § 837 provides that a private person may arrest another:

- (a) For a public offense committed or attempted in his or her presence;
- (b) When the person arrested has committed a felony, although not in his or her presence;
- (c) When a felony has been in fact committed, and he or she has reasonable cause for believing the person arrested has committed it.

Unlike peace officers, private persons may not make an arrest on suspicion that a felony has been committed - the felony must in fact have taken place.

### 309.4 INVESTIGATOR RESPONSIBILITIES

Any investigator presented with a private person wishing to make an arrest must determine whether or not there is reasonable cause to believe that such an arrest would be lawful (Penal Code § 847).

- (a) Should any investigator determine that there is no reasonable cause to believe that a private person's arrest is lawful, the investigator should take no action to further detain or restrain the individual beyond that which reasonably appears necessary to investigate the matter, determine the lawfulness of the arrest and protect the public safety.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Private Persons Arrests*

---

1. Any investigator who determines that a private person's arrest appears to be unlawful should promptly release the arrested individual pursuant to Penal Code § 849(b)(1). The investigator must include the basis of such a determination in a related report.
  2. Absent reasonable cause to support a private person's arrest or other lawful grounds to support an independent arrest by the investigator, the investigator should advise the parties that no arrest will be made and that the circumstances will be documented in a related report.
- (b) Whenever an investigator determines that there is reasonable cause to believe that a private person's arrest is lawful, the investigator may exercise any of the following options:
1. Take the individual into physical custody for booking
  2. Release the individual pursuant to a Notice to Appear
  3. Release the individual pursuant to Penal Code § 849

## Limited English Proficiency Services

### 310.1 PURPOSE AND SCOPE

This policy provides guidance to members when communicating with individuals with limited English proficiency (LEP) (42 USC § 2000d).

#### 310.1.1 DEFINITIONS

Definitions related to this policy include:

**Authorized interpreter** - A person who has been screened and authorized by the Bureau to act as an interpreter and/or translator for others.

**Interpret or interpretation** - The act of listening to a communication in one language (source language) and orally converting it to another language (target language), while retaining the same meaning.

**Limited English proficient (LEP)** - Any individual whose primary language is not English and who has a limited ability to read, write, speak or understand English. These individuals may be competent in certain types of communication (e.g., speaking or understanding) but still be LEP for other purposes (e.g., reading or writing). Similarly, LEP designations are context-specific; an individual may possess sufficient English language skills to function in one setting but these skills may be insufficient in other situations.

**Qualified bilingual member** - A member of the Stanislaus County District Attorney's Office, who has the ability to communicate fluently, directly and accurately in both English and another language. Bilingual members may be fluent enough to communicate in a non-English language but may not be sufficiently fluent to interpret or translate from one language into another.

**Translate or translation** - The replacement of written text from one language (source language) into an equivalent written text (target language).

### 310.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to reasonably ensure that LEP individuals have meaningful access to law enforcement services, programs and activities, while not imposing undue burdens on its members.

The Bureau will not discriminate against or deny any individual access to services, rights or programs based upon national origin or any other protected interest or right.

### 310.3 TYPES OF LEP ASSISTANCE AVAILABLE

Stanislaus County District Attorney's Office members should never refuse service to an LEP individual who is requesting assistance, nor should they require an LEP individual to furnish an interpreter as a condition for receiving assistance. The Bureau will make every reasonable effort to provide meaningful and timely assistance to LEP individuals through a variety of services.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Limited English Proficiency Services*

---

The Bureau will utilize all reasonably available tools, such as language identification cards, when attempting to determine an LEP individual's primary language.

LEP individuals may choose to accept bureau-provided LEP services at no cost or they may choose to provide their own.

Bureau-provided LEP services may include, but are not limited to, the assistance methods described in this policy.

#### **310.4 QUALIFIED BILINGUAL MEMBERS**

Bilingual members may be qualified to provide LEP services when they have demonstrated through established bureau procedures a sufficient level of skill and competence to fluently communicate in both English and a non-English language. Members utilized for LEP services must demonstrate knowledge of the functions of an interpreter/translator and the ethical issues involved when acting as a language conduit. Additionally, bilingual members must be able to communicate technical and law enforcement terminology, and be sufficiently proficient in the non-English language to perform complicated tasks, such as conducting interrogations, taking statements, collecting evidence or conveying rights or responsibilities.

When a qualified bilingual member from this bureau is not available, personnel from other County departments, who have been identified by the Bureau as having the requisite skills and competence, may be requested.

#### **310.5 AUTHORIZED INTERPRETERS**

Any person designated by the Bureau to act as an authorized interpreter and/or translator must have demonstrated competence in both English and the involved non-English language, must have an understanding of the functions of an interpreter that allows for correct and effective translation, and should not be a person with an interest in the bureau case or investigation involving the LEP individual. A person providing interpretation or translation services may be required to establish the accuracy and trustworthiness of the interpretation or translation in a court proceeding.

##### **310.5.1 SOURCES OF AUTHORIZED INTERPRETERS**

The Bureau may contract with authorized interpreters who are available over the telephone. Members may use these services with the approval of a supervisor and in compliance with established procedures.

Other sources may include:

- Qualified bilingual members of this bureau or personnel from other County departments.
- Individuals employed exclusively to perform interpretation services.
- Contracted in-person interpreters, such as state or federal court interpreters, among others.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Limited English Proficiency Services*

---

- Interpreters from other agencies who have been qualified as interpreters by this bureau, and with whom the Bureau has a resource-sharing or other arrangement that they will interpret according to bureau guidelines.

#### **310.5.2 COMMUNITY VOLUNTEERS AND OTHER SOURCES OF LANGUAGE ASSISTANCE**

Language assistance may be available from community volunteers who have demonstrated competence in either monolingual (direct) communication and/or in interpretation or translation (as noted in above), and have been approved by the Bureau to communicate with LEP individuals.

Where qualified bilingual members or other authorized interpreters are unavailable to assist, approved community volunteers who have demonstrated competence may be called upon when appropriate. However, bureau members must carefully consider the nature of the contact and the relationship between the LEP individual and the volunteer to ensure that the volunteer can provide neutral and unbiased assistance.

While family or friends of an LEP individual may offer to assist with communication or interpretation, members should carefully consider the circumstances before relying on such individuals. For example, children should not be relied upon except in exigent or very informal and non-confrontational situations.

#### **310.6 CONTACT AND REPORTING**

While all law enforcement contacts, services and individual rights are important, this bureau will utilize the four-factor analysis to prioritize service to LEP individuals so that such services may be targeted where they are most needed, according to the nature and importance of the particular law enforcement activity involved.

Whenever any member of this bureau is required to complete a report or other documentation, and interpretation services are provided to any involved LEP individual, such services should be noted in the related report. Members should document the type of interpretation services utilized and whether the individual elected to use services provided by the Bureau or some other identified source.

#### **310.7 FIELD ENFORCEMENT**

Field enforcement will generally include such contacts as traffic stops, pedestrian stops, serving warrants and restraining orders, crowd/traffic control and other routine field contacts that may involve LEP individuals. The scope and nature of these activities and contacts will inevitably vary. Members and/or supervisors must assess each situation to determine the need and availability of language assistance to all involved LEP individuals and utilize the methods outlined in this policy to provide such assistance.

Although not every situation can be addressed in this policy, it is important that members are able to effectively communicate the reason for a contact, the need for information and the meaning or consequences of any enforcement action. For example, it would be meaningless to request consent to search if the investigator is unable to effectively communicate with an LEP individual.



### *Limited English Proficiency Services*

---

If available, investigators should obtain the assistance of a qualified bilingual member or an authorized interpreter before placing an LEP individual under arrest.

#### **310.8 INVESTIGATIVE FIELD INTERVIEWS**

In any situation where an interview may reveal information that could be used as the basis for arrest or prosecution of an LEP individual and a qualified bilingual member is unavailable or lacks the skills to directly communicate with the LEP individual, an authorized interpreter should be used. This includes interviews conducted during an investigation with victims, witnesses and suspects. In such situations, audio recordings of the interviews should be made when reasonably possible. Identification and contact information for the interpreter (e.g., name, address) should be documented so that the person can be subpoenaed for trial if necessary.

If an authorized interpreter is needed, investigators should consider calling for an authorized interpreter in the following order:

- An authorized bureau member or allied agency interpreter
- An authorized telephone interpreter
- Any other authorized interpreter

Any *Miranda* warnings shall be provided to suspects in their primary language by an authorized interpreter or, if the suspect is literate, by providing a translated *Miranda* warning card.

The use of an LEP individual's bilingual friends, family members, children, neighbors or bystanders may be used only when a qualified bilingual member or authorized interpreter is unavailable and there is an immediate need to interview an LEP individual.

#### **310.9 CUSTODIAL INTERROGATIONS**

Miscommunication during custodial interrogations may have a substantial impact on the evidence presented in a criminal prosecution. Only qualified bilingual members or, if none is available or appropriate, authorized interpreters shall be used during custodial interrogations. *Miranda* warnings shall be provided to suspects in their primary language by the qualified bilingual member or an authorized interpreter.

In order to ensure that translations during custodial interrogations are accurately documented and are admissible as evidence, interrogations should be recorded whenever reasonably possible. See guidance on recording custodial interrogations in the Investigation and Prosecution Policy.

#### **310.10 BOOKINGS**

When gathering information during the booking process, members should remain alert to the impediments that language barriers can create. In the interest of the arrestee's health and welfare, the safety and security of the facility, and to protect individual rights, it is important that accurate medical screening and booking information be obtained. Members should seek the assistance of a qualified bilingual member whenever there is concern that accurate information cannot be obtained or that booking instructions may not be properly understood by an LEP individual.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Limited English Proficiency Services*

---

#### **310.11 COMPLAINTS**

The Bureau shall ensure that LEP individuals who wish to file a complaint regarding members of this bureau are able to do so. The Bureau may provide an authorized interpreter or translated forms, as appropriate.

Investigations into such complaints shall be handled in accordance with the Personnel Complaints Policy. Authorized interpreters used for any interview with an LEP individual during an investigation should not be members of this bureau.

Any notice required to be sent to an LEP individual as a complaining party pursuant to the Personnel Complaints Policy should be translated or otherwise communicated in a language-accessible manner.

#### **310.12 TRAINING**

To ensure that all members who may have contact with LEP individuals are properly trained, the Bureau will provide periodic training on this policy and related procedures, including how to access bureau-authorized interpreters and other available resources.

# Mandatory Employer Notification

## 311.1 PURPOSE AND SCOPE

The purpose of this policy is to describe the requirements and procedures to follow when a public or private school employee (teacher and non-teacher) has been arrested under certain circumstances.

## 311.2 POLICY

When an arrest is made by a sworn member of the Bureau of Investigation, the bureau will meet the reporting requirements of California law to minimize the risks to children and others.

## 311.3 MANDATORY SCHOOL EMPLOYEE ARREST REPORTING

In the event a school employee is arrested for any offense enumerated below, the Chief of Investigations or his/her designee is required to report the arrest as follows.

### 311.3.1 ARREST OF PUBLIC SCHOOL TEACHER

In the event a public school teacher is arrested for any controlled substance offense enumerated in Health and Safety Code § 11591 or Health and Safety Code § 11364, in so far as that section relates to Health and Safety Code § 11054(d)(12), or for any of the offenses enumerated in Penal Code § 290, Penal Code § 261(a), or Education Code § 44010, the Chief of Investigations or his/her designee is mandated to immediately notify by telephone the superintendent of the school district employing the teacher and to immediately give written notice of the arrest to the Commission on Teacher Credentialing and to the superintendent of schools in the county where the person is employed (Health and Safety Code § 11591; Penal Code § 291).

### 311.3.2 ARREST OF PUBLIC SCHOOL NON-TEACHER EMPLOYEE

In the event a public school non-teacher employee is arrested for any controlled substance offense enumerated in Health and Safety Code § 11591 or Health and Safety Code § 11364, in so far as that section relates to Health and Safety Code § 11054(d)(12), or for any of the offenses enumerated in Penal Code § 290, Penal Code § 261(a), or Education Code § 44010, the Chief of Investigations or his/her designee is mandated to immediately notify by telephone the superintendent of the school district employing the non-teacher and to immediately give written notice of the arrest to the governing board of the school district employing the person (Health and Safety Code § 11591; Penal Code § 291).

### 311.3.3 ARREST OF PRIVATE SCHOOL TEACHER

In the event a private school teacher is arrested for any controlled substance offense enumerated in Health and Safety Code § 11591 or Health and Safety Code § 11364, in so far as that section relates to Health and Safety Code § 11054(d)(12), or for any of the offenses enumerated in Penal Code § 290 or Education Code § 44010, the Chief of Investigations or his/her designee is mandated to immediately notify by telephone the private school authority employing the teacher and to immediately give written notice of the arrest to the private school authority employing the teacher (Health and Safety Code § 11591; Penal Code § 291.1).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Mandatory Employer Notification*

---

#### **311.3.4 ARREST OF COMMUNITY COLLEGE INSTRUCTOR**

In the event a teacher or instructor employed in a community college district school is arrested for any controlled substance offense enumerated in Health and Safety Code § 11591.5 or Health and Safety § 11364, in so far as that section relates to Health and Safety Code § 11054(d)(9), or for any of the offenses enumerated in Penal Code § 290 or in Penal Code § 261(a)(1), the Chief of Investigations or the authorized designee is mandated to immediately notify by telephone the superintendent of the community college district employing the person, and shall immediately give written notice of the arrest to the California Community Colleges Chancellor's Office (Health and Safety Code § 11591.5; Penal Code § 291.5).

#### **311.4 ARREST OF PERSONS EMPLOYED IN COMMUNITY CARE FACILITIES**

In the event an employee of a community treatment facility, a day treatment facility, a group home, a short-term residential therapeutic program or a foster family agency is arrested for child abuse (as defined in Penal Code § 11165.6) and the employee is free to return to work where children are present, the investigating member shall notify the licensee of the charge of abuse (Health and Safety Code § 1522.2).

## Child and Dependent Adult Safety

### 312.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure that children and dependent adults are not left without appropriate care in the event their caregiver or guardian is arrested or otherwise prevented from providing care due to actions taken by members of this bureau (Penal Code § 833.2(a)).

This policy does not address the actions to be taken during the course of a child abuse or dependent adult investigation. These are covered in the Child Abuse and Senior and Disability Victimization policies.

### 312.2 POLICY

It is the policy of this bureau to mitigate, to the extent reasonably possible, the stressful experience individuals may have when their parent or caregiver is arrested. The Stanislaus County District Attorney's Office will endeavor to create a strong, cooperative relationship with local, state and community-based social services to ensure an effective, collaborative response that addresses the needs of those affected, including call-out availability and follow-up responsibilities.

### 312.3 PROCEDURES DURING AN ARREST

When encountering an arrest or prolonged detention situation, investigators should make reasonable attempts to determine if the arrestee is responsible for children or dependent adults. In some cases this may be obvious, such as when children or dependent adults are present. However, investigators should inquire if the arrestee has caregiver responsibilities for any children or dependent adults who are without appropriate supervision. The following steps should be taken (Penal Code § 13517.7(b)(1)):

- (a) Inquire about and confirm the location of any children or dependent adults.
- (b) Look for evidence of children and dependent adults. Investigators should be mindful that some arrestees may conceal the fact that they have a dependent for fear the individual may be taken from them.
- (c) Consider inquiring of witnesses, neighbors, friends and relatives of the arrestee as to whether the person is responsible for a child or dependent adult.

Whenever reasonably possible, investigators should take reasonable steps to accomplish the arrest of a parent, guardian or caregiver out of the presence of his/her child or dependent adult. Removing children or dependent adults from the scene in advance of the arrest will generally ensure the best outcome for the individual.

Whenever it is safe to do so, investigators should allow the parent or caregiver to assure children or dependent adults that they will be provided care. If this is not safe or if the demeanor of the parent or caregiver suggests this conversation would be non-productive, the investigator at the scene should explain the reason for the arrest in age-appropriate language and offer reassurance to the child or dependent adult that he/she will receive appropriate care.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Child and Dependent Adult Safety*

---

#### 312.3.1 AFTER AN ARREST

Whenever an arrest is made, the investigator should take all reasonable steps to ensure the safety of the arrestee's disclosed or discovered children or dependent adults.

Investigators should allow the arrestee reasonable time to arrange for care of children and dependent adults. Temporary placement with family or friends may be appropriate. However, any decision should give priority to a care solution that is in the best interest of the child or dependent adult. In such cases the following guidelines should be followed:

- (a) Allow the person reasonable time to arrange for the care of children and dependent adults with a responsible party, as appropriate.
  - 1. Investigators should consider allowing the person to use his/her cell phone to facilitate arrangements through access to contact phone numbers, and to lessen the likelihood of call screening by the recipients due to calls from unknown sources.
- (b) Unless there is evidence to the contrary (e.g., signs of abuse, drug use, unsafe environment), investigators should respect the parent or caregiver's judgment regarding arrangements for care. It is generally best if the child or dependent adult remains with relatives or family friends that he/she knows and trusts because familiarity with surroundings and consideration for comfort, emotional state and safety are important.
  - 1. Except when a court order exists limiting contact, the investigator should attempt to locate and place children or dependent adults with the non-arrested parent, guardian or caregiver.
- (c) Provide for the immediate supervision of children or dependent adults until an appropriate caregiver arrives.
- (d) Notify Child Protective Services or the Division of Aging and Adult Services, if appropriate.
- (e) Notify the field supervisor or Lieutenant of the disposition of children or dependent adults.

If children or dependent adults are at school or another known location outside the household at the time of arrest, the arresting investigator should attempt to contact the school or other known location and inform the principal or appropriate responsible adult of the caregiver's arrest and of the arrangements being made for the care of the arrestee's dependent. The result of such actions should be documented in the associated report.

#### 312.3.2 DURING THE BOOKING PROCESS

During the booking process the arrestee shall be allowed to make additional telephone calls to relatives or other responsible individuals as is reasonably necessary to arrange for the care of any child or dependent adult. These telephone calls should be given as soon as practicable and are in addition to any other telephone calls allowed by law (Penal Code § 851.5(c)).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Child and Dependent Adult Safety*

---

If an arrestee is unable to resolve the care of any child or dependent adult through this process, a supervisor should be contacted to determine the appropriate steps to arrange for care. These steps may include additional telephone calls or contacting a local, county or state services agency.

#### 312.3.3 REPORTING

- (a) For all arrests where children are present or living in the household, the reporting member will document the following information:
  - 1. Name
  - 2. Sex
  - 3. Age
  - 4. Special needs (e.g., medical, mental health)
  - 5. How, where and with whom or which agency the child was placed
  - 6. Identities and contact information for other potential caregivers
  - 7. Notifications made to other adults (e.g., schools, relatives)
- (b) For all arrests where dependent adults are present or living in the household, the reporting member will document the following information:
  - 1. Name
  - 2. Sex
  - 3. Age
  - 4. Whether he/she reasonably appears able to care for him/herself
  - 5. Disposition or placement information if he/she is unable to care for him/herself

#### 312.3.4 SUPPORT AND COUNSELING REFERRAL

If, in the judgment of the handling investigators, the child or dependent adult would benefit from additional assistance, such as counseling services, contact with a victim advocate or a crisis telephone number, the appropriate referral information may be provided.

#### **312.4 DEPENDENT WELFARE SERVICES**

Whenever an arrestee is unwilling or incapable of arranging for the appropriate care of any child or dependent adult, the handling investigator should contact the appropriate welfare service or other department-approved social service to determine whether protective custody is appropriate (Welfare and Institutions Code § 305).

Only when other reasonable options are exhausted should a child or dependent adult be transported to the investigator facility, transported in a marked patrol car, or taken into formal protective custody.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Child and Dependent Adult Safety*

---

Under no circumstances should a child or dependent adult be left unattended or without appropriate care.

#### **312.5 TRAINING**

The Lieutenant is responsible to ensure that all personnel of this bureau who may be involved in arrests affecting children or dependent adults receive approved POST-approved training on effective safety measures when a parent, guardian or caregiver is arrested (Penal Code § 13517.7).



## Off-Duty Law Enforcement Actions

### 313.1 PURPOSE AND SCOPE

The decision to become involved in a law enforcement action when off-duty can place an investigator as well as others at great risk and must be done with careful consideration. This policy is intended to provide guidelines for investigators of the Stanislaus County District Attorney's Office with respect to taking law enforcement action while off-duty.

### 313.2 POLICY

Initiating law enforcement action while off-duty is generally discouraged. Investigators should not attempt to initiate enforcement action when witnessing minor crimes, such as suspected intoxicated drivers, reckless driving or minor property crimes. Such incidents should be promptly reported to the appropriate law enforcement agency.

Investigators are not expected to place themselves in unreasonable peril. However, any sworn member of this bureau who becomes aware of an incident or circumstance that he/she reasonably believes poses an imminent threat of serious bodily injury or death, or significant property damage may take reasonable action to minimize the threat.

When public safety or the prevention of major property damage requires immediate action, investigators should first consider reporting and monitoring the activity and only take direct action as a last resort.

### 313.3 FIREARMS

Investigators of this bureau may carry firearms while off-duty in accordance with federal regulations and bureau policy. All firearms and ammunition must meet guidelines as described in the bureau Firearms Policy. When carrying firearms while off-duty investigators shall also carry their bureau-issued badge and identification.

Investigators should refrain from carrying firearms when the consumption of alcohol is likely or when the need to carry a firearm is outweighed by safety considerations. Firearms shall not be carried by any investigator who has consumed an amount of an alcoholic beverage or taken any drugs or medications or any combination thereof that would tend to adversely affect the investigator's senses or judgment.

### 313.4 DECISION TO INTERVENE

There is no legal requirement for off-duty investigators to take law enforcement action. However, should investigators decide to intervene, they must evaluate whether the action is necessary or desirable, and should take into consideration the following:

- (a) The tactical disadvantage of being alone and the fact there may be multiple or hidden suspects.
- (b) The inability to communicate with responding units.
- (c) The lack of equipment, such as handcuffs, OC or baton.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Off-Duty Law Enforcement Actions*

---

- (d) The lack of cover.
- (e) The potential for increased risk to bystanders if the off-duty investigator were to intervene.
- (f) Unfamiliarity with the surroundings.
- (g) The potential for the off-duty investigator to be misidentified by other peace officers or members of the public.

Investigators should consider waiting for on-duty uniformed investigators to arrive, and gather as much accurate intelligence as possible instead of immediately intervening.

#### **313.4.1 INTERVENTION PROCEDURE**

If involvement is reasonably necessary the investigator should attempt to call or have someone else call 9-1-1 to request immediate assistance. The dispatcher should be informed that an off-duty investigator is on-scene and should be provided a description of the officer if possible.

Whenever practicable, the investigator should loudly and repeatedly identify him/herself as a peace officer until acknowledged. Official identification should also be displayed.

#### **313.4.2 INCIDENTS OF PERSONAL INTEREST**

Investigators should refrain from handling incidents of personal interest, (e.g., family or neighbor disputes) and should remain neutral. In such circumstances investigators should call the responsible agency to handle the matter.

#### **313.4.3 OTHER CONSIDERATIONS**

When encountering a non-uniformed investigator in public, uniformed investigators should wait for acknowledgement by the non-uniformed investigator in case he/she needs to maintain an undercover capability.

### **313.5 REPORTING**

Any off-duty investigator who engages in any law enforcement activity, regardless of jurisdiction, shall notify the Lieutenant as soon as practicable. The Lieutenant shall determine whether a report should be filed by the employee.

Investigators should cooperate fully with the agency having jurisdiction in providing statements or reports as requested or as appropriate.

# **Bureau of Investigation and Victim Services Unit Mass Victimization Partnership and Response Plan**

## **314.1 PURPOSE**

To outline the process by which the District Attorney's Victim Services Crisis Response Team (CRT) and the Bureau of Investigation (Bureau) can coordinate a response during a crime-related mass victimization incident. CRT Advocates will be deployed, as directed per protocol, to provide secondary response to crime-related mass victimization incidents. Documented partnership between the Victim Services Unit and the Bureau of Investigation will facilitate CRT access to secured locations following mass victimization incidents and will incorporate safety precautions for deployed CRT Advocates.

## **314.2 ORGANIZATION**

1. The Victim Services Unit CRT will respond after a mass victimization incident when directed by the District Attorney and the Victim Services Program Manager.
2. Upon approval, the Victim Services Program Manager will contact the Bureau of Investigation Chief, or designee, to notify that the CRT has been activated and will deploy Advocates to provide secondary response services to victims and witnesses.
3. At the direction of the Victim Services Program Manager and the Bureau of Investigation Chief, or designee, deployment of DA Investigators and CRT Advocates will be coordinated and a designated meeting place will be identified.
4. CRT Advocates and DA Investigators will travel together from the meeting location to the incident location/incident command and will return together.
5. The Victim Services Unit and the Bureau will designate a CRT Advocate and a DA Investigator to act as Leads throughout the deployment and will be responsible for communication flow while on site. The Victim Services Program Manager will maintain communication with the Bureau of Investigation Chief, or designee, throughout the deployment.

## **314.3 RESPONSIBILITIES**

1. CRT advocates and DA Investigators will review and understand the Mass Victimization Partnership and Response Plan.
2. CRT Advocates will receive training on basic incident command structure as provided by FEMA through their online ICS Resource Center, Baseline Training Courses (<https://training.fema.gov/emiweb/is/icsresource/index.htm>).
3. DA Investigators will escort CRT Advocates through secured perimeters and into the Information & Notification Center. This center is a temporary site and is typically operational for the first 24 to 48 hours following an incident.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Bureau of Investigation and Victim Services Unit Mass Victimization Partnership and Response Plan*

---

4. The Lead DA Investigator will assist the Lead CRT Advocate in locating the appropriate Official in charge and will assist in facilitating communication within the Incident Command Structure.
5. If it is not clear whether the mass victimization is crime related, DA Investigators will assist CRT Advocates in obtaining information as to whether the mass victimization incident is being investigated/classified as crime-related in order to support the use of the Victim Services Unit and the California Victim Compensation Board (CalVCB) funds which are designated for victims of crime.
6. The Lead CRT Advocate will explain to the Official in charge what services will be provided by the CRT and will obtain instructions on what areas within the Information & Notification Center the CRT and Bureau Team can access/work.
7. The Lead CRT Advocate will meet with the leaders of the other on-site crisis response agencies offering services to victims and families to determine what tasks each agency will perform and how to coordinate efforts.
8. DA Investigators will help to ensure safety of CRT Advocates while deployed at the Information & Notification Center and will facilitate ongoing communication within the incident command structure for the Lead CRT Advocate.
9. The Lead CRT Advocate will check in with the Lead DA Investigator hourly and will be responsible for relaying relevant updates to the Victim Services Program Manager who will communicate with the Bureau of Investigation Chief or designee.
10. Following a crime-related mass victimization incident, the Victim Services Unit CRT will provide ongoing support services when/if a Family Assistance Center is established and will continue to mutually coordinate a response with the Bureau if needed.

## Drop Charges Request

### **315.1 PURPOSE**

The purpose of this policy is to establish a procedure for office personnel to follow when a victim walks into the District Attorney's Office and requests to drop charges or not pursue prosecution.

### **315.2 PROCEDURE**

When a victim walks into the District Attorney's Office lobby and requests to drop charges or not pursue criminal prosecution, the following steps will be taken by agency personnel:

#### **First Floor lobby security:**

First floor lobby security will advise the victim they will need to fill out a form and provide some type of identification. Security will then refer the victim to Communications on the 3rd floor and advise Communications someone is here to fill out a drop charges form.

#### **Communications:**

Communications will ask the victim what type of case they are requesting charges to be dropped and the case number. For example: Domestic Violence, Battery, Auto Theft, etc. Communications will look up the case in ICJIS. If we have not issued the case, the victim will be told there is not an active case to drop and they need to wait until after an issuing decision has been made by our office. If there is an open case we have issued, Communications will provide the victim with a Request to Drop Charges Form and ask them to have a seat and fill it out. Once completed, Communications will take the completed form from the victim, ask to see some type of identification (driver's license, ID card), make a copy of the ID, and attach it to the Request to Drop Charges Form. If the victim does not have identification, Communications will accept the drop charges form without it, and will advise the victim that an Investigator may be contacting them to follow up on their request. Communications will then deliver the forms to a Lieutenant in Investigations to review.

#### **Investigator Assigned:**

If an Investigator is assigned for follow up, they will obtain a statement from the victim by going over the the Request to Drop Charges Form and confirm why they want to drop charges. The Investigator will then write a supplemental report and attach the Request to Drop Charges form to their supplemental report. Both the Investigators report and Request to Drop Form will be uploaded into the Records Management System (RMS).

#### **Victim Services Unit:**

# Stanislaus County District Attorney's Office

## Policy Manual

### *Drop Charges Request*

---

If a victim is meeting with anyone from the Victim Services Unit at the office and requests to drop charges, VSU will refer the victim to Communications and provide Communications with the case number. Communications will then take the steps outlined above.

If the victim says they want to drop charges over the phone, and the victim is not calling from the first-floor lobby of the DA's office, VSU will input notes in the RMS and advise the assigned DDA and an investigations supervisor. If there is no DDA assigned to the case, VSU will input notes in RMS and advise an Investigations supervisor.

If the victim is calling from the first-floor lobby phone of the DA's office, VSU will refer the victim to Communications and provide Communications with the case number. Communications will then take the steps outlined above.

## Bias-Based Policing

### 316.1 PURPOSE AND SCOPE

This policy provides guidance to bureau members that affirms the Stanislaus County District Attorney's Office's commitment to policing that is fair and objective.

Nothing in this policy prohibits the use of specified characteristics in law enforcement activities designed to strengthen the bureau's relationship with its diverse communities (e.g., cultural and ethnicity awareness training, youth programs, community group outreach, partnerships).

#### 316.1.1 DEFINITIONS

Definitions related to this policy include:

**Bias-based policing or improper profiling** - An inappropriate reliance on actual or perceived characteristics such as race, ethnicity, national origin (including limited English proficiency), religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, disability, or affiliation with any non-criminal group (protected characteristics) as the basis for providing differing law enforcement service or enforcement (Penal Code § 13519.4). This includes explicit and implicit biases (i.e., conscious and unconscious beliefs or attitudes towards certain groups).

### 316.2 POLICY

The Stanislaus County District Attorney's Office is committed to providing law enforcement services to the community with due regard for the racial, cultural or other differences of those served. It is the policy of this bureau to provide law enforcement services and to enforce the law equally, fairly, objectively and without discrimination toward any individual or group.

### 316.3 BIAS-BASED POLICING PROHIBITED

Bias-based policing is strictly prohibited.

However, nothing in this policy is intended to prohibit an investigator from considering protected characteristics in combination with credible, timely and distinct information connecting a person or people of a specific characteristic to a specific unlawful incident, or to specific unlawful incidents, specific criminal patterns or specific schemes.

#### 316.3.1 CALIFORNIA RELIGIOUS FREEDOM ACT

Members shall not collect information from a person based on religious belief, practice, affiliation, national origin or ethnicity unless permitted under state or federal law (Government Code § 8310.3).

Members shall not assist federal government authorities (Government Code § 8310.3):

- (a) In compiling personal information about a person's religious belief, practice, affiliation, national origin or ethnicity.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Bias-Based Policing*

---

- (b) By investigating, enforcing or assisting with the investigation or enforcement of any requirement that a person register with the federal government based on religious belief, practice, or affiliation, or national origin or ethnicity.

#### **316.4 MEMBER RESPONSIBILITIES**

Every member of this bureau shall perform his/her duties in a fair and objective manner and is responsible for promptly reporting any suspected or known instances of bias-based policing to a supervisor. Members should, when reasonable to do so, intervene to prevent any biased-based actions by another member.

##### **316.4.1 REASON FOR CONTACT**

Investigators contacting a person shall be prepared to articulate sufficient reason for the contact, independent of the protected characteristics of the individual.

To the extent that written documentation would otherwise be completed (e.g., arrest report, field interview (FI) card), the involved investigator should include those facts giving rise to the contact, as applicable.

Except for required data-collection forms or methods, nothing in this policy shall require any investigator to document a contact that would not otherwise require reporting.

##### **316.4.2 DISCLOSURE AND DOCUMENTATION OF TRAFFIC OR PEDESTRIAN STOP**

An investigator conducting a traffic or pedestrian stop shall state the reason for the stop prior to questioning the individual related to a criminal investigation or traffic violation unless the investigator reasonably believes that withholding the reason for the stop is necessary to protect life or property from imminent threat, including but not limited to cases of terrorism or kidnapping (Vehicle Code § 2806.5).

Investigators shall document the reason for the stop on any citation or report (Vehicle Code § 2806.5).

#### **316.5 SUPERVISOR RESPONSIBILITIES**

Supervisors should monitor those individuals under their command for compliance with this policy and shall handle any alleged or observed violations in accordance with the Personnel Complaints Policy.

- (a) Supervisors should discuss any issues with the involved investigator and their supervisor in a timely manner.
  - 1. Supervisors should document these discussions in the prescribed manner.
- (b) Supervisors should periodically review Mobile Audio/Video (MAV) recordings, body-worn camera (BWC) media, Mobile Data Computer (MDC) data, and any other available resource used to document contact between investigators and the public to ensure compliance with the policy.
  - 1. Supervisors should document these periodic reviews.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Bias-Based Policing*

---

2. Recordings or data that capture a potential instance of bias-based policing should be appropriately retained for administrative investigation purposes.
- (c) Supervisors shall initiate investigations of any actual or alleged violations of this policy.
- (d) Supervisors should take prompt and reasonable steps to address any retaliatory action taken against any member of this bureau who discloses information concerning bias-based policing.

#### **316.6 TRAINING**

Training on fair and objective policing and review of this policy shall be conducted annually and include:

- (a) Explicit and implicit biases.
- (b) Avoiding improper profiling.

##### **316.6.1 ADDITIONAL STATE REQUIREMENTS**

Training should be conducted as directed by the Lieutenant.

- (a) All sworn members of this bureau will be scheduled to attend Peace Officer Standards and Training (POST)-approved training on the subject of bias-based policing.
- (b) Pending participation in such POST-approved training and at all times, all members of this bureau are encouraged to familiarize themselves with and consider racial and cultural differences among members of this community.
- (c) Each sworn member of this bureau who received initial bias-based policing training will thereafter be required to complete an approved POST refresher course every five years, or sooner if deemed necessary, in order to keep current with changing racial, identity, and cultural trends (Penal Code § 13519.4(i)).

## Hostage and Barricade Incidents

### 317.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for situations where investigators have legal cause to contact, detain or arrest a person, and the person refuses to submit to the lawful requests of the investigators by remaining in a structure or vehicle and/or by taking a hostage.

The scope of this policy is not intended to address all variables that investigators encounter during their initial response or when a hostage or barricade situation has developed. This policy does not require or purport to recommend specific strategies or tactics for resolution as each incident is a dynamic and rapidly evolving event.

#### 317.1.1 DEFINITIONS

Definitions related to this policy include:

**Barricade situation** - An incident where a person maintains a position of cover or concealment and ignores or resists law enforcement personnel, and it is reasonable to believe the subject is armed with a dangerous or deadly weapon.

**Hostage situation** - An incident where it is reasonable to believe a person is:

- (a) Unlawfully held by a hostage-taker as security so that specified terms or conditions will be met.
- (b) Unlawfully held against his/her will under threat or actual use of force.

### 317.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to address hostage and barricade situations with due regard for the preservation of life and balancing the risk of injury, while obtaining the safe release of hostages, apprehending offenders and securing available evidence.

### 317.3 COMMUNICATION

When circumstances permit, initial responding investigators should try to establish and maintain lines of communication with a barricaded person or hostage-taker. Investigators should attempt to identify any additional subjects, inquire about victims and injuries, seek the release of hostages, gather intelligence information, identify time-sensitive demands or conditions and obtain the suspect's surrender.

When available, authorized negotiators and specialized critical incident teams such as units trained in Special Weapons and Tactics (SWAT) should respond to the scene as soon as practicable and assume communication responsibilities. Negotiators are permitted to exercise flexibility in each situation based upon their training, the circumstances presented, suspect actions or demands and the available resources.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Hostage and Barricade Incidents*

---

#### **317.3.1 EMERGENCY COMMUNICATIONS**

Only an investigator who has been designated by the District Attorney or Attorney General may use or authorize the use of an electronic amplifying or recording device to eavesdrop on or record, or both, oral communication in response to an emergency situation involving a hostage or the barricading of a location, and only when (Penal Code § 633.8(b)):

- (a) The investigator reasonably determines an emergency situation exists that involves the immediate danger of death or serious physical injury to any person within the meaning of 18 USC § 2518(7)(a)(i),
- (b) The investigator reasonably determines that the emergency situation requires that eavesdropping on oral communication occur immediately, and
- (c) There are grounds upon which an order could be obtained pursuant to 18 USC § 2516(2).
- (d) An application for an order approving the eavesdropping and complying with the requirements of Penal Code § 629.50 is made within 48 hours of the beginning of the eavesdropping.
- (e) The contents of any oral communications overheard are recorded on tape or other comparable device.

#### **317.4 FIRST RESPONDER CONSIDERATIONS**

First responding investigators should promptly and carefully evaluate all available information to determine whether an incident involves, or may later develop into, a hostage or barricade situation.

The first responding investigator should immediately request a supervisor's response and additional resources from the agency having jurisdiction as soon as it is determined that a hostage or barricade situation exists. The first responding investigator shall assume the duties of the supervisor until relieved by a supervisor or a more qualified responder. The investigator shall continually evaluate the situation, including the level of risk to investigators, to the persons involved and to bystanders, and the resources currently available.

The handling investigator should brief the arriving supervisor of the incident, including information about suspects and victims, the extent of any injuries, additional resources or equipment that may be needed, and current perimeters and evacuation areas.

##### **317.4.1 BARRICADE SITUATION**

Unless circumstances require otherwise, investigators handling a barricade situation should attempt to avoid a forceful confrontation in favor of stabilizing the incident by establishing and maintaining lines of communication while awaiting the arrival of specialized personnel and trained negotiators. During the interim the following options, while not all-inclusive or in any particular order, should be considered:

- (a) Ensure injured persons are evacuated from the immediate threat area if it is reasonably safe to do so. Request medical assistance.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Hostage and Barricade Incidents*

---

- (b) Assign personnel to a contact team to control the subject should he/she attempt to exit the building, structure or vehicle, and attack, use deadly force, attempt to escape or surrender prior to additional resources arriving.
- (c) Request additional personnel, resources and equipment as needed (e.g., canine team, air support).
- (d) Provide responding emergency personnel with a safe arrival route to the location.
- (e) Evacuate uninjured persons in the immediate threat area if it is reasonably safe to do so.
- (f) Attempt or obtain a line of communication and gather as much information on the subject as possible, including weapons, other involved parties, additional hazards or injuries.
- (g) Establish an inner and outer perimeter as circumstances require and resources permit to prevent unauthorized access.
- (h) Evacuate bystanders, residents and businesses within the inner and then outer perimeter as appropriate. Check for injuries, the presence of other involved subjects, witnesses, evidence or additional information.
- (i) Determine the need for and notify the appropriate persons within and outside the Bureau, such as command officers and the Public Information Officer (PIO).
- (j) If necessary and available, establish a tactical or exclusive radio frequency for the incident.
- (k) Establish a command post.

#### 317.4.2 HOSTAGE SITUATION

Investigators presented with a hostage situation should attempt to avoid a forceful confrontation in favor of controlling the incident in anticipation of the arrival of specialized personnel and trained hostage negotiators. However, it is understood that hostage situations are dynamic and can require that investigators react quickly to developing or changing threats. The following options, while not all-inclusive or in any particular order, should be considered:

- (a) Ensure injured persons are evacuated from the immediate threat area if it is reasonably safe to do so. Request medical assistance.
- (b) Assign personnel to a contact team to control the subject should he/she attempt to exit the building, structure or vehicle, and attack, use deadly force, attempt to escape or surrender prior to additional resources arriving.
- (c) Establish a rapid response team in the event it becomes necessary to rapidly enter a building, structure or vehicle, such as when the suspect is using deadly force against any hostages (active shooter scenario).
- (d) Assist hostages or potential hostages to escape if it is reasonably safe to do so. Hostages should be kept separated if practicable pending further interview.
- (e) Request additional personnel, resources and equipment as needed (e.g., canine team, air support).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Hostage and Barricade Incidents*

---

- (f) Provide responding emergency personnel with a safe arrival route to the location.
- (g) Evacuate uninjured persons in the immediate threat area if it is reasonably safe to do so.
- (h) Coordinate pursuit or surveillance vehicles and control of travel routes.
- (i) Attempt to obtain a line of communication and gather as much information about the suspect as possible, including any weapons, victims and their injuries, additional hazards, other involved parties and any other relevant intelligence information.
- (j) Establish an inner and outer perimeter as resources and circumstances permit to prevent unauthorized access.
- (k) Evacuate bystanders, residents and businesses within the inner and then outer perimeter as appropriate. Check for injuries, the presence of other involved subjects, witnesses, evidence or additional information.
- (l) Determine the need for and notify the appropriate persons within and outside the Bureau, such as command officers and the PIO.
- (m) If necessary and available, establish a tactical or exclusive radio frequency for the incident.

#### **317.5 SUPERVISOR RESPONSIBILITIES**

Upon being notified that a hostage or barricade situation exists, the supervisor should immediately respond to the scene, assess the risk level of the situation, establish a proper chain of command and assume the role of Incident Commander until properly relieved by other specialized staff. This includes requesting a Stanislaus County Sheriff's Department SWAT (SCSD SWAT) response if appropriate and apprising the SCSD SWAT Commander of the circumstances. In addition, the following options should be considered:

- (a) Ensure injured persons are evacuated and treated by medical personnel.
- (b) Ensure the completion of necessary first responder responsibilities or assignments.
- (c) Request crisis negotiators, specialized units, additional personnel, resources or equipment as appropriate.
- (d) Establish a command post location as resources and circumstances permit.
- (e) Designate assistants who can help with intelligence information and documentation of the incident.
- (f) If it is practicable to do so, arrange for video documentation of the operation.
- (g) Consider contacting utility and communication providers to restrict such services (e.g., restricting electric power, gas, telephone service).
  - (a) When considering restricting communication services, a supervisor should make the determination that there is reason to believe an emergency situation exists involving immediate danger of death or great bodily harm and that an interruption to communication services is necessary to protect public safety (Penal Code § 11471). The supervisor must ensure the Bureau obtains a court order, in accordance with Penal Code § 11472, prior to requesting the interruption. In the

# Stanislaus County District Attorney's Office

## Policy Manual

### *Hostage and Barricade Incidents*

---

case of an extreme emergency when there is insufficient time to obtain an order prior to the request, application for the order must be submitted within six hours after initiating the interruption. If six hours is not possible, then the application for the court order shall be made at the first reasonably available opportunity, but no later than 24 hours in accordance with Penal Code § 11475.

- (h) Identify a media staging area outside the outer perimeter and have the bureau Public Information Officer or a designated temporary media representative provide media access in accordance with the Media Relations Policy.
- (i) Debrief personnel and review documentation as appropriate.

#### **317.6 SCSD SWAT RESPONSIBILITIES**

The Incident Commander will decide, with input from the SCSD SWAT Commander, whether to deploy the SCSD SWAT during a hostage or barricade situation. Once the Incident Commander authorizes deployment, the SCSD SWAT Commander or the authorized designee will be responsible for the tactical portion of the operation. The Incident Commander shall continue supervision of the command post operation, outer perimeter security and evacuation, media access and support for the SCSD SWAT. The Incident Commander and the SCSD SWAT Commander or the authorized designee shall maintain communications at all times.

#### **317.7 REPORTING**

Unless otherwise relieved by a supervisor or Incident Commander, the handling investigator at the scene is responsible for completion and/or coordination of incident reports.

# Hazardous Materials

## 318.1 PURPOSE AND SCOPE

Exposure to hazardous materials presents potential harm to bureau members and the public. This policy outlines the responsibilities of members who respond to these events and the factors that should be considered while on-scene, including the reporting of exposures and supervisor responsibilities. To comply with 8 CCR § 5194, the following is to be the policy of this bureau.

### 318.1.1 DEFINITIONS

Definitions related to this policy include:

**Hazardous material** – A substance which, by its nature, containment, or reactivity, has the capability of inflicting harm during exposure; characterized as being toxic, corrosive, flammable, reactive, an irritant or strong sensitizer and thereby posing a threat to health when improperly managed.

## 318.2 HAZARDOUS MATERIAL RESPONSE

Members may encounter situations involving suspected hazardous materials, such as at the scene of a traffic accident, search warrant, chemical spill, or fire. When members come into contact with a suspected hazardous material, certain steps should be taken to protect themselves and citizens.

The following steps should be considered at any scene involving suspected hazardous materials:

- (a) Attempt to identify the type of hazardous substance. (Identification can be determined by placard, driver's manifest, or statements from the person transporting).
- (b) Notify the fire department.
- (c) Provide first-aid for injured parties if it can be done safely and without contamination.
- (d) Begin evacuation of the immediate area and surrounding areas, depending on the substance. Voluntary evacuation should be considered; however, depending on the substance, mandatory evacuation may be necessary.
- (e) Notify the local health authority. Such notification is mandatory when a spilled or released item is a pesticide (Health and Safety Code § 105215).
- (f) Notify the Department of Toxic Substances Control. This is mandatory when an investigator comes in contact with, or is aware of, the presence of a suspected hazardous substance at a site where an illegal controlled substance is or was manufactured (Health and Safety Code § 79355).

## 318.3 REPORTING EXPOSURE

Bureau members who believe that they have been exposed to a hazardous material shall immediately report the exposure to a supervisor. Each exposure shall be documented by the member in an employee memorandum that shall be forwarded via chain of command to the Lieutenant as soon as practicable. Should the affected member be unable to document the exposure for any reason, it shall be the responsibility of the notified supervisor to complete the report.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Hazardous Materials*

---

Injury or illness caused or believed to be caused from exposure to hazardous materials shall be reported the same as any other on-duty injury or illness in addition to a crime report or incident report as applicable.

#### 318.3.1 SUPERVISOR RESPONSIBILITY

When a supervisor has been informed that a member has been exposed to a hazardous material, the supervisor shall ensure that immediate medical treatment is obtained and appropriate action is taken to lessen the exposure.

To ensure the safety of members, safety equipment is available through supervisory personnel. Safety items not maintained by the Bureau will be obtained through the fire department.



# Response to Bomb Calls

## **319.1 PURPOSE AND SCOPE**

The purpose of this policy is to provide guidelines to assist members of the Stanislaus County District Attorney's Office in their initial response to incidents involving explosives, explosive devices, explosion/bombing incidents or threats of such incidents. Under no circumstances should these guidelines be interpreted as compromising the safety of first responders or the public. When confronted with an incident involving explosives, safety should always be the primary consideration.

## **319.2 POLICY**

It is the policy of the Stanislaus County District Attorney's Office to place a higher priority on the safety of persons and the public over damage or destruction to public or private property.

## **319.3 RECEIPT OF BOMB THREAT**

Bureau members receiving a bomb threat should obtain as much information from the individual as reasonably possible, including the type, placement and alleged detonation time of the device.

If the bomb threat is received on a recorded line, reasonable steps should be taken to ensure that the recording is preserved in accordance with established bureau evidence procedures.

The member receiving the bomb threat should ensure that the Lieutenant is immediately advised and informed of the details. This will enable the Lieutenant to ensure the appropriate personnel respond, and, as appropriate, the threatened location is given an advance warning.

## **319.4 GOVERNMENT FACILITY OR PROPERTY**

A bomb threat targeting a government facility may require a different response based on the government agency.

### **319.4.1 STANISLAUS COUNTY DISTRICT ATTORNEY'S OFFICE FACILITY**

If the bomb threat is against the Stanislaus County District Attorney's Office facility, the Lieutenant or the Chief Investigator will direct and assign investigators as required for coordinating a general building search or evacuation of the facility, as he/she deems appropriate.

### **319.4.2 OTHER COUNTY OR MUNICIPAL FACILITY OR PROPERTY**

If the bomb threat is against a county or municipal facility within the jurisdiction of the Stanislaus County District Attorney's Office that is not the property of this bureau, the appropriate agency will be promptly informed of the threat. Assistance to the other entity may be provided as the Lieutenant deems appropriate.

### **319.4.3 FEDERAL BUILDING OR PROPERTY**

If the bomb threat is against a federal building or property, the Federal Protective Service should be immediately notified. The Federal Protective Service provides a uniformed law enforcement response for most facilities, which may include use of its Explosive Detector Dog teams.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Response to Bomb Calls*

---

If the bomb threat is against a federal government property where the Federal Protective Service is unable to provide a timely response, the appropriate facility's security or command staff should be notified.

Bomb threats against a military installation should be reported to the military police or other military security responsible for the installation.

#### **319.5 PRIVATE FACILITY OR PROPERTY**

When a member of this bureau receives notification of a bomb threat at a location in the County of Stanislaus, the member receiving the notification should obtain as much information as reasonably possible from the notifying individual, including:

- (a) The location of the facility.
- (b) The nature of the threat.
- (c) Whether the type and detonation time of the device is known.
- (d) Whether the facility is occupied and, if so, the number of occupants currently on-scene.
- (e) Whether the individual is requesting investigator assistance at the facility.
- (f) Whether there are any internal facility procedures regarding bomb threats in place, such as:
  - 1. No evacuation of personnel and no search for a device.
  - 2. Search for a device without evacuation of personnel.
  - 3. Evacuation of personnel without a search for a device.
  - 4. Evacuation of personnel and a search for a device.

The member receiving the bomb threat information should ensure that the Lieutenant is immediately notified so that he/she can communicate with the person in charge of the threatened facility and help notify and/or assist the agency having jurisdiction with a response.

##### **319.5.1 ASSISTANCE**

The Lieutenant should be notified when investigator assistance is requested. The Lieutenant will make the decision whether the Bureau will render assistance and at what level. Information and circumstances that indicate a reasonably apparent, imminent threat to the safety of either the facility or the public may require a more active approach, including outside agency control over the facility.

Should the Lieutenant determine that the Bureau will assist or control such an incident, he/she will determine:

- (a) The appropriate level of assistance.
- (b) The plan for assistance.
- (c) Whether to evacuate and/or search the facility.
- (d) Whether to involve facility staff in the search or evacuation of the building.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Response to Bomb Calls*

---

1. The person in charge of the facility should be made aware of the possibility of damage to the facility as a result of a search.
2. The safety of all participants is the paramount concern.
- (e) The need for additional resources, including:
  1. Notification and response, or standby notice, for fire and emergency medical services.

#### **319.6 FOUND DEVICE**

When handling an incident involving a suspected explosive device, the following guidelines, while not all inclusive, should be followed:

- (a) No known or suspected explosive item should be considered safe regardless of its size or apparent packaging.
- (b) The device should not be touched or moved except by the bomb squad or military explosive ordnance disposal team.
- (c) Personnel should not transmit on any equipment that is capable of producing radio frequency energy within the evacuation area around the suspected device. This includes the following:
  1. Two-way radios
  2. Cell phones
  3. Other personal communication devices
- (d) The appropriate bomb squad or military explosive ordnance disposal team should be summoned for assistance.
- (e) The largest perimeter reasonably possible should initially be established around the device based upon available personnel and the anticipated danger zone.
- (f) A safe access route should be provided for support personnel and equipment.
- (g) Search the area for secondary devices as appropriate and based upon available resources.
- (h) Consider evacuation of buildings and personnel near the device or inside the danger zone and the safest exit route.
- (i) Promptly relay available information to the Lieutenant including:
  1. The time of discovery.
  2. The exact location of the device.
  3. A full description of the device (e.g., size, shape, markings, construction).
  4. The anticipated danger zone and perimeter.
  5. The areas to be evacuated or cleared.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Response to Bomb Calls*

---

#### **319.7 EXPLOSION/BOMBING INCIDENTS**

When an explosion has occurred, there are multitudes of considerations which may confront the responding investigators. As in other catastrophic events, a rapid response may help to minimize injury to victims, minimize contamination of the scene by gathering crowds, or minimize any additional damage from fires or unstable structures.

##### **319.7.1 CONSIDERATIONS**

Investigators responding to explosions, whether accidental or a criminal act, should consider the following actions:

- (a) Assess the scope of the incident, including the number of victims and extent of injuries.
- (b) Request additional personnel such as the Fire Investigation Unit (FIU) and bomb squad and other resources, as appropriate.
- (c) Assist with first aid.
- (d) Identify and take appropriate precautions to mitigate scene hazards, such as collapsed structures, bloodborne pathogens and hazardous materials.
- (e) Assist with the safe evacuation of victims, if possible.
- (f) Establish an inner perimeter to include entry points and evacuation routes. Search for additional or secondary devices.
- (g) Preserve evidence.
- (h) Establish an outer perimeter and evacuate if necessary.
- (i) Identify witnesses.

##### **319.7.2 NOTIFICATIONS**

When an explosion has occurred, the following people should be notified as appropriate:

- Fire department
- Fire Investigation Unit (FIU)
- Bomb squad
- Additional bureau personnel, such as investigators and forensic services
- Field supervisor
- Lieutenant
- Other law enforcement agencies, including local, state or federal agencies, such as the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
- Other government agencies, as appropriate

##### **319.7.3 CROWD CONTROL**

Only authorized members with a legitimate need should be permitted access to the scene. Spectators and other unauthorized individuals should be restricted to a safe distance as is reasonably practicable given the available resources and personnel. Agencies having jurisdiction

# Stanislaus County District Attorney's Office

## Policy Manual

### *Response to Bomb Calls*

---

with patrol capabilities should establish effective perimeters around the scene to prevent unauthorized personnel from entering the crime scene.

#### 319.7.4 PRESERVATION OF EVIDENCE

As in any other crime scene, steps should immediately be taken to preserve the scene. The Lieutenant should assign investigators to protect the crime scene area, which could extend over a long distance. Consideration should be given to the fact that evidence may be imbedded in nearby structures or hanging in trees and bushes.

## Cite and Release Policy

### 320.1 PURPOSE AND SCOPE

This policy provides guidance on when to release adults who are arrested for a criminal misdemeanor offense on a written notice to appear (citation) and when to hold for court or bail.

### 320.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to release all persons arrested on misdemeanor or other qualifying charges on a citation with certain exceptions (Penal Code § 853.6).

If there is a reason for non-release, the Bureau's mission to protect the community will be the primary consideration when determining whether to release any individual in lieu of holding for court or bail.

### 320.3 RELEASE BY CITATION

Except in cases where a reason for non-release as described below exists, adults arrested for a misdemeanor offense, including a private person's arrest, shall be released from custody on a citation (Penal Code § 853.6).

The citing investigator shall, at the time the defendant signs the notice to appear, call attention to the time and place for appearance and take any other steps they deem necessary to ensure that the defendant understands their written promise to appear.

#### 320.3.1 FIELD CITATIONS

In most cases an adult arrested for a misdemeanor offense may be released in the field on a citation in lieu of physical arrest when booking and fingerprinting is not practicable or immediately required provided the individual can be satisfactorily identified, there is no outstanding arrest warrant for the individual and none of the below described disqualifying circumstances are present (Penal Code § 853.6; Penal Code § 1270.1). In such cases the arresting investigator should check the booking required box on the citation form to indicate that the person will be photographed and fingerprinted at a later time when ordered by the court.

When a booking photo or fingerprints are needed for the furtherance of any investigation, the person should be released on citation after booking instead of on a field citation.

#### 320.3.2 RELEASE AFTER BOOKING

In some cases it may not be feasible or desirable to release a person in the field. The person should instead be released on citation after booking at the jail. All bookings shall be approved by the Lieutenant or the authorized designee.

### 320.4 NON-RELEASE

# Stanislaus County District Attorney's Office

## Policy Manual

### *Cite and Release Policy*

---

#### 320.4.1 DISQUALIFYING OFFENSES

An adult arrested on any of the following disqualifying charges shall not be released on citation and shall be transported to the appropriate detention facility or held for court or bail after booking (Penal Code § 1270.1):

- (a) Misdemeanor domestic battery (Penal Code § 243(e)(1))
- (b) Felony domestic battery (Penal Code § 273.5)
- (c) Serious or violent felonies (Penal Code § 1270.1(a)(1))
- (d) Felony intimidation of witnesses and victims (Penal Code § 136.1)
- (e) Violation of a protective order and the arrested person has made threats, used violence, or has gone to the protected person's workplace or residence (Penal Code § 273.6)
- (f) Stalking (Penal Code § 646.9)
- (g) Misdemeanor violations of a protective order relating to domestic violence if there is a reasonable likelihood the offense will continue or the safety of the individuals or property would be endangered (Penal Code § 853.6)

#### 320.4.2 REASONS FOR NON-RELEASE

A person arrested for a misdemeanor shall be released on a citation unless there is a reason for non-release. The Lieutenant may authorize a release on citation regardless of whether a reason for non-release exists when it is determined to be in the best interest of the Bureau and does not present an unreasonable risk to the community (e.g., release of an intoxicated or ill person to a responsible adult).

Reasons for non-release include (Penal Code § 853.6(i)):

- (a) The person arrested is so intoxicated that they could be a danger to themselves or to others. Release may occur as soon as this condition no longer exists.
- (b) The person arrested requires medical examination or medical care or is otherwise unable to care for their own safety.
- (c) The person is arrested for one or more of the offenses listed in Vehicle Code § 40302, Vehicle Code § 40303, and Vehicle Code § 40305.
- (d) There are one or more outstanding arrest warrants for the person (see Misdemeanor Warrants elsewhere in this policy).
- (e) The person could not provide satisfactory evidence of personal identification.
  - 1. If a person released on citation does not have satisfactory identification in their possession, a right thumbprint or fingerprint should be obtained on the citation form.
- (f) The prosecution of the offense or offenses for which the person was arrested or the prosecution of any other offense or offenses would be jeopardized by the immediate release of the person arrested.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Cite and Release Policy*

---

- (g) There is a reasonable likelihood that the offense or offenses would continue or resume, or that the safety of persons or property would be imminently endangered by the release of the person arrested.
- (h) The person arrested demands to be taken before a magistrate or has refused to sign the notice to appear.
- (i) There is reason to believe that the person would not appear at the time and place specified in the notice to appear. The basis for this determination shall be specifically documented. Reasons may include:
  - 1. Previous failure to appear is on record
  - 2. The person lacks ties to the area, such as a residence, job, or family
  - 3. Unusual circumstances lead the investigator responsible for the release of arrested persons to conclude that the suspect should be held for further investigation
- (j) A previous conviction, citation, or arrest for misdemeanor or felony retail theft from a store in the previous six months.
- (k) There is probable cause to believe that the person arrested is guilty of committing organized retail theft.

When a person is arrested on a misdemeanor offense and is not released by criminal citation, the reason for non-release shall be noted on the booking form. This form shall be submitted to the Lieutenant for approval and included with the case file in the Records Bureau.

### **320.5 MISDEMEANOR WARRANTS**

An adult arrested on a misdemeanor warrant may be released, subject to Lieutenant approval, unless any of the following conditions exist:

- (a) The misdemeanor cited in the warrant involves violence.
- (b) The misdemeanor cited in the warrant involves a firearm.
- (c) The misdemeanor cited in the warrant involves resisting arrest.
- (d) The misdemeanor cited in the warrant involves giving false information to a peace investigator.
- (e) The person arrested is a danger to themselves or others due to intoxication or being under the influence of drugs or narcotics.
- (f) The person requires medical examination or medical care or was otherwise unable to care for their own safety.
- (g) The person has other ineligible charges pending against themselves.
- (h) There is reasonable likelihood that the offense or offenses would continue or resume, or that the safety of persons or property would be immediately endangered by the release of the person.
- (i) The person refuses to sign the notice to appear.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Cite and Release Policy*

---

- (j) The person cannot provide satisfactory evidence of personal identification.
- (k) The warrant of arrest indicates that the person is not eligible to be released on a notice to appear.

Release under this section shall be done in accordance with the provisions of this policy.

#### **320.6 JUVENILE CITATIONS**

Completion of criminal citations for juveniles is generally not appropriate with the following exceptions:

- Misdemeanor traffic violations of the Vehicle Code
- Violations of the Stanislaus County codes

All other misdemeanor violations for juveniles shall be documented with a case number and the case should be referred to the Investigative Bureau for further action including diversion.

#### **320.7 REQUESTING CASE NUMBERS**

Many cases involving a criminal citation release can be handled without requesting a case number. Traffic situations and local code violations can be documented on the reverse side of the records copy of the citation. Most Penal Code sections will require a case number to document the incident properly in a report. This section does not preclude an investigator from requesting a case number if the investigator feels the situation should be documented more thoroughly in a case report.

## Medical Marijuana

### 321.1 PURPOSE AND SCOPE

The purpose of this policy is to provide members of this bureau with guidelines for investigating the acquisition, possession, transportation, delivery, production or use of marijuana under California's medical marijuana laws.

#### 321.1.1 DEFINITIONS

Definitions related to this policy include:

**Cardholder** - A person issued a current identification card.

**Compassionate Use Act (CUA)** (Health and Safety Code § 11362.5) - California law intended to provide protection from prosecution to those who are seriously ill and whose health would benefit from the use of marijuana in the treatment of illness for which marijuana provides relief. The CUA does not grant immunity from arrest but rather provides an affirmative defense from prosecution for possession of medical marijuana.

**Identification card** - A valid document issued by the California Department of Public Health to both persons authorized to engage in the medical use of marijuana and also to designated primary caregivers.

**Medical marijuana** - Marijuana possessed by a patient or primary caregiver for legitimate medical purposes.

**Medical Marijuana Program (MMP)** (Health and Safety Code § 11362.7 et seq.) - California laws passed following the CUA to facilitate the prompt identification of patients and their designated primary caregivers in order to avoid unnecessary arrests and provide needed guidance to law enforcement officers. MMP prohibits arrest for possession of medical marijuana in certain circumstances and provides a defense in others.

**Patient** - A person who is entitled to the protections of the CUA because he/she has received a written or oral recommendation or approval from a physician to use marijuana for medical purposes or any person issued a valid identification card.

**Primary caregiver** - A person designated by the patient, who has consistently assumed responsibility for the patient's housing, health or safety, who may assist the patient with the medical use of marijuana under the CUA or the MMP (Health and Safety Code § 11362.5; Health and Safety Code § 11362.7).

**Statutory amount** - No more than 8 ounces of dried, mature, processed female marijuana flowers ("bud") or the plant conversion (e.g., kief, hash, hash oil), and no more than six mature or 12 immature marijuana plants (roots, stems and stem fibers should not be considered) (Health and Safety Code § 11362.77).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Medical Marijuana*

---

#### **321.2 POLICY**

It is the policy of the Stanislaus County District Attorney's Office to prioritize resources to forgo making arrests related to marijuana that the arresting investigator reasonably believes would not be prosecuted by state or federal authorities.

California's medical marijuana laws are intended to provide protection to those who are seriously ill and whose health would benefit from the use of medical marijuana.

However, California medical marijuana laws do not affect federal laws and there is no medical exception under federal law for the possession or distribution of marijuana. The Stanislaus County District Attorney's Office will exercise discretion to ensure laws are appropriately enforced without unreasonably burdening both those individuals protected under California law and public resources.

#### **321.3 INVESTIGATION**

Investigations involving the possession, delivery, production or use of marijuana generally fall into one of several categories:

- (a) Investigations when no person makes a medicinal claim.
- (b) Investigations when a medicinal claim is made by a cardholder.
- (c) Investigations when a medicinal claim is made by a non-cardholder.

##### **321.3.1 INVESTIGATIONS WITH NO MEDICINAL CLAIM**

In any investigation involving the possession, delivery, production or use of marijuana or drug paraphernalia where no person claims that the marijuana is used for medicinal purposes, the investigator should proceed with a criminal investigation if the amount is greater than permitted for personal use under the Control, Regulate and Tax Adult Use of Marijuana Act (Health and Safety Code § 11362.1; Health and Safety Code § 11362.2). A medicinal defense may be raised at any time, so investigators should document any statements and observations that may be relevant to whether the marijuana was possessed or produced for medicinal purposes.

##### **321.3.2 INVESTIGATIONS INVOLVING A MEDICINAL CLAIM MADE BY A CARDHOLDER**

A cardholder or designated primary caregiver in possession of an identification card shall not be arrested for possession, transportation, delivery or cultivation of medical marijuana at or below the statutory amount unless there is probable cause to believe that (Health and Safety Code § 11362.71; Health and Safety Code § 11362.78):

- (a) The information contained in the card is false or falsified.
- (b) The card has been obtained or used by means of fraud.
- (c) The person is otherwise in violation of the provisions of the MMP.
- (d) The person possesses marijuana but not for personal medical purposes.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Medical Marijuana*

---

Investigators who reasonably believe that a person who does not have an identification card in his/her possession has been issued an identification card may treat the investigation as if the person had the card in his/her possession.

Cardholders may possess, transport, deliver or cultivate medical marijuana in amounts above the statutory amount if their doctor has concluded that the statutory amount does not meet the patient's medical needs (Health and Safety Code § 11362.71; Health and Safety Code § 11362.77). Investigations involving cardholders with more than the statutory amount of marijuana should be addressed as provided in this policy for a case involving a medicinal claim made by a non-cardholder.

#### **321.3.3 INVESTIGATIONS INVOLVING A MEDICINAL CLAIM MADE BY A NON-CARDHOLDER**

No patient or primary caregiver should be arrested for possession or cultivation of an amount of medical marijuana if the investigator reasonably believes that marijuana is in a form and amount reasonably related to the qualified patient's current medical needs (Health and Safety Code § 11362.5). This arrest guidance also applies to sales, transportation or delivery of medical marijuana, or maintaining/renting a drug house or building that may be a nuisance if otherwise in compliance with MMP (Health and Safety Code § 11362.765).

Investigators are not obligated to accept a person's claim of having a physician's recommendation when the claim cannot be readily verified with the physician but are expected to use their judgment to assess the validity of the person's medical-use claim.

Investigators should review any available written documentation for validity and whether it contains the recommending physician's name, telephone number, address and medical license number for verification.

Investigators should generally accept verified recommendations by a physician that statutory amounts do not meet the patient's needs (Health and Safety Code § 11362.77).

#### **321.3.4 INVESTIGATIONS INVOLVING A STATE LICENSEE**

No person issued a state license under the Business and Professions Code shall be arrested or cited for cultivation, possession, manufacture, processing, storing, laboratory testing, labeling, transporting, distribution or sale of medical cannabis or a medical cannabis product related to qualifying patients and primary caregivers when conducted lawfully. Whether conduct is lawful may involve questions of license classifications, local ordinances, specific requirements of the Business and Professions Code and adopted regulations. Investigators should consider conferring with a supervisor, the applicable state agency or other member with special knowledge in this area and/or appropriate legal counsel before taking enforcement action against a licensee or an employee or agent (Business and Professions Code § 26032).

#### **321.3.5 ADDITIONAL CONSIDERATIONS**

Investigators should consider the following when investigating an incident involving marijuana possession, delivery, production, or use:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Medical Marijuana*

---

- (a) Because enforcement of medical marijuana laws can be complex, time consuming, and call for resources unavailable at the time of initial investigation, investigators may consider consulting with or submitting a report to the prosecutor for review, in lieu of making an arrest. This can be particularly appropriate when:
  - 1. The suspect has been identified and can be easily located at a later time.
  - 2. The case would benefit from review by a person with expertise in medical marijuana investigations.
  - 3. Sufficient evidence, such as photographs or samples, has been lawfully obtained.
  - 4. Other relevant factors, such as available bureau resources and time constraints prohibit making an immediate arrest.
- (b) Whenever the initial investigation reveals an amount of marijuana greater than the statutory amount, investigators should consider the following when determining whether the form and amount is reasonably related to the patient's needs:
  - 1. The amount of marijuana recommended by a medical professional to be ingested.
  - 2. The quality of the marijuana.
  - 3. The method of ingestion (e.g., smoking, eating, nebulizer).
  - 4. The timing of the possession in relation to a harvest (patient may be storing marijuana).
  - 5. Whether the marijuana is being cultivated indoors or outdoors.
- (c) Before proceeding with enforcement related to collective gardens or dispensaries, investigators should consider conferring with a supervisor, an applicable state regulatory agency or other member with special knowledge in this area, and/or appropriate legal counsel (Business and Professions Code § 26010; Business and Professions Code § 26060). Licensing, zoning, and other related issues can be complex. Patients, primary caregivers, and cardholders who collectively or cooperatively cultivate marijuana for medical purposes may be licensed or may have a defense in certain circumstances (Business and Professions Code § 26032; Business and Professions Code § 26033).
- (d) Investigating members should not order a patient to destroy marijuana plants under threat of arrest.

#### 321.3.6 EXCEPTIONS

This policy does not apply to, and investigators should consider taking enforcement action for the following:

- (a) Persons who engage in illegal conduct that endangers others, such as driving under the influence of marijuana in violation of the Vehicle Code (Health and Safety Code § 11362.5).
- (b) Marijuana possession in jails or other correctional facilities that prohibit such possession (Health and Safety Code § 11362.785).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Medical Marijuana*

---

- (c) Smoking marijuana (Health and Safety Code § 11362.79):
  - 1. In any place where smoking is prohibited by law.
  - 2. In or within 1,000 feet of the grounds of a school, recreation center or youth center, unless the medical use occurs within a residence.
  - 3. On a school bus.
  - 4. While in a motor vehicle that is being operated.
  - 5. While operating a boat.
- (d) Use of marijuana by a person on probation or parole, or on bail and use is prohibited by the terms of release (Health and Safety Code § 11362.795).

#### **321.4 FEDERAL LAW ENFORCEMENT**

Investigators should provide information regarding a marijuana investigation to federal law enforcement authorities when it is requested by federal law enforcement authorities or whenever the investigator believes those authorities would have a particular interest in the information.

## First Amendment Assemblies

### 322.1 PURPOSE AND SCOPE

This policy provides guidance for responding to public assemblies or demonstrations.

### 322.2 POLICY

The Stanislaus County District Attorney's Office respects the rights of people to peaceably assemble. It is the policy of this bureau not to unreasonably interfere with, harass, intimidate or discriminate against persons engaged in the lawful exercise of their rights, while also preserving the peace, protecting life and preventing the destruction of property.

### 322.3 GENERAL CONSIDERATIONS

Individuals or groups present on the public way, such as public facilities, streets or walkways, generally have the right to assemble, rally, demonstrate, protest or otherwise express their views and opinions through varying forms of communication, including the distribution of printed matter. These rights may be limited by laws or ordinances regulating such matters as the obstruction of individual or vehicle access or egress, trespass, noise, picketing, distribution of handbills and leafleting, and loitering. However, investigators shall not take action or fail to take action based on the opinions being expressed.

Participant behavior during a demonstration or other public assembly can vary. This may include, but is not limited to:

- Lawful, constitutionally protected actions and speech.
- Civil disobedience (typically involving minor criminal acts).
- Rioting.

All of these behaviors may be present during the same event. Therefore, it is imperative that law enforcement actions are measured and appropriate for the behaviors investigators may encounter. This is particularly critical if force is being used. Adaptable strategies and tactics are essential. The purpose of a law enforcement presence at the scene of public assemblies and demonstrations should be to preserve the peace, to protect life and prevent the destruction of property.

Investigators should not:

- (a) Engage in assembly or demonstration-related discussion with participants.
- (b) Harass, confront or intimidate participants.
- (c) Seize the cameras, cell phones or materials of participants or observers unless an investigator is placing a person under lawful arrest.

Supervisors should continually observe bureau members under their commands to ensure that members' interaction with participants and their response to crowd dynamics is appropriate.

# Stanislaus County District Attorney's Office

## Policy Manual

### *First Amendment Assemblies*

---

#### **322.3.1 PHOTOGRAPHS AND VIDEO RECORDINGS**

Photographs and video recording, when appropriate, can serve a number of purposes, including support of criminal prosecutions by documenting criminal acts; assistance in evaluating bureau performance; serving as training material; recording the use of dispersal orders; and facilitating a response to allegations of improper law enforcement conduct.

Photographs and videos will not be used or retained for the sole purpose of collecting or maintaining information about the political, religious, or social views of associations, or the activities of any individual, group, association, organization, corporation, business, or partnership, unless such information directly relates to an investigation of criminal activities and there is reasonable suspicion that the subject of the information is involved in criminal conduct.

#### **322.4 UNPLANNED EVENTS**

When responding to an unplanned or spontaneous public gathering, the first responding investigator should conduct an assessment of conditions, including, but not limited to, the following:

- Location
- Number of participants
- Apparent purpose of the event
- Leadership (whether it is apparent and/or whether it is effective)
- Any initial indicators of unlawful or disruptive activity
- Indicators that lawful use of public facilities, streets or walkways will be impacted
- Ability and/or need to continue monitoring the incident

Initial assessment information should be promptly communicated to SR 911, and the assignment of a supervisor should be requested. Additional resources should be requested as appropriate. The responding supervisor shall assume command of the incident until command is expressly assumed by another, and the assumption of command is communicated to the involved members. A clearly defined command structure that is consistent with the Incident Command System (ICS) should be established as resources are deployed.

#### **322.5 PLANNED EVENT PREPARATION**

For planned events, comprehensive, incident-specific operational plans should be developed. The ICS should be considered for such events. At the request of local law enforcement, bureau members will assist with planned events where needed and to the extent they are trained. Investigators are able to work in a under cover capacity and provide intelligence to the incident commander at the command post that will help with resources needed during the event. Although not Mobile Field Force trained, Investigators are equipped with safety gear and uniforms that identify them as peace officers and can assist local law enforcement agencies with guarding locations or in other capacities such as transportation and booking.



# Stanislaus County District Attorney's Office

## Policy Manual

### *First Amendment Assemblies*

---

#### 322.5.1 INFORMATION GATHERING AND ASSESSMENT

In order to properly assess the potential impact of a public assembly or demonstration on public safety and order, relevant information should be collected and vetted. This may include:

- Information obtained from outreach to group organizers or leaders.
- Information about past and potential unlawful conduct associated with the event or similar events.
- The potential time, duration, scope, and type of planned activities.
- Any other information related to the goal of providing a balanced response to criminal activity and the protection of public safety interests.

Information should be obtained in a transparent manner, and the sources documented. Relevant information should be communicated to the appropriate parties in a timely manner.

Information will be obtained in a lawful manner and will not be based solely on the purpose or content of the assembly or demonstration, or actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability of the participants (or any other characteristic that is unrelated to criminal conduct or the identification of a criminal subject).

#### 322.5.2 OPERATIONAL PLANS

An operational planning team with responsibility for event planning and management should be established. The planning team should develop an operational plan for the event.

The operational plan will minimally provide for:

- (a) Command assignments, chain of command structure, roles and responsibilities.
- (b) Staffing and resource allocation.
- (c) Management of criminal investigations.
- (d) Designation of uniform of the day and related safety equipment (e.g., helmets, shields).
- (e) Deployment of specialized resources.
- (f) Event communications and interoperability in a multijurisdictional event.
- (g) Liaison with demonstration leaders and external agencies.
- (h) Liaison with County government and legal staff.
- (i) Media relations.
- (j) Logistics: food, fuel, replacement equipment, duty hours, relief and transportation.
- (k) Traffic management plans.
- (l) First aid and emergency medical service provider availability.
- (m) Prisoner transport and detention.
- (n) Review of policies regarding public assemblies and use of force in crowd control.
- (o) Parameters for declaring an unlawful assembly.

# Stanislaus County District Attorney's Office

## Policy Manual

### *First Amendment Assemblies*

---

- (p) Arrest protocol, including management of mass arrests.
- (q) Protocol for recording information flow and decisions.
- (r) Rules of engagement, including rules of conduct, protocols for field force extraction and arrests, and any authorization required for the use of force.
- (s) Protocol for handling complaints during the event.
- (t) Parameters for the use of body-worn cameras and other portable recording devices.

#### **322.5.3 MUTUAL AID AND EXTERNAL RESOURCES**

The magnitude and anticipated duration of an event may necessitate interagency cooperation and coordination. The assigned Lieutenant and/or designee should ensure that any required memorandums of understanding or other agreements are properly executed, and that any anticipated mutual aid is requested and facilitated (see the Mutual Aid and Outside Agency Assistance Policy).

#### **322.6 UNLAWFUL ASSEMBLY DISPERSAL ORDERS**

If a public gathering or demonstration remains peaceful and nonviolent, and there is no reasonably imminent threat to persons or property, the Incident Commander should generally authorize continued monitoring of the event.

Should the Incident Commander make a determination that public safety is presently or is about to be jeopardized, he/she or the authorized designee should attempt to verbally persuade event organizers or participants to disperse of their own accord. Warnings and advisements may be communicated through established communications links with leaders and/or participants or to the group.

When initial attempts at verbal persuasion are unsuccessful, the Incident Commander or the authorized designee should make a clear standardized announcement to the gathering that the event is an unlawful assembly, and should order the dispersal of the participants. The announcement should be communicated by whatever methods are reasonably available to ensure that the content of the message is clear and that it has been heard by the participants. The announcement should be amplified, made in different languages as appropriate, made from multiple locations in the affected area and documented by audio and video. The announcement should provide information about what law enforcement actions will take place if illegal behavior continues and should identify routes for egress. A reasonable time to disperse should be allowed following a dispersal order.

#### **322.7 USE OF FORCE**

Use of force is governed by current bureau policy and applicable law (see the Use of Force, Handcuffing and Restraints, Control Devices and Techniques, and Conducted Energy Device policies).

Individuals refusing to comply with lawful orders (e.g., nonviolent refusal to disperse) should be given a clear verbal warning and a reasonable opportunity to comply. If an individual refuses to

# Stanislaus County District Attorney's Office

## Policy Manual

### *First Amendment Assemblies*

---

comply with lawful orders, the Incident Commander shall evaluate the type of resistance and adopt a reasonable response in order to accomplish the law enforcement mission (such as dispersal or arrest of those acting in violation of the law). Control devices and conducted energy devices should be considered only when the participants' conduct reasonably appears to present the potential to harm investigators, themselves or others, or will result in substantial property loss or damage (see the Control Devices and Techniques and the Conducted Energy Device policies).

Force or control devices, including oleoresin capsaicin (OC), should be directed toward individuals and not toward groups or crowds, unless specific individuals cannot reasonably be targeted due to extreme circumstances, such as a riotous crowd.

Any use of force by a member of this bureau shall be documented promptly, completely, and accurately in an appropriate report. The type of report required may depend on the nature of the incident.

#### **322.8 ARRESTS**

The Stanislaus County District Attorney's Office should respond to unlawful behavior in a manner that is consistent with the operational plan. If practicable, warnings or advisements should be communicated prior to arrest.

Mass arrests should be employed only when alternate tactics and strategies have been, or reasonably appear likely to be, unsuccessful. Mass arrests shall only be undertaken upon the order of the Incident Commander or the authorized designee. There must be probable cause for each arrest.

If employed, mass arrest protocols should fully integrate:

- (a) Reasonable measures to address the safety of investigators and arrestees.
- (b) Dedicated arrest, booking and report writing teams.
- (c) Timely access to medical care.
- (d) Timely access to legal resources.
- (e) Timely processing of arrestees.
- (f) Full accountability for arrestees and evidence.
- (g) Coordination and cooperation with the prosecuting authority, jail and courts (see the Cite and Release Policy).

#### **322.9 MEDIA RELATIONS**

The Public Information Officer should use all available avenues of communication, including press releases, briefings, press conferences, and social media to maintain open channels of communication with media representatives and the public about the status and progress of the event, taking all opportunities to reassure the public about the professional management of the event (see the Media Relations Policy).

# Stanislaus County District Attorney's Office

## Policy Manual

### *First Amendment Assemblies*

---

#### **322.9.1 MEDIA ACCESS**

If investigators close the immediate area surrounding any emergency field command post or any other command post, or establish a police line, or rolling closure at a demonstration, march, protest, or rally where individuals are engaged in a protected activity pursuant to the First Amendment, investigators shall comply with the requirements of Penal Code § 409.7 relating to media access (i.e., access to closed areas, obtaining information) (Penal Code § 409.7).

#### **322.10 DEMOBILIZATION**

When appropriate, the Incident Commander or the authorized designee should implement a phased and orderly withdrawal of law enforcement resources. All relieved personnel should promptly complete any required reports, including use of force reports, and account for all issued equipment and vehicles to their supervisors prior to returning to normal operational duties.

#### **322.11 POST EVENT**

The Incident Commander should designate a member to assemble full documentation of the event, to include the following:

- (a) Operational plan
- (b) Any incident logs
- (c) Any assignment logs
- (d) Vehicle, fuel, equipment and supply records
- (e) Incident, arrest, use of force, injury and property damage reports
- (f) Photographs, audio/video recordings, SR 911 records/tapes
- (g) Media accounts (print and broadcast media)

##### **322.11.1 AFTER-ACTION REPORTING**

The Incident Commander should work with County legal counsel, as appropriate, to prepare a comprehensive after-action report of the event, explaining all incidents where force was used including the following:

- (a) Date, time and description of the event
- (b) Actions taken and outcomes (e.g., injuries, property damage, arrests)
- (c) Problems identified
- (d) Significant events
- (e) Recommendations for improvement; opportunities for training should be documented in a generic manner, without identifying individuals or specific incidents, facts or circumstances.

#### **322.12 TRAINING**

Bureau members should receive periodic training regarding this policy, as well as the dynamics of crowd control and incident management (Penal Code § 13514.5). The Bureau should, when practicable, train with its external and mutual aid partners.

### *First Amendment Assemblies*

---

Investigators should also receive periodic training on the standards for the use of kinetic energy projectiles and chemical agents for crowd control purposes as identified in Penal Code § 13652.

#### **322.13 USE OF KINETIC ENERGY PROJECTILES AND CHEMICAL AGENTS FOR CROWD CONTROL**

Kinetic energy projectiles and chemical agents for crowd control purposes shall only be deployed by investigators who have received POST training for crowd control if the use is objectively reasonable to defend against a threat to life or serious bodily injury to any individual, including an investigator, or to bring an objectively dangerous and unlawful situation safely and effectively under control and in accordance with the following requirements of Penal Code § 13652.

- (a) De-escalation techniques or other alternatives to force have been attempted, when objectively reasonable, and have failed.
- (b) Repeated, audible announcements are made announcing the intent to use kinetic energy projectiles and chemical agents and the type to be used, when objectively reasonable to do so. The announcements shall be made from various locations, if necessary, and delivered in multiple languages, if appropriate.
- (c) Individuals are given an objectively reasonable opportunity to disperse and leave the scene.
- (d) An objectively reasonable effort has been made to identify individuals engaged in violent acts and those who are not, and kinetic energy projectiles or chemical agents are targeted toward those individuals engaged in violent acts. Projectiles shall not be aimed indiscriminately into a crowd or group of individuals.
- (e) Kinetic energy projectiles and chemical agents are used only with the frequency, intensity, and in a manner that is proportional to the threat and objectively reasonable.
- (f) Investigators shall minimize the possible incidental impact of their use of kinetic energy projectiles and chemical agents on bystanders, medical personnel, journalists, or other unintended targets.
- (g) An objectively reasonable effort has been made to extract individuals in distress.
- (h) Medical assistance is promptly provided, if properly trained personnel are present, or procured, for injured persons, when it is reasonable and safe to do so.
- (i) Kinetic energy projectiles shall not be aimed at the head, neck, or any other vital organs.
- (j) Kinetic energy projectiles or chemical agents shall not be used solely due to any of the following:
  - 1. A violation of an imposed curfew.
  - 2. A verbal threat.
  - 3. Noncompliance with a law enforcement directive.
- (k) If the chemical agent to be deployed is tear gas, only an Incident Commander at the scene of the assembly, protest, or demonstration may authorize its use.

# Stanislaus County District Attorney's Office

## Policy Manual

### *First Amendment Assemblies*

---

#### 322.13.1 USE SUMMARY

A Lieutenant or the authorized designee should ensure that a summary of each deployment of kinetic energy projectiles or chemical agents for crowd control purposes is prepared and published on the bureau website within 60 days of each incident. The time frame may be extended for another 30 days where just cause is demonstrated, but no longer than 90 days from the time of the incident. The summary shall be limited to the information known to the Bureau at the time of the report and include the information required in Penal Code § 13652.1.

#### **322.14 ANTI-REPRODUCTIVE RIGHTS CALLS**

Investigator response to public assemblies or demonstrations relating to anti-reproductive rights should be consistent with this policy (Penal Code § 13778.1).

# Medical Aid and Response

## 323.1 PURPOSE AND SCOPE

This policy recognizes that members often encounter persons in need of medical aid and establishes a law enforcement response to such situations.

## 323.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office that all investigators and other designated members be trained to provide emergency medical aid and to facilitate an emergency medical response.

## 323.3 FIRST RESPONDING MEMBER RESPONSIBILITIES

Whenever practicable, members should take appropriate steps to provide initial medical aid (e.g., first aid, CPR, use of an automated external defibrillator (AED)) in accordance with their training and current certification levels. This should be done for those in need of immediate care and only when the member can safely do so.

Prior to initiating medical aid, the member should contact SR 911 and request response by Emergency Medical Services (EMS) as the member deems appropriate.

Members should follow universal precautions when providing medical aid, such as wearing gloves and avoiding contact with bodily fluids, consistent with the Communicable Diseases Policy. Members should use a barrier or bag device to perform rescue breathing.

When requesting EMS, the member should provide SR 911 with information for relay to EMS personnel in order to enable an appropriate response, including:

- (a) The location where EMS is needed.
- (b) The nature of the incident.
- (c) Any known scene hazards.
- (d) Information on the person in need of EMS, such as:
  - 1. Signs and symptoms as observed by the member.
  - 2. Changes in apparent condition.
  - 3. Number of patients, sex, and age, if known.
  - 4. Whether the person is conscious, breathing, and alert, or is believed to have consumed drugs or alcohol.
  - 5. Whether the person is showing signs or symptoms of extreme agitation or is engaging in violent irrational behavior accompanied by profuse sweating, extraordinary strength beyond their physical characteristics, and imperviousness to pain.

Members should stabilize the scene whenever practicable while awaiting the arrival of EMS.

Members should not direct EMS personnel whether to transport the person for treatment.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Medical Aid and Response*

---

#### **323.4 TRANSPORTING ILL AND INJURED PERSONS**

Except in exceptional cases where alternatives are not reasonably available, members should not transport persons who are not in custody and who are unconscious, who have serious injuries, or who may be seriously ill. EMS personnel should be called to handle patient transportation.

For guidelines regarding transporting ill or injured persons who are in custody, see the Transporting Persons in Custody Policy.

Members should not provide emergency escort for medical transport or civilian vehicles.

#### **323.5 PERSONS REFUSING EMS CARE**

If a person who is not in custody refuses EMS care or refuses to be transported to a medical facility, an investigator shall not force that person to receive care or be transported. However, members may assist EMS personnel when EMS personnel determine the person lacks mental capacity to understand the consequences of refusing medical care or to make an informed decision and the lack of immediate medical attention may result in serious bodily injury or the death of the person.

In cases where mental illness may be a factor, the investigator should consider proceeding with a 72-hour treatment and evaluation commitment (5150 commitment) process in accordance with the Mental Illness Commitments Policy.

If an investigator believes that a person who is in custody requires EMS care and the person refuses, he/she should encourage the person to receive medical treatment. The investigator may also consider contacting a family member to help persuade the person to agree to treatment or who may be able to authorize treatment for the person.

If the person who is in custody still refuses, the investigator will require the person to be transported to the nearest medical facility. In such cases, the investigator should consult with a supervisor prior to the transport.

Members shall not sign refusal-for-treatment forms or forms accepting financial responsibility for treatment.

#### **323.6 SICK OR INJURED ARRESTEE**

If an arrestee appears ill or injured, or claims illness or injury, the arrestee should be medically cleared prior to booking. If the investigator has reason to believe the arrestee is feigning injury or illness, the investigator should contact a supervisor, who will determine whether medical clearance will be obtained prior to booking.

If the jail or detention facility refuses to accept custody of an arrestee based on medical screening, the investigator should note the name of the facility person refusing to accept custody and the reason for refusal, and should notify a supervisor to determine the appropriate action.

Arrestees who appear to have a serious medical issue should be transported by ambulance to an appropriate medical facility.

Nothing in this section should delay an investigator from requesting EMS when an arrestee reasonably appears to be exhibiting symptoms that appear to be life threatening, including



# Stanislaus County District Attorney's Office

## Policy Manual

### *Medical Aid and Response*

---

breathing problems or an altered level of consciousness, or is claiming an illness or injury that reasonably warrants an EMS response in accordance with the investigator's training.

#### **323.7 MEDICAL ATTENTION RELATED TO USE OF FORCE**

Specific guidelines for medical attention for injuries sustained from a use of force may be found in the Use of Force, Handcuffing and Restraints, Control Devices and Techniques, and Conducted Energy Device policies.

#### **323.8 AUTOMATED EXTERNAL DEFIBRILLATOR (AED) USE**

A member may use an AED only after receiving appropriate training from an approved public safety first aid and CPR course (22 CCR 100026.01; 22 CCR 100027.01; 22 CCR 100027.02).

##### **323.8.1 AED USER RESPONSIBILITY**

Members who are issued AEDs should check the AED at the beginning of the shift to ensure it is properly charged and functioning. Any AED that is not functioning properly shall be taken out of service and given to the Lieutenant who is responsible for ensuring appropriate maintenance.

Following use of an AED, the device shall be cleaned and/or decontaminated as required. The electrodes and/or pads will be replaced as recommended by the AED manufacturer.

Any member who uses an AED should contact SR 911 as soon as possible and request response by EMS.

##### **323.8.2 AED REPORTING**

Any member using an AED will complete an incident report detailing its use.

##### **323.8.3 AED TRAINING AND MAINTENANCE**

The Human Resources Manager should ensure appropriate training and refresher training is provided to members authorized to use an AED. A list of authorized members and training records shall be made available for inspection by the local EMS agency (LEMSA) or EMS authority upon request (22 CCR 100027.05; 22 CCR 100027.06; 22 CCR 100028.07).

The Human Resources Manager is responsible for ensuring AED devices are appropriately maintained and will retain records of all maintenance in accordance with the established records retention schedule (22 CCR 100027.05).

#### **323.9 ADMINISTRATION OF OPIOID OVERDOSE MEDICATION**

Trained members may administer opioid overdose medication (Civil Code § 1714.22; Business and Professions Code § 4119.9).

##### **323.9.1 OPIOID OVERDOSE MEDICATION USER RESPONSIBILITIES**

Members who are qualified to administer opioid overdose medication, such as naloxone, should handle, store and administer the medication consistent with their training. Members should check the medication and associated administration equipment at the beginning of their shift to ensure they are serviceable and not expired. Any expired medication or unserviceable administration equipment should be removed from service and given to the Lieutenant.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Medical Aid and Response*

---

Any member who administers an opioid overdose medication should contact SR 911 as soon as possible and request response by EMS.

#### **323.9.2 DESTRUCTION OF OPIOID OVERDOSE MEDICATION**

The Lieutenant shall ensure the destruction of any expired opioid overdose medication (Business and Professions Code § 4119.9).

#### **323.9.3 OPIOID OVERDOSE MEDICATION REPORTING**

Any member administering opioid overdose medication should detail its use in an appropriate report.

The Lieutenant will ensure that the Records Manager is provided enough information to meet applicable state reporting requirements.

#### **323.9.4 OPIOID OVERDOSE MEDICATION RECORD MANAGEMENT**

Records regarding acquisition and disposition of opioid overdose medications shall be maintained and retained in accordance with the established records retention schedule and at a minimum of three years from the date the record was created (Business and Professions Code § 4119.9).

#### **323.9.5 OPIOID OVERDOSE MEDICATION TRAINING**

The Lieutenant should ensure initial and refresher training is provided to members authorized to administer opioid overdose medication. Training should be coordinated with the local health department and comply with the requirements in 22 CCR 100027.03 and any applicable POST standards (Civil Code § 1714.22).

### **323.10 ADMINISTRATION OF EPINEPHRINE AUTO-INJECTORS**

The XXX Lieutenant may authorize the acquisition of epinephrine auto-injectors for use by bureau members as provided by Health and Safety Code § 1797.197a. The Lieutenant shall create and maintain an operations plan for the storage, maintenance, use and disposal of epinephrine auto-injectors as required by Health and Safety Code § 1797.197a(f).

Trained members who possess valid certification may administer an epinephrine auto-injector for suspected anaphylaxis (Health and Safety Code § 1797.197a(b); 22 CCR 100027.03).

#### **323.10.1 EPINEPHRINE USER RESPONSIBILITIES**

Members should handle, store and administer epinephrine auto-injectors consistent with their training and the Bureau operations plan. Members should check the auto-injectors at the beginning of their shift to ensure the medication is not expired. Any expired medication should be removed from service in accordance with the Bureau Operations Plan.

Any member who administers an epinephrine auto-injector medication should contact SR 911 as soon as possible and request response by EMS (Health and Safety Code § 1797.197a(b)).

#### **323.10.2 EPINEPHRINE AUTO-INJECTOR REPORTING**

Any member who administers an epinephrine auto-injector should detail its use in an appropriate report.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Medical Aid and Response*

---

The Lieutenant should ensure that the Records Manager is provided enough information for required reporting to the EMS Authority within 30 days after each use (Health and Safety Code § 1797.197a(f)).

Records regarding the acquisition and disposition of epinephrine auto-injectors shall be maintained pursuant to the established records retention schedule but no less than three years (Business and Professions Code § 4119.4(d)).

#### **323.10.3 EPINEPHRINE AUTO-INJECTOR TRAINING**

The Lieutenant should ensure that members authorized to administer epinephrine auto-injectors are provided with initial and refresher training that meets the requirements of Health and Safety Code § 1797.197a(c) and 22 CCR 100027.03.

#### **323.11 FIRST-AID TRAINING**

The Bureau training manager and Human Resource manager should ensure investigators receive initial first-aid training within one year of employment and refresher training every two years thereafter (22 CCR 100026.03; 22 CCR 100027.06).

## Body-Worn Cameras

### 324.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use of a body-worn camera (BWC) by members of this bureau and for the access, use, and retention of bureau BWC media.

The provisions of this policy, including notice, documentation, access, and retention, also apply to other portable audio/video recording devices used by members, where applicable.

This policy does not apply to undercover operations, wiretaps, or eavesdropping (concealed listening devices).

#### 324.1.1 DEFINITIONS

Definitions related to this policy include:

**Activate** - To place a BWC in active mode (also called event mode). In active mode, the BWC records both video and audio.

**BWC media** - The video, audio, and images captured by bureau BWCs and the associated metadata.

**BWC media systems** - Any software, including web-based programs and mobile applications, used by the Bureau to upload/download, store, view, transfer, and otherwise maintain BWC media.

**Deactivate** - To place a BWC in buffering mode (also called ready or pre-event mode). In buffering mode, the BWC records video (without audio) in short, predetermined intervals that are retained only temporarily. However, when a BWC is activated, the interval recorded immediately prior to activation is then stored as part of the BWC media. Deactivate does not mean powering off the BWC.

**Event** - A general term referring to a set of circumstances that may, but does not necessarily, correlate directly to a single public safety incident.

### 324.2 POLICY

It is the policy of the Bureau to use BWCs and BWC media for evidence collection and to accurately document events in a way that promotes member safety and bureau accountability and transparency while also protecting the privacy of members of the public. Tampering with or altering BWC media is a violation of this policy subjects the member to discipline (see Penal Code § 132 and the Personnel Complaints Policy).

### 324.3 RESPONSIBILITIES

#### 324.3.1 BWC COORDINATOR RESPONSIBILITIES

The Bureau of Investigation Chief will delegate certain responsibilities to a BWC coordinator.

The responsibilities of the coordinator include (Penal Code § 832.18):

# Stanislaus County District Attorney's Office

## Policy Manual

### *Body-Worn Cameras*

---

- (a) Serving as a liaison between the Bureau and the BWC manufacturer/distributor and any third-party media storage vendor.
- (b) Developing inventory procedures for issuing and tracking BWC equipment, including properly marking BWCs as property of the Stanislaus County District Attorney's Office (SCDA) and recording the date each BWC is placed into or taken out of service.
- (c) Assisting with troubleshooting and maintenance of BWC equipment and media systems and, when necessary, coordinating the repair or replacement of BWCs.
  - 1. All equipment and system malfunctions and their resolutions should be documented, and maintenance and repair records should be maintained for all BWCs.
- (d) Managing BWC media systems so that:
  - 1. Access is limited to the minimum necessary authorized users and user privileges are restricted to those necessary for the member to conduct assigned bureau duties.
  - 2. Security requirements, such as two-factor authentication and appropriate password parameters, are in place for user credentials.
- (e) Configuring BWC media systems, or developing manual procedures, so that media is appropriately categorized and retained according to the event type tagged by members.
- (f) Retaining audit logs or records of all access, alteration, and deletion of BWC media and media systems, and conducting periodic audits to ensure compliance with applicable laws, regulations, and bureau policy.
- (g) Developing and updating BWC training for members who are assigned a BWC or given access to BWC media systems.
- (h) Coordinating with the SCDA Public Information Officer (PIO) for the following community relations:
  - 1. Provide the public with the notice of the uses of BWCs (e.g. posting on the website or social media pages).
  - 2. Gain insight into community expectations regarding BWC use.
- (i) Coordinating with the Records Manager to (see the Records Bureau and Records Maintenance and Release policies):
  - 1. Determine and apply proper retention periods to BWC media. Agency legal counsel should be consulted in determining retention periods.
  - 2. Develop procedures for the appropriate release of BWC media.
- (j) Coordinating with the Evidence Room to develop procedures for the transfer, storage, and backup of evidentiary BWC media (see the Property and Evidence Policy).
- (k) Establishing a system to prevent tampering with, deleting, or copying recordings, and to ensure chain of custody integrity.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Body-Worn Cameras*

---

- (l) Designating the persons responsible for downloading the recorded data from the BWC.

#### **324.3.2 MEMBER RESPONSIBILITIES**

Every member issued a BWC is responsible for its proper use, safekeeping, and maintenance (Penal Code § 832.18).

At the beginning of each shift or period of BWC use, the member should inspect their assigned BWC to confirm it is charged and in good working order. As part of the inspection, the member should perform a function test by activating the BWC and recording a brief video stating their name, identification number, assignment, and the date and time.

When wearing a tactical ballistic vest, members should wear their assigned BWC at or near chest level and as close to the center of their body as practicable. When not wearing a tactical ballistic vest, members should wear their assigned BWC on their outermost clothing, on their belt or upper garment as close to the center of the body as practicable. Members are responsible for ensuring there are no obstructions and that the BWC remains in a position suitable for recording.

Members should have their BWC accessible while on duty including driving to and from their duty assignment. When a BWC is not in the physical possession of the member to which it is assigned, it should be placed on the charging dock, or charged on a computer via cable, and stored in a secure location.

Members shall report any malfunction or damage to the BWC coordinator or on-duty supervisor as soon as practicable and, if possible, obtain a functioning BWC to use either temporarily while repairs are being made to the member's BWC or as a permanent replacement.

#### **324.4 BWC USE**

The following guidelines apply to the use of BWCs:

- (a) Only bureau-approved BWCs should be used without the express consent of the Chief of Investigations or the authorized designee. Exception: Members assigned to a federal task force are permitted to use issued federal BWCs during federal operations and enforcement.
- (b) BWCs should only be used by the member or members to whom it was issued unless otherwise authorized by a supervisor.
- (c) The use of bureau-issued BWCs shall be strictly limited to bureau-related activities (Penal Code § 832.18). Exception: Members assigned to a task force are permitted to use issued BWCs during any law enforcement related function as outlined in this policy.
- (d) Members shall not use BWCs or BWC media systems for which they have not received prior authorization and appropriate training.
- (e) Members shall immediately report unauthorized access or use of BWCs or BWC media systems by another member to their supervisor or the Chief of Investigations.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Body-Worn Cameras*

---

#### 324.4.1 PROHIBITIONS

BWCs should not be used to record:

- (a) Routine administrative activities of the Bureau that do not involve interactions with the public. Care should be taken to avoid incidentally recording confidential documents that the Bureau has a duty to keep secure (i.e., criminal justice information).
- (b) Areas within the bureau facilities where members have a reasonable expectation of privacy (e.g., locker rooms or dressing areas, breakrooms) unless responding to a call for service or conducting an investigation.
- (c) Conversations of other members without their knowledge.
- (d) When a member is taking an authorized break or otherwise engaged in personal activities.
- (e) In a courtroom unless responding to a call for service or emergency situation.
- (f) Interactions with undercover investigators or confidential informants.
- (g) Strip searches.

BWCs shall not be used for the purpose of embarrassment, harassment, or ridicule of any individual or group.

#### **324.5 ACTIVATION OF BWC**

Members should activate their BWC during the performance of law enforcement-related functions. Members are not required to activate their BWC during casual or informal contacts with members of the public that are not part of or related to law enforcement functions. However, members should activate their BWC any time a contact with an individual becomes hostile or adversarial.

Unless otherwise authorized by this policy or approved by a supervisor, BWCs should remain activated until the law enforcement-related function has concluded. A member may cease recording if they are simply waiting for a return phone call, tow truck, or a family member to arrive, or in other similar situations.

At no time is a member expected to jeopardize their safety to activate their BWC. However, the BWC should be activated as soon as reasonably practicable in required situations.

If a member attempts to activate their BWC but the BWC fails to record an event, the member should notify their supervisor as soon as practicable.

#### 324.5.1 NOTICE OF RECORDING

Unless otherwise approved based on unique circumstances, a member should wear the BWC in a manner that is conspicuous and shall answer truthfully if asked whether they are equipped with a BWC or if their BWC is activated.

#### 324.5.2 PRIVACY CONSIDERATIONS

Members should remain sensitive to the dignity of individuals being recorded and should exercise sound discretion with respect to privacy concerns.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Body-Worn Cameras*

---

Members may mute or deactivate their BWC in the following circumstances:

- (a) To protect the privacy of a juvenile victim or witness..
- (b) When an individual wishes to provide information anonymously.
- (c) To avoid recording a confidential informant or undercover investigator.
- (d) When discussing case tactics or strategy.
- (e) During private conversations with other members or emergency responders.

Members should choose to mute rather than deactivate BWCs when practicable. Deactivation should only be used when muting the BWC will not accomplish the level of privacy necessary for the situation.

Before muting or deactivating their BWC, the member should verbally narrate the reason on the recording. As soon as possible once the privacy concern is no longer an issue, or when circumstances change so that the privacy concern no longer outweighs the bureau's interest in recording the event (e.g., the individual becomes combative, the conversation ends), the member should unmute or reactivate their BWC and verbally note that recording has resumed.

#### 324.5.3 LIVESTREAMING

Livestreaming enables authorized individuals to remotely view the audio and video captured by a member's BWC in real time. Only bureau supervisors approved by the Chief of Investigations shall have access to livestreaming capabilities.

Livestreaming should only be activated:

- (a) For purposes of member safety when the member is not responding to their radio or there is some other indication of distress.
- (b) To assist with situational awareness or tactical decisions during a significant incident.
- (c) When requested by the member.

#### 324.5.4 DOCUMENTATION

Members are encouraged to provide narration while using a BWC when it would be useful to provide context or clarification of the events being recorded. However, the use of a BWC is not a replacement for written reports and should not be referred to in a written report in place of detailing the event.

Every report prepared by a member who is issued a BWC should state whether or not a BWC was used and should document:

- (a) To the extent practicable and relevant, the identity of individuals appearing in the BWC media.
- (b) An explanation of why BWC media is unavailable including any malfunction, damage, or battery issue that resulted in the failure of the BWC to capture all or part of the event.
- (c) Any exigency or other circumstances that prevented the member from immediately activating the recording at the beginning of the event.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Body-Worn Cameras*

---

- (d) Any period of the event in which the member deactivated or muted their BWC and the reason for such action.
- (e) If livestreaming was activated during the event, the reason for livestreaming and the members who communicated or participated in the event through BWC livestreaming.

#### **324.6 DOWNLOADING BWC MEDIA**

Unless otherwise authorized by a supervisor, all media from a member's BWC should be properly downloaded and tagged before the end of their shift. BWC media related to a serious or high-profile event (e.g., search for a missing child, active shooter situation) should be downloaded and tagged as soon as practicable upon returning to the Bureau (Penal Code § 832.18).

Following an officer involved shooting or death or other event deemed necessary, a supervisor should take possession of the BWC for each member present and download and tag the BWC media if the storage system does not have automatic downloading capacity (Penal Code § 832.18).

##### **324.6.1 TAGGING BWC MEDIA**

Members should tag all media captured by providing the agency case number or DA intake number and a brief description of the media. For example, when completing followup (DAIF) any media captured should contain the agency case number in the **ID Box**. If working on an investigation that started out of the Bureau of Investigation, members should list a DA intake number in the **ID box**.

In the **Title Box**, members should list what the media contains. For example, (W) Jones interview, (D) Jones arrest/use of force, Evidence collection assist MPD, Citizen Complaint Jones statement etc.

BWC media should be tagged upon downloading or, if capabilities permit tagging in the field, as close to the time of the event as possible. If more than one event type applies to BWC media, it should be tagged separately.

The Axon View application allows the user to select a **Category**. Members need not select a category when tagging their media. Only the ID (case number or intake number) and Title (description of event) are required when tagging media.

Bureau supervisors should tag BWC media depicting sensitive circumstances or events as restricted. BWC media should be flagged for supervisor review when it pertains to a significant event such as:

- (a) An incident that is the basis of a formal or informal complaint or is likely to result in a complaint.
- (b) When a member has sustained a serious injury or a line-of-duty death has occurred.
- (c) When a firearm discharge or use of force incident has occurred.
- (d) An event that has attracted or is likely to attract significant media attention.

Supervisors should conduct audits at regular intervals to confirm BWC media is being properly downloaded and tagged by their subordinates.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Body-Worn Cameras*

---

#### **324.7 BWC MEDIA**

All BWC media is the sole property of the SCDA (Penal Code § 832.18). Members shall have no expectation of privacy or ownership interest in the content of BWC media.

All BWC media shall be stored and transferred in a manner that is physically and digitally secure with appropriate safeguards to prevent unauthorized modification, use, release, or transfer. Contracts with any third-party vendors for the storage of BWC media should include provisions specifying that all BWC media remains the property of the SCDA and shall not be used by the vendor for any purpose without explicit approval of the Chief of Investigations or the elected District Attorney (Penal Code § 832.18).

Members shall not alter, copy, delete, release, or permit access to BWC media other than as permitted in this policy without the express consent of the Chief of Investigations (Penal Code § 832.18).

BWC media systems should not be accessed using personal devices unless authorized by the Chief of Investigations.

##### **324.7.1 ACCESS AND USE OF BWC MEDIA**

BWC media systems shall only be accessed by authorized members using the member's own login credentials and in accordance with the Information Technology Use Policy.

BWC media shall only be accessed and viewed for legitimate bureau-related purposes in accordance with the following guidelines:

- (a) BWC media tagged as restricted should only be accessible by those designated by a bureau supervisor.
- (b) Members may review their own BWC media for bureau-related purposes. Members should document in their report if they reviewed BWC media before completing the report.
- (c) Investigators may review BWC media pertaining to their assigned cases.
- (d) A member testifying regarding a bureau-related event may review the pertinent BWC media before testifying.
- (e) Supervisors are permitted to access and view BWC media of their subordinates.
  - 1. Supervisors should review BWC media that is tagged as a significant event or that the supervisor is aware pertains to a significant event.
  - 2. Supervisors should conduct documented reviews of their subordinate's BWC media at least annually to evaluate the member's performance, verify compliance with bureau procedures, and determine the need for additional training. The review should include a variety of event types when possible. Supervisors should review BWC media with the recording member when it would be beneficial to provide guidance or to conduct one-on-one informal training for the member.
  - 3. Supervisors should conduct periodic reviews of a sample of each subordinate's BWC media to evaluate BWC use and ensure compliance with this policy.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Body-Worn Cameras*

---

- (f) The Lieutenant is permitted to access and view BWC media for training purposes.
  - 1. The Lieutenant should conduct a quarterly review of a random sampling of BWC media to evaluate bureau performance and effectiveness and to identify specific areas where additional training or changes to protocols would be beneficial. Training Committee members may review BWC media as part of their review to identify training needs.
  - 2. The Lieutenant may use BWC media for training purposes with the approval of the Chief of Investigations. The Lieutenant should use caution to avoid embarrassing or singling out a member and, to the extent practicable, should seek consent from the members appearing in the BWC media before its use for training. When practicable, sensitive issues depicted in BWC media should be redacted before being used for training.
- (g) The bureau support personnel may access BWC media when necessary to conduct bureau-related duties.
- (h) The BWC coordinator may access BWC media and the BWC media system as needed to ensure the system is functioning properly, provide troubleshooting assistance, conduct audits, and fulfill other responsibilities related to their role.

#### **324.7.2 PUBLIC ACCESS**

Unless disclosure is required by law or a court order, BWC media should not be released to the public if it unreasonably violates a person's privacy or sense of dignity or depicts the interior of:

- (a) A private residence.
- (b) A facility that offers health care, mental health or substance abuse treatment, or social services.
- (c) A school building.
- (d) Any other building in which public access is restricted or which implicates heightened security concerns.

Requests for the release of BWC media shall be processed in accordance with the Records Maintenance and Release Policy. A bureau Lieutenant should review BWC media before public release.

#### **324.8 RETENTION OF BWC MEDIA**

Non-evidentiary BWC media should be retained for a minimum of 60 days, after which it may be erased, destroyed, or recycled. Non-evidentiary media may be kept for more than 60 days for availability in case of a civilian complaint and to preserve transparency (Penal Code § 832.18).

Unless circumstances justify continued retention, BWC media should be permanently deleted upon the expiration of the retention period in a way that it cannot be retrieved. BWC media shall not otherwise be deleted by any person without the authorization of the Chief of Investigations.

Records or logs of access and deletion of recordings should be retained permanently (Penal Code § 832.18).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Body-Worn Cameras*

---

#### **324.8.1 EVIDENTIARY BWC MEDIA**

BWC media relevant to a criminal prosecution should be exported from the BWC media system and securely transferred to digital evidence storage according to established bureau procedures. Evidentiary BWC media is subject to the same laws, policies, and procedures as all other evidence, including chain of custody, accessibility, and retention periods (see the Property and Evidence Policy).

Evidentiary BWC media should be retained for a minimum of two years under the following circumstances (Penal Code § 832.18):

- (a) The recording is of an incident involving the use of force by an investigator or an officer-involved shooting.
- (b) The recording is of an incident that leads to the detention or arrest of an individual.
- (c) The recording is relevant to a formal or informal complaint against an investigator or the Stanislaus County District Attorney's Office.

Recordings containing evidence that may be relevant to a criminal prosecution should be retained for any additional period required by law for other evidence relevant to a criminal prosecution (Penal Code § 832.18).

#### **324.9 TRAINING**

The BWC coordinator should ensure that each member issued a BWC receives initial training before use, and periodic refresher training thereafter. Training should include:

- (a) Proper use of the BWC device and accessories.
- (b) When BWC activation is required, permitted, and prohibited.
- (c) How to respond to an individual's request to stop recording.
- (d) Proper use of the BWC media systems, including downloading and tagging procedures.
- (e) Security procedures for BWC media, including appropriate access and use.

Members who are not issued a BWC but who have access to BWC media systems shall receive training on the BWC media system, including appropriate access, use, and security procedures.

## Vehicle Pursuits

### 325.1 PURPOSE AND SCOPE

This policy provides guidelines for vehicle pursuits in order to protect the safety of involved investigators, the public, and fleeing suspects (Vehicle Code § 17004.7).

#### 325.1.1 DEFINITIONS

Definitions related to this policy include:

**Blocking** - A preventive maneuver where emergency vehicles are strategically positioned to prevent a suspect from moving their vehicle, usually before a pursuit starts or at low speeds.

**Boxing-in** - A low-speed tactic designed to stop a fleeing vehicle by surrounding it with emergency vehicles and then slowing all vehicles to a stop.

**Pursuit Intervention Technique (PIT)** - A low-speed tactic designed to apply lateral pressure to the rear quarter panel of a fleeing vehicle, causing it to spin out, stall, and come to a stop (also known as a Precision Immobilization Technique).

**Ramming** - The deliberate act of impacting a fleeing vehicle with another vehicle to functionally damage or otherwise force the fleeing vehicle to stop.

**Roadblock** - A tactic designed to stop a fleeing vehicle by intentionally placing an emergency vehicle or other immovable object in the path of the fleeing vehicle.

**Tire deflation device** - A device designed to be placed on the roadway and puncture the tires of a fleeing vehicle, sometimes referred to as spike strips.

**Vehicle pursuit** - An event involving one or more law enforcement officers attempting to apprehend a suspect who is attempting to avoid arrest while operating a motor vehicle by using high-speed driving or other evasive tactics, such as driving off a highway, turning suddenly, or driving in a legal manner but willfully failing to yield to an investigator's signal to stop.

### 325.2 POLICY

It is the policy of this bureau to balance the need to apprehend a fleeing suspect with the risks associated with vehicle pursuits.

### 325.3 INITIATING A PURSUIT

Criminal Investigators are assigned to and operate undercover emergency vehicles equip with emergency lights and siren. As a general rule, Investigators should avoid initiating or engaging in a pursuit while operating an undercover vehicle. When the need to apprehend a fleeing suspect clearly outweighs the risks of a vehicle pursuit, Investigators who have received appropriate training are authorized to initiate or engage in a vehicle pursuit.

When balancing the risk of a pursuit with the need to apprehend the suspect, investigators shall consider:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Pursuits*

---

- (a) The seriousness of the known or reasonably suspected crime committed by the suspect and the threat to the safety of the public if the suspect remains at large.
- (b) Whether the identity of the suspect is known with enough certainty to enable apprehension at a later time.
- (c) The speed of the vehicles relative to the conditions of the area, such as the population density, amount of vehicular and pedestrian traffic (e.g., school zones), time of day, road conditions, environmental conditions (e.g., hills, curves, mountains), and weather conditions.
- (d) The pursuing investigator's driving capabilities, familiarity with the area, and quality of radio communications with the dispatcher/supervisor.
- (e) The nature of the pursuing unit (e.g., marked vs. unmarked) and its speed and performance capabilities in relation to the fleeing vehicle (e.g., performance motorcycle).
- (f) Whether there are other persons in or on the fleeing vehicle and their relationship to the situation (e.g., passengers, co-offenders, hostages).
- (g) Whether the pursuing unit is carrying passengers other than on-duty investigatorinvestigators. Pursuits should not be undertaken with an arrestee in the pursuit vehicle unless exigent circumstances exist.
- (h) The availability of other resources such as air support or vehicle locator/deactivation technology.

#### **325.4 PURSUIT UNITS**

Vehicle pursuits should be limited to three investigatorbureau emergency vehicles (two pursuit units and the supervisor vehicle). However, an investigator or supervisor may request that additional units join a pursuit if, after assessing the factors outlined above, it reasonably appears that the number of investigators involved may be insufficient to safely arrest the number of suspects.

##### **325.4.1 EMERGENCY EQUIPMENT**

Vehicle pursuits shall only be conducted using authorized investigatorbureau vehicles that are equipped with emergency lighting and sirens as required by Vehicle Code § 21055. Each pursuit unit's emergency lights and sirens should remain activated throughout the unit's participation in the pursuit.

Investigators operating vehicles not equipped with emergency lights and siren are prohibited from pursuing a fleeing vehicle or joining a pursuit. Investigators in such vehicles may provide support to pursuing units when needed, but should operate the vehicle in compliance with all traffic laws and should discontinue such support immediately upon arrival of a sufficient number of authorized emergency vehicles or any air support.

##### **325.4.2 UNMARKED UNITS**

When involved in a pursuit, investigatorbureau unmarked vehicles should be replaced by marked four-wheel emergency vehicles as soon as practicable.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Pursuits*

---

#### 325.4.3 PRIMARY UNIT

The initial pursuing investigator should be designated as the primary unit and will be responsible for the conduct of the pursuit unless that unit is unable to remain reasonably close to the suspect's vehicle. The primary responsibility of the investigator initiating the pursuit is the apprehension of the suspect without unreasonable danger to themselves or others.

As soon as practicable, the primary unit should notify SR 911 of the pursuit, request priority radio traffic, and provide appropriate information including:

- (a) The location, direction of travel, and estimated speed of the pursuit.
- (b) The description of the fleeing vehicle, including the license plate number, if known.
- (c) The reason for the pursuit.
- (d) A description of the fleeing vehicle's evasive driving behavior (e.g., rapid lane changes, no headlights, driving on the wrong side of the road).
- (e) Known or suspected weapons, threat of force, violence, injuries, hostages, or other unusual hazards.
- (f) The suspected number of occupants and their identities or descriptions.
- (g) The weather, road, and traffic conditions.
- (h) The need for any additional resources or equipment.
- (i) The identities of other law enforcement agencies involved in the pursuit.

The primary unit is responsible for broadcasting the progress of the pursuit until a secondary or air unit joins the pursuit. Once an additional unit joins the pursuit, the primary unit should relinquish the responsibility of broadcasting the progress to the secondary or air unit unless circumstances reasonably indicate otherwise.

#### 325.4.4 SECONDARY UNIT

The second investigator in the pursuit should be designated as the secondary unit and is responsible for:

- (a) Notifying SR 911 of their entry into the pursuit.
- (b) Broadcasting the progress of the pursuit, updating known or critical information, and providing changes in the pursuit, unless the situation indicates otherwise.
- (c) Identifying the need for and requesting additional resources or equipment as appropriate.
- (d) Serving as backup to the primary unit once the fleeing vehicle has been stopped.

#### 325.4.5 AIR UNITS

When available, air unit assistance should be requested. The air unit should assume responsibility of broadcasting the pursuit once they have established visual contact with the fleeing vehicle. Ground units should maintain operational control and consider whether the continued close proximity and/or involvement in the pursuit is warranted.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Pursuits*

---

The air unit should coordinate the activities of resources on the ground, report progress of the pursuit, and provide pursuing units with details of upcoming traffic congestion, road hazards, or other information pertinent to evaluating whether to continue the pursuit. If ground units are not within visual contact of the fleeing vehicle and the air unit determines that it is unsafe to continue the pursuit, the air unit should recommend termination.

#### **325.5 PURSUIT DRIVING**

The decision to use specific driving tactics requires consideration of the same factors as initiating a pursuit. In addition, investigators involved in the pursuit should adhere to the following:

- (a) Pursuing units should space themselves far enough from other involved vehicles to be able to see and avoid hazards and react safely to maneuvers by the fleeing vehicle.
- (b) Pursuing units should exercise caution and slow down as necessary when proceeding through intersections.
- (c) Pursuing units should not follow a fleeing vehicle driving against traffic (wrong way) and should instead:
  - 1. Request assistance from available air support.
  - 2. Maintain visual contact with the fleeing vehicle by paralleling it on the correct side of the roadway.
  - 3. Request other units to observe exits available to the fleeing vehicle.
- (d) Pursuing units should request that SR 911 notify the California Highway Patrol (CHP) and/or another law enforcement agency if it appears that the pursuit may enter its jurisdiction.
- (e) Pursuing units should not attempt to pass other pursuit units unless the situation indicates otherwise or they are requested to do so. Passing another pursuit unit should only be attempted with a clear understanding of the maneuver.

##### **325.5.1 RULES OF THE ROAD**

The speed of a vehicle pursuit is a factor that should be evaluated on a continuing basis by the investigator and supervisor. Evaluation of vehicle speeds should take into consideration public safety, officer safety, and the safety of the occupants of the fleeing vehicle.

Should high vehicle speeds be reached during a pursuit, investigators and supervisors should also consider these factors when determining the reasonableness of the speed of the pursuit:

- (a) Pursuit speeds have become unreasonably unsafe for the surrounding conditions.
- (b) Pursuit speeds have exceeded the driving ability of the investigator.
- (c) Pursuit speeds are beyond the capabilities of the pursuit vehicle, thus making its operation unsafe.

##### **325.5.2 INVESTIGATORS NOT INVOLVED IN THE PURSUIT**

Investigators not directly involved in the pursuit should stay alert to its progress and location and may proceed safely to intersections ahead of the pursuit to warn cross traffic. When clearing



# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Pursuits*

---

intersections along the pursuit path, investigators are authorized to use emergency equipment and should attempt to place their vehicles in locations that provide some safety or an escape route in the event of an unintended collision or a suspect intentionally trying to ram the investigator's vehicle.

Other than clearing intersections along the pursuit path, uninvolved investigators should avoid operating under emergency conditions (emergency lights and siren) and should remain in their assigned areas unless directed otherwise by a supervisor.

When needed, non-pursuing investigators and investigators who have dropped out of the pursuit should respond to the pursuit termination point in a non-emergency manner, observing the rules of the road. Investigators should not parallel the pursuit route.

#### **325.6 SUPERVISORY CONTROL AND RESPONSIBILITIES**

The supervisor of the investigator initiating the pursuit, or if unavailable, the nearest supervisor, will be responsible for:

- (a) Immediately notifying the involved units and the dispatcher of supervisory presence and ascertaining all reasonably available information in order to continuously assess the situation and risk factors associated with the pursuit.
- (b) Exercising management and control of the pursuit and, when appropriate, engaging in the pursuit to provide on-scene supervision.
- (c) Confirming that no more pursuing units than required are involved in the pursuit.
- (d) Directing that the pursuit be terminated if, in the supervisor's judgment, continuing the pursuit is not justified under the guidelines of this policy.
- (e) Assessing the emotional state of the investigators involved and directing an investigator to disengage from the pursuit if it appears they are unable to control their emotions.
- (f) Requesting additional assistance from air support, canines, or other resources, if available and appropriate.
- (g) Verifying that the proper radio channel is being used.
- (h) Confirming the Lieutenant has been notified of the pursuit.
- (i) Overseeing the notification and/or coordination of outside agencies if the pursuit leaves or is likely to leave the jurisdiction of this bureau.
- (j) Continuing the management and control of Stanislaus County District Attorney's Office units when a pursuit enters another jurisdiction.
- (k) Preparing documentation of the pursuit and conducting a post-pursuit review, as required.

#### **325.7 SR 911**

Radio communications during a pursuit should be conducted on the primary channel unless instructed otherwise by a supervisor or dispatcher. If the pursuit leaves the jurisdiction of

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Pursuits*

---

this bureau or such is imminent, involved units should, whenever available, switch radio communications to a tactical or emergency channel most accessible by participating agencies.

#### **325.7.1 SR 911 RESPONSIBILITIES**

Upon notification or becoming aware that a pursuit has been initiated, the dispatcher is responsible for:

- (a) Clearing the radio channel of non-emergency traffic.
- (b) Coordinating pursuit communications of the involved units and personnel.
- (c) Broadcasting pursuit updates as well as other pertinent information as necessary.
- (d) Ensuring that a field supervisor is notified of the pursuit.
- (e) Notifying and coordinating with other involved or affected agencies as practicable.
- (f) Notifying the Lieutenant as soon as practicable.
- (g) Assigning an incident number and logging all pursuit activities.

#### **325.8 INTERJURISDICTIONAL CONSIDERATIONS**

Unless entry into another jurisdiction is expected to be brief, the primary unit or supervisor should ensure that notification is provided to each outside jurisdiction into which the pursuit is reasonably expected to enter, regardless of whether such jurisdiction is expected to assist.

##### **325.8.1 ASSUMPTION OF PURSUIT BY ANOTHER AGENCY**

When a pursuit enters another agency's jurisdiction, the primary unit or the supervisor should determine whether to request the other agency assume the pursuit, taking into consideration the distance traveled, familiarity with the area, and other pertinent facts.

Once another agency has agreed to assume the pursuit, pursuing units should relinquish control and discontinue participation unless the continued assistance of the Stanislaus County District Attorney's Office is requested by the agency assuming the pursuit. Upon relinquishing control of the pursuit, the involved investigators may, with supervisory approval, proceed to the termination point in order to provide information and assistance for the arrest of the suspect and reporting of the incident. The supervisor should coordinate such assistance with the assuming agency and obtain any information that is necessary for bureau reports.

##### **325.8.2 PURSUITS EXTENDING INTO THIS JURISDICTION**

Investigators from this bureau should not join a pursuit being conducted by another agency unless specifically requested to do so by that agency and with approval from a supervisor.

When a request is made for this bureau to assist or take over a pursuit that has entered the jurisdiction of the Stanislaus County District Attorney's Office, the Lieutenant should review the request as soon as practicable, taking into consideration:

- (a) Whether the need to apprehend the fleeing suspect outweighs the risks of the pursuit to investigators and the public.
- (b) Whether there is adequate staffing to continue the pursuit.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Pursuits*

---

- (c) The available units' capabilities to maintain the pursuit.
- (d) The number of available units and other resources of the pursuing agency.

Assistance to a pursuing agency by investigators of this bureau should terminate at the County limits, provided that the pursuing agency has sufficient assistance from other sources. Ongoing participation from this bureau should continue only until sufficient assistance is present.

In the event that a pursuit from another agency terminates within this jurisdiction, investigators should provide appropriate assistance to the pursuing agency such as scene control, inter-agency coordination, completion of supplemental reports, and any other reasonable assistance requested or needed.

### **325.9 PURSUIT INTERVENTION**

Pursuit interventions should only be used when it reasonably appears that using the intervention will contain or prevent the pursuit, and the need to immediately stop the fleeing vehicle outweighs the risks of injury or death to investigators and others.

Pursuit interventions may be construed as a use of force, including deadly force, and are subject to the policies guiding such use. Investigators should consider the guidelines for the use of force when deciding how, when, where, and if a pursuit intervention should be employed. Refer to the Use of Force Policy for additional guidance.

Whenever practicable, an investigator should seek approval from a supervisor before employing any pursuit intervention to stop a fleeing vehicle. Investigators should not attempt a pursuit intervention unless they have received the appropriate training for the intervention being used.

#### **325.9.1 TIRE DEFLATION DEVICE**

Before deploying a tire deflation device, investigators should consider factors such as:

- (a) Speed of the fleeing vehicle - Traveling at high speeds increases the risk the suspect will lose control of the vehicle after driving over or swerving to avoid a tire deflation device.
- (b) Weather and visibility - Tire deflation devices should only be deployed when the location, weather, and other conditions allow the deploying investigator to clearly see the fleeing vehicle, pursuit units, and other approaching traffic.
- (c) Cover - Deployment should occur in a location that provides the deploying investigator adequate cover and escape from intentional or unintentional exposure to the approaching vehicles.
- (d) Road conditions - Soft or loose material such as dirt or gravel may prevent a tire deflation device from puncturing the vehicle's tire. Deploying the device on loose pavement or icy or wet roads increases the risk of the suspect losing control of the vehicle.
- (e) Characteristics of the deployment area - A tire deflation device should not be deployed in areas that are heavily populated with pedestrians, at times of heavy traffic, or at a location where there is a heightened chance of striking a fixed object.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Pursuits*

---

- (f) Characteristics of the fleeing vehicle - Except in extraordinary circumstances, a tire deflation device should not be used when the fleeing vehicle is a motorcycle or other vehicle with fewer than four wheels, an ATV, a vehicle transporting hazardous materials, or a school bus transporting children.

Because of the risks to deploying investigators, the intent to deploy a tire deflation device and its location should be clearly communicated to the dispatcher and all involved units.

#### 325.9.2 PIT

A PIT should only be attempted with marked police vehicles equip with a reinforced bumpers. Investigators operating unmarked emergency vehicles are not permitted to perform a PIT on a fleeing vehicle.

#### 325.9.3 BOXING-IN OR BLOCKING

Boxing-in or blocking should only be used when the suspect's vehicle is stopped or traveling at a low speed.

Boxing-in requires the participation of multiple units and therefore must be carefully coordinated with all involved.

#### 325.9.4 RAMMING AND ROADBLOCKS

Ramming and roadblocks shall only be used when deadly force is warranted and all other reasonable alternatives have been exhausted or reasonably appear ineffective.

#### 325.9.5 FIREARMS

Specific guidance on the use of a firearm during a vehicle pursuit is addressed in the Use of Force Policy.

### **325.10 TERMINATING A PURSUIT**

The factors considered when initiating a pursuit should be continually reevaluated by pursuing units during the pursuit, as the circumstances and conditions change, and as new information becomes available. If at any time the risk of continuing the pursuit outweighs the need to immediately apprehend the suspect, the pursuit should be terminated.

In addition, a pursuit should be terminated when:

- (a) A supervisor directs the pursuit to be terminated.
- (b) The location of the fleeing vehicle is no longer known.
- (c) The distance between the pursuing units and the fleeing vehicle is so great that further pursuit would be futile or would continue for an unreasonable time and/or distance.
- (d) The pursuing unit sustains damage or a mechanical failure that makes it unsafe to drive or renders the emergency lighting and sirens partially or completely inoperable and there are no additional units readily available to take over the pursuit.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Pursuits*

---

When a pursuit terminates for any reason, all pursuit units should verbally acknowledge termination, turn off emergency lights and sirens, reduce their speed, and obey all traffic laws. The primary unit should communicate the location of pursuit termination to the dispatcher.

#### **325.10.1 LOSS OF PURSUED VEHICLE**

When a pursuit is terminated because the location of the fleeing vehicle is no longer known, the primary unit should broadcast pertinent information for other units to assist in locating the suspect. The primary unit or supervisor will be responsible for coordinating any further search for the pursued vehicle.

#### **325.10.2 APPREHENSION OF SUSPECTS**

Investigators should exercise proper self-discipline and sound professional judgment at the conclusion of a pursuit and while apprehending the suspect.

Unless otherwise directed by a supervisor, an investigator other than the primary unit should coordinate efforts to apprehend the suspect following the pursuit.

Any use of force necessary to apprehend the suspect shall be consistent with the Use of Force Policy.

#### **325.11 DEBRIEFING**

Participating investigators should return to the Bureau as soon as practical following a pursuit to debrief with a supervisor.

#### **325.12 REPORTING REQUIREMENTS**

Appropriate reports should be completed as required by applicable laws, policies, and procedures.

- (a) Pursuing investigators should complete appropriate crime/arrest and pursuit reports.
- (b) The involved Lieutenant shall obtain available information and promptly complete a written post-pursuit review to the Chief of Investigations. The post-pursuit should summarize the pursuit and include, at a minimum:
  - 1. Date and time of the pursuit.
  - 2. Reason and circumstances surrounding the pursuit (e.g., seriousness of the crime, road and traffic conditions, speed and driving behavior of the fleeing vehicle) that warranted initiation and continuation of the pursuit.
  - 3. Length of pursuit in distance and time, including the starting and termination points.
  - 4. Involved vehicles and investigators.
  - 5. Alleged offenses.
  - 6. Whether a suspect was apprehended, as well as the means and methods used.
  - 7. Arrestee information, if applicable.
  - 8. Any injuries and/or medical treatment.
  - 9. Any property or equipment damage.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Pursuits*

---

10. Name of supervisor at the scene or who handled the incident.
11. Identified training issues.
12. Findings and conclusion (determination whether the pursuit was within or out of policy)

Post-pursuit reviews will be used for annual analysis of bureau vehicle pursuits to minimally include policy suitability, policy compliance, and training or equipment needs. The review should not contain the names of investigators, suspects, or case numbers.

#### **325.12.1 STATE-SPECIFIC REPORTING REQUIREMENTS**

The Lieutenant shall ensure that an Allied Agency Vehicle Pursuit Report (form CHP 187A) is filed with the CHP not later than 30 days following the pursuit (Vehicle Code § 14602.1). The primary investigator should complete as much of the required information on the form as is known and forward the report to the Lieutenant for review and distribution.

#### **325.13 PURSUIT TRAINING**

The Lieutenant should ensure that members of this bureau receive initial and annual training on this policy and vehicle pursuits relevant to their role (e.g., investigators, supervisors, air units, dispatchers).

Investigator training should address decision-making involved in initiating, continuing, and terminating a pursuit by balancing the need to apprehend the suspect with the risk of a pursuit. Subject to available resources, training on pursuit driving and the deployment of pursuit intervention tactics should include scenario-based training and behind-the-wheel practice, in addition to classroom instruction.

#### **325.13.1 STATE-SPECIFIC TRAINING REQUIREMENTS**

The Lieutenant shall make available to all investigators initial and supplementary POST training on pursuits required by Penal Code § 13519.8, Vehicle Code § 17004.7(d), and 11 CCR 1081, and no less than annual training addressing:

- (a) This policy.
- (b) The importance of vehicle safety and protecting the public.
- (c) The need to balance the known offense and the need for immediate capture against the risks to investigators and others.

#### **325.14 POLICY ACKNOWLEDGEMENT**

Investigators of this bureau shall certify in writing that they have received, read, and understand this policy initially, upon any amendments, and whenever training on this policy is provided. The POST attestation form, or an equivalent form, may be used to document the compliance and should be retained in the member's training file.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Pursuits*

---

#### **325.15 APPLICATION OF VEHICLE PURSUIT POLICY**

This policy is expressly written and adopted pursuant to the provisions of Vehicle Code § 17004.7, with additional input from the POST Vehicle Pursuit Guidelines.

## ADA Compliance

### 326.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for equal access to Stanislaus County District Attorney's Office services, programs, and activities for persons with disabilities, in accordance with Title II of the Americans with Disabilities Act (ADA).

This policy also includes guidelines to provide effective communication with persons with disabilities. See the Service Animals Policy for guidance on protecting the rights of individuals who use service animals in accordance with the ADA.

#### 326.1.1 DEFINITIONS

Definitions related to this policy include (28 CFR 35.104):

**ADA coordinator** - The member designated by the District Attorney to coordinate the bureau's efforts to comply with the ADA (28 CFR 35.107).

**Assistive devices, auxiliary aids, and services** - Tools used by persons with disabilities to facilitate their participation in services, programs, and activities offered by the Stanislaus County District Attorney's Office and to facilitate effective communication. They include but are not limited to the use of gestures or visual aids to supplement oral communication; a notepad and pen or pencil to exchange written notes; a computer or typewriter; an assistive listening system or device to amplify sound; a teletypewriter (TTY) or videophones (video relay service or VRS); taped text; a qualified reader; or a qualified interpreter.

**Disability** - A physical or mental impairment that substantially limits a major life activity including hearing, seeing, or speaking, regardless of whether the person uses assistive devices, auxiliary aids, and services. Individuals who wear ordinary eyeglasses or contact lenses are not considered to have a disability (42 USC § 12102; 28 CFR 35.108).

**Facility** - All aspects of bureau buildings, structures, sites, complexes, equipment, rolling stock or other conveyances, roads, walkways, parking areas, and other real or personal property (28 CFR 35.108).

**Modification** - Any change, adjustment, alteration, adaptation, or accommodation that renders a bureau service, program, or activity suitable for use, enjoyment, or participation by a person with a disability. This may include alteration of existing buildings and facilities.

A modification includes any change or exception to a policy, practice, or procedure that allows a person with a disability to have equal access to services, programs, and activities. It also includes the provision or use of assistive devices, auxiliary aids, and services.

**Qualified interpreter** - A person who is able to interpret effectively, accurately, and impartially, both receptively and expressively, using any necessary specialized vocabulary. Qualified interpreters include oral interpreters, transliterators, sign language interpreters, and intermediary interpreters.



# Stanislaus County District Attorney's Office

## Policy Manual

### *ADA Compliance*

---

#### **326.2 POLICY**

It is the policy of the Stanislaus County District Attorney's Office that persons with disabilities, including victims, witnesses, suspects, and arrestees, have equal access to services, programs, and activities of the Bureau.

The Bureau will not discriminate against or deny any individual access to services, programs, or activities based upon the presence or suspected presence of disabilities.

#### **326.3 ADA COORDINATOR RESPONSIBILITIES**

The responsibilities of the ADA coordinator include but are not limited to (28 CFR 35.130):

- (a) Collaborating with the County ADA coordinator regarding the Stanislaus County District Attorney's Office's efforts to provide equal access to services, programs, and activities.
  - 1. Maintaining bureau compliance with accessibility standards for bureau web content and mobile applications as required by 28 CFR 35 Subpart H (28 CFR 35.200).
- (b) Collaborating with the County ADA coordinator to facilitate a process of periodic self-evaluation. The process should include:
  - 1. Inspection of current bureau facilities to identify access issues.
  - 2. Review of current bureau services, activities, and programs for access issues.
  - 3. Assessment and update, if necessary, of current compliance measures.
  - 4. Identification of recurring areas of complaint for which new methods of modification should be considered.
  - 5. Review of the bureau's emergency programs, services, and activities as they apply to persons with disabilities.
  - 6. Recommendation of a schedule to implement needed improvements.
- (c) Acting as a liaison with local disability advocacy groups or other disability-focused groups regarding access to bureau services, programs, and activities.
- (d) Developing procedures that will enable members to access assistive devices, auxiliary aids, and services, and making the procedures available as appropriate.
  - 1. A list of qualified interpreter services with contact and availability information should be maintained and easily accessible to members.
- (e) Developing procedures for the review and processing of requests for modifications that will help members provide persons with disabilities access to bureau services, programs, and activities, as appropriate.
- (f) Establishing procedures for the booking process to assist members with managing commonly encountered disabilities such as sight or mobility impairments and intellectual or developmental disabilities.
- (g) Providing notice to the public regarding the rights and protections afforded by the ADA. This may include posters, published notices, handbooks, manuals, and pamphlets.

# Stanislaus County District Attorney's Office

## Policy Manual

### ADA Compliance

---

describing bureau services, programs, and activities and the availability of assistive devices, auxiliary aids, and services, as well as modifications (28 CFR 35.106).

- (h) Collaborating with other county departments during the planning process to provide that new construction and any alteration to an existing building or facility are undertaken in compliance with the ADA (28 CFR 35.151).
- (i) Developing, implementing, and publishing appropriate procedures to provide for the prompt and equitable resolution of complaints and inquiries regarding discrimination in access to services, programs, and activities. The complaint procedures should include an appeal process (28 CFR 35.107).
- (j) Verifying that third parties providing bureau services, programs, or activities through contract, outsourcing, licensing, or other arrangement have established reasonable policies and procedures to prevent discrimination against and denial of access to persons with disabilities.
- (k) Recommending amendments to this policy as needed.

#### **326.4 REQUESTS**

The goal of any modification should be to allow a person with a disability to participate in a service, program, or activity the same as a person who does not have a disability.

Upon receiving a request for a modification, members should make reasonable efforts to accommodate the request based on the preference of the person with the disability. Members should not ask about the nature and extent of a person's disability but should limit questions to elicit information necessary to determine the need for a modification and the appropriate type of modification.

If the requested modification or an alternative modification can reasonably be made at the time of the request, the member should make the modification. A member who is unable to accommodate a request or unsure about whether a request should be accommodated should contact a supervisor.

The supervisor should review and approve the request, if practicable and appropriate. Otherwise, the supervisor should document the requesting person's contact information and the modification being requested and forward the request to the ADA coordinator for processing as soon as reasonably practicable.

##### **326.4.1 DENIAL OF A REQUEST**

The following should be considered before denying a request for modification:

- (a) Requests for modifications should be approved unless complying with the request would result in (28 CFR 35.150):
  - 1. A substantial alteration of the service, program, or activity.
  - 2. An undue financial or administrative burden on the Bureau. All resources available for use in the funding and operation of the service, program, or activity at issue should be considered in this determination.

# Stanislaus County District Attorney's Office

## Policy Manual

### ADA Compliance

---

3. A threat to or the destruction of the historic significance of a historic property.
  4. A direct threat to the health or safety of others (28 CFR 35.139).
- (b) If any of these circumstances are present, the ADA coordinator should work with bureau members and the person requesting the modification to determine if an alternative modification is available.
- (c) Where new construction or physical modification of an existing building or facility would be unfeasible or unduly burdensome, the ADA coordinator should work with bureau members to determine whether alternative modifications are available. Alternative methods that should be considered include (28 CFR 35.150):
1. Reassigning services, programs, or activities to accessible buildings or facilities.
  2. Utilizing technology, equipment, rolling stock, or other conveyances.
  3. Delivering the services, programs, or activities directly to a person with a disability by way of home visits or meeting the person at an accessible location.
  4. Any other means or methods that would make services, programs, or activities readily accessible.
- (d) If no alternative modification is appropriate, the ADA coordinator shall issue a written statement explaining why a modification of the service, program, or activity will not be made (28 CFR 35.150).

#### 326.4.2 PERSONAL DEVICES AND ASSISTANCE

Although members should make every effort to comply with requests, the provision of personal devices or assistance (e.g., wheelchairs, eyeglasses, hearing aids, personal assistance in eating or using the restroom) to persons with disabilities is not required (28 CFR 35.135).

#### 326.4.3 SURCHARGES

Surcharges shall not be imposed upon persons with disabilities to cover the costs of providing modifications (28 CFR 35.130(f)).

#### 326.5 COMMUNICATIONS WITH PERSONS WITH DISABILITIES

Members should remain alert to the possibility of communication problems when engaging with persons with disabilities. When a member knows or suspects an individual requires assistance to effectively communicate, the member should identify the individual's choice of assistive devices, auxiliary aids, and services. The individual's preferred communication method should be honored unless another effective method of communication exists under the circumstances (28 CFR 35.160).

Factors to consider when determining whether an alternative method may be effective include:

- (a) The methods of communication usually used by the individual.
- (b) The nature, length, and complexity of the communication involved.
- (c) The context of the communication.

# Stanislaus County District Attorney's Office

## Policy Manual

### ADA Compliance

---

In emergency situations involving an imminent threat to the safety or welfare of any person, members may use whatever modification reasonably appears effective under the circumstances. This may include exchanging written notes or using the services of a person who knows sign language but is not a qualified interpreter, even if the person who is deaf or hard of hearing would prefer a qualified sign language interpreter. Once the emergency has ended, the method of communication should be reconsidered. The member should inquire as to the individual's preference and give primary consideration to that preference.

#### 326.5.1 TYPES OF ASSISTANCE AVAILABLE

Bureau members shall not refuse an available type of assistive device, auxiliary aid, or service to a person with a disability who is requesting assistance. The Bureau will not require persons with disabilities to furnish their own assistive device, auxiliary aid, or service as a condition for receiving access to bureau services, programs, and activities. The Bureau will make every reasonable effort to provide equal access and timely assistance to persons with disabilities through a variety of assistive devices, auxiliary aids, and services (28 CFR 35.160).

The Bureau will not require that persons with disabilities use bureau-provided assistive devices, auxiliary aids, and services. Bureau-provided assistive devices, auxiliary aids, and services may include but are not limited to the means described in this policy.

#### 326.5.2 AUDIO RECORDINGS AND ENLARGED PRINT

The Bureau may develop audio recordings to assist people who are blind or have a visual impairment. If such a recording is not available, members may read aloud from the appropriate form or provide forms with enlarged print.

#### 326.5.3 QUALIFIED INTERPRETERS

A qualified interpreter may be needed in lengthy or complex transactions (e.g., interviewing a victim, witness, suspect, or arrestee) with individuals who normally rely on sign language or speechreading (i.e., lip-reading) to understand what others are saying. The qualified interpreter should not be a person with an interest in the matter. A person providing interpretation services may be required to establish the accuracy and trustworthiness of the interpretation in a legal proceeding.

Qualified interpreters should be:

- (a) Available within a reasonable amount of time.
- (b) Experienced in providing interpretation services related to law enforcement matters in the person's primary language.
- (c) Familiar with the use of text- and video-based communications products and systems.
- (d) Certified in either American Sign Language (ASL) or Signing Exact English (SEE).
- (e) Able to understand and adhere to the interpreter role without deviating into other roles, such as counselor or legal adviser.
- (f) Knowledgeable of the ethical issues involved when providing interpreter services.

# Stanislaus County District Attorney's Office

## Policy Manual

### *ADA Compliance*

---

Members should use bureau-approved procedures to request a qualified interpreter at the earliest reasonable opportunity or when it is reasonably apparent that an interpreter is needed. The use of a video remote interpreting service should be considered, where appropriate, if a live interpreter is not available. Persons with disabilities shall not be required to provide an interpreter (28 CFR 35.160).

#### **326.5.4 TELECOMMUNICATION SERVICES**

In situations where an individual without a disability would have access to a telephone (e.g., during booking or attorney contacts), members must also provide those with communication-related disabilities the opportunity to place calls using an available TTY, TDD, or other voice, text, or video-based communications product or system. Members shall provide additional time, as needed, for effective communication due to the slower nature of assisted communications.

The Bureau will accept all TDD and computer modem calls placed by individuals with communications-related disabilities and received via a telecommunications relay service (28 CFR 35.162).

#### **326.5.5 COMMUNITY VOLUNTEERS**

Where qualified interpreters are unavailable to assist members, bureau-approved community volunteers who have demonstrated competence in communication services, such as ASL or SEE, may be called upon to provide interpreter services when appropriate. However, bureau members must carefully consider the nature of the interaction and the relationship between the individual with the disability and the volunteer to be reasonably satisfied that the volunteer can provide neutral and unbiased assistance.

#### **326.5.6 FAMILY AND FRIENDS**

While family or friends may offer to assist with interpretation, members should carefully consider the circumstances before relying on such individuals. The nature of the interaction and relationship between the individual with the disability and the person offering services must be carefully considered to determine whether the family member or friend can provide neutral and unbiased assistance.

Except in an emergency involving an imminent threat to the safety or welfare of any person and no qualified interpreter is reasonably available, members shall not use a minor child as an interpreter (28 CFR 35.160).

#### **326.5.7 FIELD ENFORCEMENT CONSIDERATIONS**

Due to the unpredictable and varied nature of field enforcement, the Bureau recognizes that it is impracticable to provide immediate access to a comprehensive supply of assistive devices, auxiliary aids, and services to every member of this bureau. Members involved in interactions with persons with disabilities that occur in the field should assess each situation to determine if communication assistance is necessary. The length, complexity, and importance of the communication, as well as the individual's preferred method of communication, should be

### ADA Compliance

---

considered when determining what, if any, resources should be used and whether a qualified interpreter or other service is needed.

#### 326.5.8 WITNESS OR VICTIM INTERVIEWS

Members who interview a witness or victim who demonstrates or states they are deaf or have a hearing loss shall make a good faith effort to secure the services of an interpreter without any unnecessary delay, unless the individual affirmatively indicates they do not need or cannot use an interpreter (Evidence Code § 754).

#### 326.6 CUSTODIAL INTERROGATIONS

In an effort to ensure that the rights of individuals with disabilities are protected during a custodial interrogation, this bureau will provide reasonable modifications before beginning an interrogation, unless exigent circumstances exist or the individual has made a clear indication that the individual understands the process and desires to proceed without receiving a modification. *Miranda* warnings should be provided to a suspect via the individual's preferred method of communication.

Interrogations should be recorded whenever reasonably practicable. See guidance on recording custodial interrogations in the Investigation and Prosecution Policy.

#### 326.7 ARREST

If an individual with a communication-related disability is arrested, the arresting investigator shall use bureau-approved procedures to provide a qualified interpreter as soon as reasonably practicable, unless the individual indicates a preference for a different assistive device, auxiliary aid, or service, or the investigator reasonably determines another effective method of communication exists under the circumstances.

Individuals who are arrested and are assisted by service animals should be permitted to make arrangements for the care of such animals prior to transport.

#### 326.8 WEBSITE ACCESS

The ADA coordinator should work with the appropriate parties to develop online content that is readily accessible to persons with disabilities. Bureau web content should be developed in conformance with the most current guidelines issued by the U.S. Department of Justice and federal regulations (28 CFR 35 Subpart H; 28 CFR 35.200).

Bureau website content should also be made available to persons with disabilities in an alternative format upon request, if reasonably practicable.

#### 326.9 DOCUMENTATION

Whenever any modification has been provided, the member involved should document:

- (a) The type of modification, assistive device, auxiliary aid, or service provided.
- (b) Whether the individual elected to use an assistive device, auxiliary aid, or service provided by the Bureau or another identified source, as applicable.

# Stanislaus County District Attorney's Office

## Policy Manual

### *ADA Compliance*

---

- (c) Whether the individual's express preference for the modification was not honored and the reason why an alternative method was used.

The documentation and any written communications exchanged should be maintained consistent with the Records Maintenance and Release Policy.

All written communications exchanged in a criminal case shall be attached to the member's report or placed into evidence.

#### **326.10 COMPLAINTS**

A member who receives a complaint or becomes aware of potential disability discrimination, an ADA violation, or a person's inability to access the bureau's programs, services, or activities should document the complaint and promptly refer the matter to the ADA coordinator (28 CFR 35.107). The Bureau shall assist persons with disabilities who require assistance to file a complaint regarding members of this bureau. The Bureau may provide a qualified interpreter or forms in enlarged print, as appropriate.

#### **326.11 TRAINING**

Members should receive periodic training on ADA compliance, to include:

- (a) Awareness and understanding of this policy, related procedures, forms, and available resources.
- (b) Procedures for handling requests for modifications.
- (c) Accessing assistive devices, auxiliary aids, and services needed to accommodate requests for modifications.
- (d) General requirements of the ADA, including modifying policies and practices, communicating with individuals with disabilities, and identifying alternate ways to provide access to programs, services, and activities as appropriate to the member's job duties.

Management staff, even if they do not interact regularly with individuals with disabilities, should receive training as appropriate to understand and reinforce this policy.

The Lieutenant should maintain records of all training provided and retain a copy in each member's training file in accordance with the established records retention schedule.

## **Chapter 4 - Investigations**



## Outside Agency Assistance

### 400.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members when requesting or responding to a request for mutual aid or when assisting another law enforcement agency.

### 400.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to promptly respond to requests for assistance by other law enforcement agencies, subject to available resources and consistent with the applicable laws and policies of this bureau.

### 400.3 ASSISTING OUTSIDE AGENCIES

Generally, requests for any type of assistance from another agency should be routed to the Chief Investigator's office for approval. In some instances, a memorandum of understanding or other established protocol may exist that eliminates the need for approval of individual requests.

When another law enforcement agency requests assistance from this bureau, a Lieutenant may authorize, if available, an appropriate number of personnel to assist. Members are reminded that their actions when rendering assistance must conform with applicable laws and be consistent with the policies of this bureau.

Investigators may respond to a request for emergency assistance, however, they shall notify a lieutenant of their activity as soon as practicable.

Arrestees may be temporarily detained by this bureau until arrangements for transportation are made by the outside agency. Probation violators who are temporarily detained by this bureau will not ordinarily be booked at this bureau. Only in exceptional circumstances, and subject to supervisor approval, will this bureau provide transportation of arrestees to other facilities on behalf of another agency.

When transportation assistance is rendered, a report shall be prepared and submitted by the handling member unless otherwise directed by a supervisor.

#### 400.3.1 INITIATED ACTIVITY

Any on-duty investigator who engages in law enforcement activities of any type that are not part of a mutual aid request and take place outside the jurisdiction of the Stanislaus County District Attorney's Office shall notify his/her lieutenant and SR 911 as soon as practicable. This requirement does not apply to special enforcement details or multi-agency units that regularly work in multiple jurisdictions.

### 400.4 REQUESTING OUTSIDE ASSISTANCE

If assistance is needed from another agency, the member requesting assistance should, if practicable, first notify a supervisor. The handling member or supervisor should direct assisting personnel to where they are needed and to whom they should report when they arrive.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Outside Agency Assistance*

---

The requesting member should arrange for appropriate radio communication capabilities, if necessary and available, so that communication can be coordinated between assisting personnel.

# Investigation and Prosecution

## 401.1 PURPOSE AND SCOPE

The purpose of this policy is to set guidelines and requirements pertaining to the handling and disposition of criminal investigations.

## 401.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to investigate crimes thoroughly and with due diligence, and to evaluate and prepare criminal cases for appropriate clearance or submission to a prosecutor.

## 401.3 INITIAL AND FOLLOWUP INVESTIGATIONS

In most cases, the initial investigation will be handled by the law enforcement agency providing police services in that jurisdiction. After an agency submits an arrest to the District Attorney's Office, a bureau investigator may be assigned to conduct followup investigation and assist the prosecutor with preparing the case for court. In some instances, law enforcement agencies may request investigative services from the bureau. In those instances, bureau supervisors will evaluate the needs and provide the appropriate resources necessary to assist that agency. Likewise, criminal investigators can and may develop probable cause for investigating a variety of criminal statutes that threaten the safety of our citizens.

### 401.3.1 INITIAL INVESTIGATION RESPONSIBILITIES

An Investigator responsible for an initial investigation shall complete no less than the following:

- (a) Make a preliminary determination of whether a crime has been committed by completing, at a minimum:
  - 1. An initial statement from any witnesses or complainants.
  - 2. A cursory examination for evidence.
- (b) If information indicates a crime has occurred, the investigator shall:
  - 1. Preserve the scene and any evidence as required to complete the initial and follow-up investigation.
    - (a) Determine if additional investigative resources (e.g., investigators or scene processing) are necessary and request assistance as required.
    - (b) If assistance is warranted, or if the incident is not routine, notify a Lieutenant.
    - (c) Make reasonable attempts to locate, identify and interview all available victims, complainants, witnesses and suspects.
    - (d) Collect any evidence.
    - (e) Take any appropriate law enforcement action.
    - (f) Complete and submit the appropriate reports and documentation in a reasonable time frame or as directed by a supervisor.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Investigation and Prosecution*

---

- (g) Conduct followup as needed.
- (c) Reports shall be turned into a supervisor for approval. Once approved, the HUB will scan the report into ICJIS.
- (d) If the preliminary determination is that no crime occurred, determine what other action may be necessary, what other resources may be available, and advise the informant or complainant of this information.

#### **401.3.2 FOLLOWUP INVESTIGATION RESPONSIBILITIES**

An Investigator assigned a followup investigation shall complete no less than the following:

- (a) Review the details of the case to become familiar with the defendant, witnesses, and the alleged crime(s).
- (b) Review the followup request for completeness and accuracy.
  - 1. Note the due date on the followup request and the assigned DDA.
  - 2. Questions about the followup request should be directed at the assigned DDA or the Investigator's supervisor.
- (c) Complete a supplemental report chronologically detailing all steps taken to complete the followup investigation.
  - 1. Reports shall be completed and turned into a supervisor prior to or on the due date listed on the followup.
  - 2. Once completed and approved, a supervisor will change the status of the followup within ICJIS.
  - 3. The HUB will scan the Investigator's supplemental report into ICJIS for the assigned DDA to review.

#### **401.4 CUSTODIAL INTERROGATION REQUIREMENTS**

Suspects who are in custody and subjected to an interrogation shall be given the *Miranda* warning, unless an exception applies. Interview or interrogation of a juvenile shall be in accordance with Policy 312, Temporary Custody of Juveniles.

##### **401.4.1 AUDIO/VIDEO RECORDINGS**

Any custodial interrogation of an individual who is suspected of having committed any violent felony offense should be recorded (audio or video with audio as available) in its entirety. Regardless of where the interrogation occurs, every reasonable effort should be made to secure functional recording equipment to accomplish such recordings.

Consideration should also be given to recording a custodial interrogation, or any investigative interview, for any other offense when it is reasonable to believe it would be appropriate and beneficial to the investigation and is otherwise allowed by law.

No recording of a custodial interrogation should be destroyed or altered without written authorization from the prosecuting attorney and the Investigative Bureau Lieutenant. Copies of recorded interrogations or interviews may be made in the same or a different format as the original

# Stanislaus County District Attorney's Office

## Policy Manual

### *Investigation and Prosecution*

---

recording, provided the copies are true, accurate and complete and are made only for authorized and legitimate law enforcement purposes.

Recordings (audio/video) should not take the place of a thorough report. A well documented report should complement an audio/video recording used during an investigative interview. Written statements from suspects should continue to be obtained when applicable.

#### **401.4.2 MANDATORY RECORDING OF ADULTS**

Any custodial interrogation of an adult who is suspected of having committed any murder shall be recorded in its entirety. The recording should be video with audio if reasonably feasible (Penal Code § 859.5).

This recording is not mandatory when (Penal Code § 859.5):

- (a) Recording is not feasible because of exigent circumstances that are later documented in a report.
- (b) The suspect refuses to have the interrogation recorded, including a refusal any time during the interrogation, and the refusal is documented in a report. If feasible, the refusal shall be electronically recorded.
- (c) The custodial interrogation occurred in another state by law enforcement officers of that state, unless the interrogation was conducted with the intent to avoid the requirements of Penal Code § 859.5.
- (d) The interrogation occurs when no member conducting the interrogation has a reason to believe that the individual may have committed murder. Continued custodial interrogation concerning that offense shall be electronically recorded if the interrogating member develops a reason to believe the individual committed murder.
- (e) The interrogation would disclose the identity of a confidential informant or would jeopardize the safety of an investigator, the individual being interrogated or another individual. Such circumstances shall be documented in a report.
- (f) A recording device fails despite reasonable maintenance and the timely repair or replacement is not feasible.
- (g) The questions are part of a routine processing or booking, and are not an interrogation.
- (h) The suspect is in custody for murder and the interrogation is unrelated to a murder. However, if any information concerning a murder is mentioned during the interrogation, the remainder of the interrogation shall be recorded.

The Bureau shall maintain an original or an exact copy of the recording until a conviction relating to the interrogation is final and all appeals are exhausted or prosecution is barred by law (Penal Code § 859.5). Additionally, it shall be the policy of the SCDA to maintain an original or exact copy of the recording until all defendants in a homicide case are deceased.

#### **401.5 DISCONTINUATION OF INVESTIGATIONS**

The investigation of a criminal case or efforts to seek prosecution should only be discontinued if one of the following applies:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Investigation and Prosecution*

---

- (a) All reasonable investigative efforts have been exhausted, no reasonable belief that the person who committed the crime can be identified, and the incident has been documented appropriately.
- (b) The perpetrator of a misdemeanor has been identified and a warning is the most appropriate disposition.
  - 1. In these cases, the investigator shall document that the person was warned and why prosecution was not sought.
  - 2. Warnings shall not be given for felony offenses or other offenses identified in this policy or by law that require an arrest or submission of a case to a prosecutor.
- (c) The case has been submitted to the appropriate prosecutor but no charges have been filed. Further investigation is not reasonable nor has the prosecutor requested further investigation.
- (d) The case has been submitted to the appropriate prosecutor, charges have been filed, and further investigation is not reasonable, warranted, or requested, and there is no need to take the suspect into custody.
- (e) Suspects have been arrested, there are no other suspects, and further investigation is either not warranted, or requested.
- (f) Investigation has proven that a crime was not committed (see the Sexual Assault Investigations Policy for special considerations in these cases).

The Domestic Violence, Child Abuse, Sexual Assault Investigations, and Senior and Disability Victimization policies may also require an arrest or submittal of a case to a prosecutor.

#### **401.6 COMPUTERS AND DIGITAL EVIDENCE**

The collection, preservation, transportation and storage of computers, cell phones and other digital devices may require specialized handling to preserve the value of the related evidence. If it is anticipated that computers or similar equipment will be seized, investigators should request that computer forensic examiners assist with seizing computers and related evidence. If a forensic examiner is unavailable, investigators should take reasonable steps to prepare for such seizure and use the resources that are available.

#### **401.7 INVESTIGATIVE USE OF SOCIAL MEDIA AND INTERNET SOURCES**

Use of social media and any other internet source to access information for the purpose of criminal investigation shall comply with applicable laws and policies regarding privacy, civil rights, and civil liberties. Information gathered via the internet should only be accessed by members while on-duty and for purposes related to the mission of this bureau. If a member encounters information relevant to a criminal investigation while off-duty or while using the member's own equipment, the member should note the dates, times, and locations of the information and report the discovery to the member's supervisor as soon as practicable. The member, or others who have been assigned to do so, should attempt to replicate the finding when on-duty and using bureau equipment.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Investigation and Prosecution*

---

Information obtained via the internet should not be archived or stored in any manner other than bureau-established record keeping systems (see the Records Maintenance and Release and the Criminal Organizations policies).

#### **401.7.1 ACCESS RESTRICTIONS**

Information that can be accessed from any bureau computer, without the need of an account, password, email address, alias or other identifier (unrestricted websites), may be accessed and used for legitimate investigative purposes without supervisory approval.

Accessing information from any Internet source that requires the use or creation of an account, password, email address, alias or other identifier, or the use of nongovernment IP addresses, requires supervisor approval prior to access. The supervisor will review the justification for accessing the information and consult with the IT manager and potentially legal counsel as necessary to identify any policy or legal restrictions. Any such access and the supervisor approval shall be documented in the related investigative report.

Accessing information that requires the use of a third party's account or online identifier requires supervisor approval and the consent of the third party. The consent must be voluntary and shall be documented in the related investigative report.

Information gathered from any Internet source should be evaluated for its validity, authenticity, accuracy and reliability. Corroborative evidence should be sought and documented in the related investigative report.

Any information collected in furtherance of an investigation through an Internet source should be documented in the related report. Documentation should include the source of information and the dates and times that the information was gathered.

#### **401.7.2 INTERCEPTING ELECTRONIC COMMUNICATION**

Intercepting social media communications in real time may be subject to federal and state wiretap laws. Investigators should seek legal counsel before any such interception.

#### **401.8 CELLULAR COMMUNICATIONS INTERCEPTION TECHNOLOGY**

The General Crimes Lieutenant is responsible for ensuring the following for cellular communications interception technology operations (Government Code § 53166):

- (a) Security procedures are developed to protect information gathered through the use of the technology.
- (b) A usage and privacy policy is developed that includes:
  - 1. The purposes for which using cellular communications interception technology and collecting information is authorized.
  - 2. Identification by job title or other designation of employees who are authorized to use or access information collected through the use of cellular communications interception technology.
  - 3. Training requirements necessary for those authorized employees.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Investigation and Prosecution*

---

4. A description of how the Bureau will monitor the use of its cellular communications interception technology to ensure the accuracy of the information collected and compliance with all applicable laws.
5. Process and time period system audits.
6. Identification of the existence of any memorandum of understanding or other agreement with any other local agency or other party for the shared use of cellular communications interception technology or the sharing of information collected through its use, including the identity of signatory parties.
7. The purpose of, process for and restrictions on the sharing of information gathered through the use of cellular communications interception technology with other local agencies and persons.
8. The length of time information gathered through the use of cellular communications interception technology will be retained, and the process the local agency will utilize to determine if and when to destroy retained information.

Members shall only use approved devices and usage shall be in compliance with bureau security procedures, the bureau's usage and privacy procedures and all applicable laws.

#### **401.9 MODIFICATION OF CHARGES FILED**

Bureau Investigators are not authorized to recommend to the prosecutor or to any other official of the court that charges on a pending case be amended or dismissed without the authorization of a Lieutenant. Any authorized request to modify the charges or to recommend dismissal of charges shall be made to the prosecutor.

#### **401.10 USE OF CERTAIN DNA SAMPLES**

Known samples of DNA collected from a victim of a crime or alleged crime, and known reference samples of DNA from any individual that were voluntarily provided for the purpose of exclusion are to be used only for the purpose directly related to the incident being investigated and in compliance with the procedures identified in Penal Code § 679.12.

#### **401.11 ANTI-REPRODUCTIVE RIGHTS CRIMES**

A member should take a report any time a person living within the jurisdiction of the Stanislaus County District Attorney's Office reports that the person has been a victim of an anti-reproductive rights crime as defined by Penal Code § 13776 and Penal Code § 423.3. This includes:

- (a) Taking a report, even if the location of the crime is outside the jurisdiction of this bureau or has not been determined (e.g., online harassment).
- (b) Providing the victim with the appropriate information, as set forth in the Victim and Witness Assistance Policy. Members should encourage the person to review the material and should assist with any questions.

A report should also be taken if a person living outside bureau jurisdiction reports an anti-reproductive rights crime that may have been committed or facilitated within this jurisdiction (e.g., use of a post office box in the county to facilitate the crime).



# Stanislaus County District Attorney's Office

## Policy Manual

### *Investigation and Prosecution*

---

A member investigating an anti-reproductive rights crime should ensure that the case is referred to the appropriate agency if it is determined that this bureau should not be the investigating agency. The victim should be advised that the case is being transferred to the agency of jurisdiction. The appropriate entries should be made into any databases that have been authorized for bureau use and are specific to this type of investigation.

The Investigative Bureau supervisor should provide the Records Manager with enough information regarding the number of calls for assistance and number of arrests to meet the reporting requirements to the California Department of Justice as required by Penal Code § 13777. See the Records Bureau Policy for additional guidance.

#### **401.12 STATE REQUIREMENTS FOR FIREARM INVESTIGATIONS**

##### **401.12.1 CALIFORNIA DOJ NOTICE OF LOCATION OF REPORTED LOST OR STOLEN FIREARM**

When notification is received from the California Department of Justice (DOJ) that a firearm purchase matches an entry made into the Automated Firearms System by the Bureau as lost or stolen, the Investigative Bureau supervisor shall assign an investigator to retrieve the firearm and book the firearm into evidence in accordance with the Property and Evidence Policy. Recovery of the firearm shall be reported pursuant to Penal Code § 11108.2, Penal Code § 11108.3, and Penal Code § 11108.5. If appropriate, arrangements may be made to have another state or local law enforcement agency retrieve the firearm on behalf of the Bureau (Penal Code § 28220).

##### **401.12.2 RELINQUISHMENT OF FIREARMS VERIFICATION**

The Investigative Bureau supervisor shall designate a member to have access to the Armed Prohibited Persons System (APPS) to receive information regarding individuals in the jurisdiction of the Bureau who have become a prohibited possessor of a firearm registered in their name and have not provided proof of relinquishment. The member shall document steps taken to verify that the individual is no longer in possession of firearms and provide the information to the Records Bureau for preparation of a quarterly report to the California DOJ (Penal Code § 29813) (see the Records Bureau Policy for additional guidance).

# Search and Seizure

## 402.1 PURPOSE AND SCOPE

Both the federal and state Constitutions provide every individual with the right to be free from unreasonable searches and seizures. This policy provides general guidelines for Stanislaus County District Attorney's Office personnel to consider when dealing with search and seizure issues.

## 402.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to respect the fundamental privacy rights of individuals. Members of this bureau will conduct searches in strict observance of the constitutional rights of persons being searched. All seizures by this bureau will comply with relevant federal and state law governing the seizure of persons and property.

The Bureau will provide relevant and current training to investigators as guidance for the application of current law, local community standards and prosecutorial considerations regarding specific search and seizure situations, as appropriate.

## 402.3 SEARCHES

The U.S. Constitution generally provides that a valid warrant is required in order for a search to be valid. There are, however, several exceptions that permit a warrantless search.

Examples of law enforcement activities that are exceptions to the general warrant requirement include, but are not limited to, searches pursuant to the following:

- Valid consent
- Incident to a lawful arrest
- Legitimate community caretaking interests
- Vehicle searches under certain circumstances
- Exigent circumstances

Certain other activities are recognized by federal and state courts and by certain statutes as legitimate law enforcement activities that also do not require a warrant. Such activities may include seizure and examination of abandoned property, and observations of activities and property located on open public areas.

Because case law regarding search and seizure is constantly changing and subject to interpretation by the courts, each member of this bureau is expected to act in each situation according to current training and his/her familiarity with clearly established rights as determined by case law.

Whenever practicable, investigators are encouraged to contact a supervisor to resolve questions regarding search and seizure issues prior to electing a course of action.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Search and Seizure*

---

#### **402.4 SEARCH PROTOCOL**

Although conditions will vary and officer safety and other exigencies must be considered in every search situation, the following guidelines should be followed whenever circumstances permit:

- (a) Members of this bureau will strive to conduct searches with dignity and courtesy.
- (b) Investigators should explain to the person being searched the reason for the search and how the search will be conducted.
- (c) Searches should be carried out with due regard and respect for private property interests and in a manner that minimizes damage. Property should be left in a condition as close as reasonably possible to its pre-search condition.
- (d) In order to minimize the need for forcible entry, an attempt should be made to obtain keys, combinations or access codes when a search of locked property is anticipated.
- (e) When the person to be searched is of the opposite sex as the searching investigator, a reasonable effort should be made to summon an investigator of the same sex as the subject to conduct the search. When it is not practicable to summon an investigator of the same sex as the subject, the following guidelines should be followed:
  1. Another investigator or a supervisor should witness the search.
  2. The investigator should not search areas of the body covered by tight-fitting clothing, sheer clothing or clothing that could not reasonably conceal a weapon.

#### **402.5 DOCUMENTATION**

Investigators are responsible to document any search and to ensure that any required reports are sufficient including, at minimum, documentation of the following:

- Reason for the search
- Any efforts used to minimize the intrusiveness of any search (e.g., asking for consent or keys)
- What, if any, injuries or damage occurred
- All steps taken to secure property
- The results of the search, including a description of any property or contraband seized
- If the person searched is the opposite sex, any efforts to summon an investigator of the same sex as the person being searched and the identification of any witness investigator

Supervisors shall review reports to ensure the reports are accurate, that actions are properly documented and that current legal requirements and bureau policy have been met.

## Warrant Service

### **403.1 PURPOSE AND SCOPE**

This policy establishes guidelines for the planning and serving of arrest and search warrants by members of this bureau. It is understood that this policy cannot address every variable or circumstance that can arise in the service of a search or arrest warrant, as these tasks can involve rapidly evolving and unique circumstances.

This policy is intended to be used in conjunction with the Operations Planning and Deconfliction Policy, which has additional guidance on planning and serving high-risk warrants.

This policy is not intended to address the service of search warrants on locations or property already secured or routine field warrant arrests by patrol investigators.

### **403.2 POLICY**

It is the policy of the Stanislaus County District Attorney's Office to balance the safety needs of the public, the safety of bureau members, privacy interests and other relevant factors when making decisions related to the service of search and arrest warrants.

### **403.3 SUPERVISOR RESPONSIBILITIES**

A bureau lieutenant (see the Operations Planning and Deconfliction Policy) shall review all risk assessment forms with the involved investigator to determine the risk level of the warrant service.

The lieutenant will also have the responsibility to oversee and coordinate the service of those warrants that are categorized as high risk. Deconfliction, risk assessment, operational planning, briefing and debriefing should follow guidelines in the Operations Planning and Deconfliction Policy 608.

### **403.4 SEARCH WARRANTS**

Investigators should communicate with their supervisor the need for preparing a search warrant that would enhance the scope of their investigation. If approved, the investigator will prepare the affidavit and search warrant, consulting with the applicable prosecuting attorney as needed. He/she will also complete the risk assessment form and submit it, along with the warrant affidavit, to the appropriate bureau lieutenant for review and classification of risk (see the Operations Planning and Deconfliction Policy 608).

If the search warrant is classified as high risk, service will be coordinated by the lieutenant. Careful consideration should be given to the safety of everyone involved as well as mutual aid assistance from Special Weapons and Tactics (SWAT) teams having jurisdiction over the location to be searched. If the search warrant is not classified as high risk, the lieutenant should weigh the risk of immediate entry into the residence against other alternatives such as surveillance tactics geared at identifying persons inside and detaining persons away from the residence to gather additional intelligence before service.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Warrant Service*

---

#### 403.4.1 ACTIONS DURING WARRANT SERVICE

- (a) When practicable and when doing so does not cause unreasonable risk, video or photographic documentation is made of the condition of the location prior to execution of a search warrant. The images should include the surrounding area and persons present.
- (b) Evidence is handled and collected only by those investigators who are designated to do so. All other investigators involved in the service of the warrant should alert one of the designated investigators to the presence of potential evidence and not touch or disturb the items.
- (c) Reasonable efforts are made during the search to maintain or restore the condition of the location.
- (d) Persons who are detained as part of the warrant service are handled appropriately under the circumstances.
- (e) Reasonable care provisions are made for children and dependent adults (see the Child and Dependent Adult Safety Policy).
- (f) A list is made of all items seized and a copy provided to the person in charge of the premises if present or otherwise left in a conspicuous place.
- (g) A copy of the search warrant is left at the location.
- (h) The condition of the property is documented with video recording or photographs after the search.

#### **403.5 ARREST WARRANTS**

If an investigator reasonably believes that serving an arrest warrant may pose a higher risk than commonly faced on a daily basis, the investigator should complete the risk assessment form and submit it to the appropriate lieutenant for review and classification of risk (see the Operations Planning and Deconfliction Policy).

If the warrant is classified as high risk, service will be coordinated by the lieutenant. Careful consideration should be given to the safety of everyone involved as well as mutual aid assistance from SWAT teams having jurisdiction of the location to be searched or tactics used to safely apprehend the wanted person. If the warrant is not classified as high risk, the lieutenant should weigh the risk of entry into a residence to make an arrest against other alternatives, such as arresting the person outside the residence where circumstances may pose a lower risk.

#### **403.6 WARRANT PREPARATION**

An investigator who prepares a warrant should ensure the documentation in support of the warrant contains as applicable:

- (a) Probable cause to support the search or arrest, including relevant dates and times to demonstrate timeliness and facts to support any request for nighttime or no-knock warrant execution.
- (b) A clear explanation of the affiant's training, experience, and relevant education.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Warrant Service*

---

- (c) Adequately supported opinions, when relevant, that are not left to unsubstantiated conclusions.
- (d) A nexus between the place to be searched and the persons or items central to the investigation. The facts supporting this nexus should be clear and current. For example, the affidavit shall explain why there is probable cause to believe that a particular person is currently residing at a particular location or that the items sought are present at a particular location.
- (e) Full disclosure of known or suspected residents at the involved location and any indication of separate living spaces at the involved location. For example, it should be disclosed that several people may be renting bedrooms at a single location, even if the exact location of the rooms is not known.
- (f) A specific description of the location to be searched, including photographs of the location, if reasonably available.
- (g) A sufficient description of the items to be seized.
- (h) Full disclosure of any known exculpatory information relevant to the warrant application (refer to the Brady Material Disclosure Policy).

#### **403.7 HIGH-RISK WARRANT SERVICE**

The operations director or the authorized designee shall coordinate the service of warrants that are categorized as high risk and shall have sole authority in determining the manner in which the warrant will be served, including the number of investigators deployed.

The member responsible for directing the service should ensure the following as applicable:

- (a) When practicable and when doing so does not cause unreasonable risk, video or photographic documentation is made of the condition of the location prior to execution of a search warrant. The images should include the surrounding area and persons present.
- (b) The warrant service is audio- and video-recorded when practicable and reasonable to do so.
- (c) Evidence is handled and collected only by those members who are designated to do so. All other members involved in the service of the warrant should alert one of the designated members to the presence of potential evidence and not touch or disturb the items.
- (d) Reasonable efforts are made during the search to maintain or restore the condition of the location.
- (e) Persons who are detained as part of the warrant service are handled appropriately under the circumstances.
- (f) Reasonable care provisions are made for children and dependent adults (see the Child and Dependent Adult Safety Policy).
- (g) A list is made of all items seized and a copy provided to the person in charge of the premises if present or otherwise left in a conspicuous place.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Warrant Service*

---

- (h) A copy of the search warrant is left at the location.
- (i) The condition of the property is documented with video recording or photographs after the search.

#### **403.8 DETENTIONS DURING WARRANT SERVICE**

Investigators must be sensitive to the safety risks of all persons involved with the service of a warrant. Depending on circumstances and facts present, it may be appropriate to control movements of any or all persons present at a warrant service, including those who may not be the subject of a warrant or suspected in the case. However, investigators must be mindful that only reasonable force may be used and weapons should be displayed no longer than the investigator reasonably believes is necessary (see the Use of Force Policy).

As soon as it can be determined that an individual is not subject to the scope of a warrant and that no further reasonable suspicion or safety concerns exist to justify further detention, the person should be promptly released.

Investigators should, when and to the extent reasonable, accommodate the privacy and personal needs of people who have been detained.

#### **403.9 ACTIONS AFTER WARRANT SERVICE**

The primary investigator and/or affiant shall ensure that all affidavits, warrants, receipts and returns, regardless of any associated cases, are filed with the issuing judge or magistrate as soon as reasonably possible, but in any event no later than any date specified on the warrant.

#### **403.10 OUTSIDE AGENCIES AND CROSS-JURISDICTIONAL WARRANTS**

A bureau lieutenant will ensure that cooperative efforts with other agencies in the service of warrants conform to existing mutual aid agreements or other memorandums of understanding and will work cooperatively to mitigate risks including, but not limited to, the following:

- Identity of team members
- Roles and responsibilities
- Familiarity with equipment
- Rules of engagement
- Asset forfeiture procedures

Any outside agency requesting assistance in the service of a warrant within this jurisdiction should be referred to a bureau lieutenant. The lieutenant should review and confirm the warrant, including the warrant location, and should discuss the service with the appropriate supervisor from the other agency. The lieutenant should ensure that members of the Stanislaus County District Attorney's Office are utilized appropriately. Any concerns regarding the requested use of bureau members should be brought to the attention of the Chief of Investigations or the authorized designee. The actual service of the warrant will remain the responsibility of the agency requesting assistance.

If the bureau lieutenant is unavailable, the Chief Investigator should assume this role.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Warrant Service*

---

If investigators intend to serve a warrant outside Stanislaus County jurisdiction, a bureau lieutenant should provide reasonable advance notice to the applicable agency, request assistance as needed and work cooperatively on operational planning and the mitigation of risks detailed in this policy.

Investigators will remain subject to the policies of the Stanislaus County District Attorney's Office when assisting outside agencies or serving a warrant outside Stanislaus County jurisdiction.

#### **403.11 MEDIA ACCESS**

No advance information regarding warrant service operations shall be released without the approval of the Chief of Investigations. Any media inquiries or press release after the fact shall be handled in accordance with the Media Relations Policy.

#### **403.12 TRAINING**

The bureau training lieutenant should ensure investigators receive periodic training on this policy and associated topics, such as legal issues, warrant preparation, warrant service and reporting requirements.

#### **403.13 NO-KNOCK ENTRIES**

No-knock entries are only authorized if a no-knock warrant has been obtained or if exigent circumstances arise at the scene such that knocking and announcing the investigator's presence would create an imminent threat of physical violence to the investigator or another person.

#### **403.14 DOCUMENTATION**

Documentation related to the service of a warrant shall be maintained in accordance with the established records retention schedule.



## Contacts and Temporary Detentions

### 404.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for temporarily detaining but not arresting persons in the field, conducting field interviews (FI) and pat-down searches, and the taking and disposition of photographs.

#### 404.1.1 DEFINITIONS

Definitions related to this policy include:

**Consensual encounter** - When an investigator contacts an individual but does not create a detention through words, actions, or other means. In other words, a reasonable individual would believe that his/her contact with the investigator is voluntary.

**Field interview** - The brief detainment of an individual, whether on foot or in a vehicle, based on reasonable suspicion for the purpose of determining the individual's identity and resolving the investigator's suspicions.

**Field photographs** - Posed photographs taken of a person during a contact, temporary detention, or arrest in the field. Undercover surveillance photographs of an individual and recordings captured by the normal operation of a Mobile Audio Video (MAV) system, body-worn camera, or public safety camera when persons are not posed for the purpose of photographing are not considered field photographs.

**Pat-down search** - A type of search used by investigators in the field to check an individual for dangerous weapons. It involves a thorough patting-down of clothing to locate any weapons or dangerous items that could pose a danger to the investigator, the detainee, or others.

**Reasonable suspicion** - When, under the totality of the circumstances, an investigator has articulable facts that criminal activity may be afoot and a particular person is connected with that possible criminal activity.

**Temporary detention** - When an investigator intentionally, through words, actions, or physical force, causes an individual to reasonably believe he/she is required to restrict his/her movement without an actual arrest. Temporary detentions also occur when an investigator actually restrains a person's freedom of movement.

### 404.2 POLICY

The Stanislaus County District Attorney's Office respects the right of the public to be free from unreasonable searches or seizures. Due to an unlimited variety of situations confronting the investigator, the decision to temporarily detain a person and complete a field interview (FI), pat-down search, or field photograph shall be left to the investigator based on the totality of the circumstances, officer safety considerations, and constitutional safeguards.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Contacts and Temporary Detentions*

---

#### **404.3 FIELD INTERVIEWS**

Based on observance of suspicious circumstances or upon information from investigation, an investigator may initiate the stop of a person, and conduct an FI, when there is articulable, reasonable suspicion to do so. A person, however, shall not be detained longer than is reasonably necessary to resolve the investigator's suspicion.

Nothing in this policy is intended to discourage consensual contacts. Frequent casual contact with consenting individuals is encouraged by the Stanislaus County District Attorney's Office to strengthen community involvement, community awareness, and problem identification.

##### **404.3.1 INITIATING A FIELD INTERVIEW**

When initiating the stop, the investigator should be able to point to specific facts which, when considered with the totality of the circumstances, reasonably warrant the stop. Such facts include but are not limited to an individual's:

- (a) Appearance or demeanor suggesting that he/she is part of a criminal enterprise or is engaged in a criminal act
- (b) Actions suggesting that he/she is engaged in a criminal activity
- (c) Presence in an area at an inappropriate hour of the day or night
- (d) Presence in a particular area is suspicious
- (e) Carrying of suspicious objects or items
- (f) Excessive clothes for the climate or clothes bulging in a manner that suggest he/she is carrying a dangerous weapon
- (g) Location in proximate time and place to an alleged crime
- (h) Physical description or clothing worn that matches a suspect in a recent crime
- (i) Prior criminal record or involvement in criminal activity as known by the investigator

#### **404.4 PAT-DOWN SEARCHES**

Once a valid stop has been made, and consistent with the investigator's training and experience, an investigator may pat a suspect's outer clothing for weapons if the investigator has a reasonable, articulable suspicion the suspect may pose a safety risk. The purpose of this limited search is not to discover evidence of a crime, but to allow the investigator to pursue the investigation without fear of violence. Circumstances that may establish justification for performing a pat-down search include but are not limited to:

- (a) The type of crime suspected, particularly in crimes of violence where the use or threat of deadly weapons is involved.
- (b) Where more than one suspect must be handled by a single investigator.
- (c) The hour of the day and the location or neighborhood where the stop takes place.
- (d) Prior knowledge of the suspect's use of force and/or propensity to carry weapons.
- (e) The actions and demeanor of the suspect.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Contacts and Temporary Detentions*

---

- (f) Visual indications which suggest that the suspect is carrying a firearm or other weapon.

Whenever practicable, a pat-down search should not be conducted by a lone investigator. A cover investigator should be positioned to ensure safety and should not be involved in the search.

#### **404.5 FIELD PHOTOGRAPHS**

All available databases should be searched before photographing any field detainee. If a photograph is not located, or if an existing photograph no longer resembles the detainee, the investigator shall carefully consider, among other things, the factors listed below.

##### **404.5.1 FIELD PHOTOGRAPHS TAKEN WITH CONSENT**

Absent a detention, an arrest, or investigative technique, field photographs may only be taken when the subject being photographed knowingly and voluntarily gives consent.

##### **404.5.2 FIELD PHOTOGRAPHS TAKEN WITHOUT CONSENT**

Field photographs may be taken without consent only if they are taken during a detention that is based upon reasonable suspicion of criminal activity, and the photograph serves a legitimate law enforcement purpose related to the detention. The investigator must be able to articulate facts that reasonably indicate that the subject was involved in or was about to become involved in criminal conduct.

If, prior to taking a photograph, the investigator's reasonable suspicion of criminal activity has been dispelled, the detention must cease and the photograph should not be taken.

All field photographs and related reports shall be submitted to a supervisor and retained in compliance with this policy.

##### **404.5.3 DISPOSITION OF PHOTOGRAPHS**

If an individual is photographed as a suspect in a particular crime, the photograph should be submitted as an evidence item in the related case, following standard evidence procedures.

If a photograph is not associated with an investigation where a case number has been issued, the investigator will obtain a case number from ICJIS, document the contact in a report, and upload the photograph to Evidence.com under that case number.

When a photograph is taken in association with a particular case, the investigator may use such photograph in a photo lineup. Thereafter, the individual photograph should be retained as a part of the case file. All other photographs shall be retained in accordance with the established records retention schedule.

##### **404.5.4 SUPERVISOR RESPONSIBILITIES**

While it is recognized that field photographs often become valuable investigative tools, supervisors should monitor such practices in view of the above listed considerations. This is not to imply that supervisor approval is required before each photograph is taken.

Access to, and use of, field photographs shall be strictly limited to law enforcement purposes.

### *Contacts and Temporary Detentions*

---

#### **404.6 WITNESS IDENTIFICATION AND INTERVIEWS**

Because potential witnesses to an incident may become unavailable or the integrity of their statements compromised with the passage of time, investigators should, when warranted by the seriousness of the case, take reasonable steps to promptly coordinate with an on-scene supervisor and/or criminal investigator to utilize available members for the following:

- (a) Identifying all persons present at the scene and in the immediate area.
  - 1. When feasible, a recorded statement should be obtained from those who claim not to have witnessed the incident but who were present at the time it occurred.
  - 2. Any potential witness who is unwilling or unable to remain available for a formal interview should not be detained absent reasonable suspicion to detain or probable cause to arrest. Without detaining the individual for the sole purpose of identification, investigators should attempt to identify the witness prior to his/her departure.
- (b) Witnesses who are willing to provide a formal interview should be asked to meet at a suitable location where criminal investigators may obtain a recorded statement. Such witnesses, if willing, may be transported by Stanislaus County District Attorney's Office members.
  - 1. A written, verbal, or recorded statement of consent should be obtained prior to transporting a witness. When the witness is a minor, consent should be obtained from the parent or guardian, if available, prior to transport.

# Operations Planning and Deconfliction

## 405.1 PURPOSE AND SCOPE

This policy provides guidelines for planning, deconfliction and execution of high-risk operations.

Additional guidance on planning and serving high-risk warrants is provided in the Warrant Service Policy 607.

### 405.1.1 DEFINITIONS

Definitions related to this policy include:

**High-risk operations** - Operations, including service of search and arrest warrants and sting operations, that are likely to present higher risks than are commonly faced by investigators on a daily basis, including suspected fortified locations, reasonable risk of violence or confrontation with multiple persons, or reason to suspect that persons anticipate the operation.

## 405.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to properly plan and carry out high-risk operations, including participation in a regional deconfliction system, in order to provide coordination, enhance the safety of members and the public, decrease the risk of compromising investigations and prevent duplicating efforts.

## 405.3 RISK ASSESSMENT

The planning and preparation of a high-risk mission will involve the use of a Operations Plan and a Risk Assessment Matrix. The matrix is designed to ask key and crucial questions about the type of operation, the suspects wanted, their involvement with gangs, access to weapons, and known violent tendencies.

[See attachment: SCDA Risk Assessment Matrix.pdf](#)

### 405.3.1 RISK ASSESSMENT FORM PREPARATION

Investigators assigned as case officers for any operation that may qualify as a high-risk operation shall complete a risk assessment matrix.

When preparing the form, the investigator should query all relevant and reasonably available intelligence resources for information about the subject of investigation, others who may be present and the involved location. These sources may include regional intelligence and criminal justice databases, target deconfliction systems, firearm records, commercial databases and property records. Where appropriate, the investigator should also submit information to these resources.

The investigator should gather available information that includes, but is not limited to:

- (a) Photographs, including aerial photographs, if available, of the involved location, neighboring yards and obstacles.
- (b) Maps of the location.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Operations Planning and Deconfliction*

---

- (c) Diagrams of any property and the interior of any buildings that are involved.
- (d) Historical information about the subject of investigation (e.g., history of weapon possession or use, known mental illness, known drug use, threats against police, gang affiliation, criminal history).
- (e) Historical information about others who may be present at the location (e.g., other criminals, innocent third parties, dependent adults, children, animals).
- (f) Obstacles associated with the location (e.g., fortification, booby traps, reinforced doors/windows, surveillance measures, number and type of buildings, geographic and perimeter barriers, the number and types of weapons likely to be present, information that suggests the presence of explosives, chemicals or other hazardous materials, the potential for multiple dwellings or living spaces, availability of keys/door combinations).
- (g) Other environmental factors (e.g., nearby venues such as schools and day care centers, proximity of adjacent homes or other occupied buildings, anticipated pedestrian and vehicle traffic at the time of service).
- (h) Other available options that may minimize the risk to investigators and others (e.g., making an off-site arrest or detention of the subject of investigation).

#### 405.3.2 RISK ASSESSMENT REVIEW

Investigators will present the risk assessment matrix with the operations plan and other relevant documents (such as copies of search warrants and affidavits and arrest warrants) to their lieutenant for review.

The lieutenant shall confer with the investigator and determine the level of risk. Supervisors should take reasonable actions if there is a change in circumstances that elevates the risks associated with the operation.

#### 405.3.3 HIGH-RISK OPERATIONS

If the lieutenant, after consultation with the involved investigator, determines that the operation is high risk, the lieutenant should:

- (a) Determine what resources will be needed at the location, and contact and/or place on standby any of the following appropriate and available resources:
  - 1. Special Weapons and Tactics (SWAT) team
  - 2. Additional personnel
  - 3. Outside agency assistance
  - 4. Special equipment
  - 5. Medical personnel
  - 6. Persons trained in negotiation
  - 7. Additional surveillance
  - 8. Canines
  - 9. Forensic specialists

# Stanislaus County District Attorney's Office

## Policy Manual

### *Operations Planning and Deconfliction*

---

10. Specialized mapping for larger or complex locations
- (b) Contact the appropriate bureau members or other agencies as warranted to begin preparation.
- (c) Ensure that all legal documents such as search warrants are complete and have any modifications reasonably necessary to support the operation.
- (d) Coordinate the actual operation.

#### **405.4 DECONFLICTION**

Deconfliction systems are designed to identify persons and locations associated with investigations or law enforcement operations and alert participating agencies when others are planning or conducting operations in close proximity or time or are investigating the same individuals, groups or locations.

The investigator who is the case officer shall ensure the subject of investigation and operations information have been entered in an applicable deconfliction system to determine if there is reported conflicting activity. This should occur as early in the process as practicable. The investigator should also enter relevant updated information when it is received.

If any conflict is discovered, the supervisor or investigator will contact the involved jurisdiction and resolve the potential conflict before proceeding.

#### **405.5 OPERATIONS PLAN**

The operations director should ensure that a written operations plan is developed for all high-risk operations. Plans should also be considered for other operations that would benefit from having a formal plan.

The plan should address such issues as:

- (a) Operation goals, objectives, and strategies.
- (b) Operation location and people:
  1. The subject of investigation (e.g., history of weapon possession/use, known mental illness issues, known drug use, threats against police, gang affiliation, criminal history)
  2. The location (e.g., fortification, booby traps, reinforced doors/windows, surveillance cameras and/or lookouts, number/type of buildings, geographic and perimeter barriers, the number and types of weapons likely to be present, information that suggests the presence of explosives, chemicals or other hazardous materials, the potential for multiple dwellings or living spaces, availability of keys/door combinations), including aerial photos, if available, and maps of neighboring yards and obstacles, diagrams and other visual aids
  3. Other environmental factors (e.g., nearby venues such as schools and day care centers, proximity of adjacent homes or other occupied buildings, anticipated pedestrian and vehicle traffic at the time of service)

# Stanislaus County District Attorney's Office

## Policy Manual

### *Operations Planning and Deconfliction*

---

4. Identification of other people who may be present in or around the operation, such as other criminal suspects, innocent third parties, and children
- (c) Information from the risk assessment form by attaching a completed copy in the operational plan.
  1. The volume or complexity of the information may indicate that the plan includes a synopsis of the information contained on the risk assessment form to ensure clarity and highlighting of critical information.
- (d) Participants and their roles.
  1. An adequate number of uniformed investigators should be included in the operation team to provide reasonable notice of a legitimate law enforcement operation.
  2. How all participants will be identified as law enforcement.
- (e) Whether deconfliction submissions are current and all involved individuals, groups, and locations have been deconflicted to the extent reasonably practicable.
- (f) Identification of all communications channels and call-signs.
- (g) Use of force issues.
- (h) Contingencies for handling medical emergencies (e.g., services available at the location, closest hospital, closest trauma center).
- (i) Plans for detaining people who are not under arrest.
- (j) Contingencies for handling children, dependent adults, animals, and other people who might be at the location in accordance with the Child Abuse, Senior and Disability Victimization, Child and Dependent Adult Safety, and Animal Control policies.
- (k) Communications plan.
- (l) Responsibilities for writing, collecting, reviewing, and approving reports.

[See attachment: DA Office Op Plan Template.pdf](#)

#### **405.5.1 OPERATIONS PLAN RETENTION**

Since the operations plan contains intelligence information and descriptions of law enforcement tactics, it shall not be filed with the investigative report. The operations plan shall be stored separately and retained by the investigator who was overall in charge of the operation.

#### **405.6 OPERATIONS BRIEFING**

A briefing should be held prior to the commencement of any high-risk operation to allow all participants to understand the operation, see and identify each other, identify roles and responsibilities and ask questions or seek clarification as needed. Anyone who is not present at the briefing should not respond to the operation location without specific supervisory approval.

- (a) The briefing should include a verbal review of plan elements, using visual aids, to enhance the participants' understanding of the operations plan.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Operations Planning and Deconfliction*

---

- (b) All participants should be provided a copy of the operations plan and search warrant, if applicable. Participating personnel should be directed to read the search warrant and initial a copy that is retained with the operation plan. Any items to be seized should be identified at the briefing.
- (c) The participating supervising lieutenant shall ensure that all participants are visually identifiable as law enforcement officers.
  - 1. Exceptions may be made by the operations director for investigators who are conducting surveillance or working under cover. However, those members exempt from visual identification should be able to transition to a visible law enforcement indicator at the time of enforcement actions, such as entries or arrests, if necessary.
- (d) The briefing should include details of the communications plan.
  - 1. It is the responsibility of the supervising lieutenant to ensure that SR 911 is notified of the time and location of the operation, and to provide a copy of the operation plan prior to investigators arriving at the location.
  - 2. If the radio channel needs to be monitored by SR 911, the dispatcher assigned to monitor the operation should attend the briefing, if practicable, but at a minimum should receive a copy of the operation plan.
  - 3. The briefing should include a communications check to ensure that all participants are able to communicate with the available equipment on the designated radio channel.

#### **405.7 SWAT PARTICIPATION**

If the supervising lieutenant determines that SWAT participation is appropriate, the lieutenant and the SWAT commander shall work together to develop a written plan. The SWAT commander shall assume operational control until all persons at the scene are appropriately detained and it is safe to begin a search. When this occurs, the SWAT commander shall transfer control of the scene to the bureau's supervising lieutenant. This transfer should be communicated to the investigators present.

#### **405.8 MEDIA ACCESS**

No advance information regarding planned operations shall be released without the approval of the Chief of Investigations. Any media inquiries or press release after the fact shall be handled in accordance with the Media Relations Policy.

#### **405.9 OPERATIONS DEBRIEFING**

High-risk operations should be debriefed as soon as reasonably practicable. The debriefing should include as many participants as possible. This debrief may be separate from any SWAT debriefing.

#### **405.10 TRAINING**

The Training Lieutenant should ensure investigators who participate in operations subject to this policy should receive periodic training including, but not limited to, topics such as legal issues, deconfliction practices, operations planning concepts and reporting requirements.

## Temporary Custody of Juveniles

### 406.1 PURPOSE AND SCOPE

This policy provides guidelines consistent with the Juvenile Justice and Delinquency Prevention Act for juveniles taken into temporary custody by members of the Stanislaus County District Attorney's Office (34 USC § 11133).

Guidance regarding contacting juveniles at schools or who may be victims is provided in the Child Abuse Policy.

#### 406.1.1 DEFINITIONS

Definitions related to this policy include:

**Juvenile non-offender** - An abused, neglected, dependent, or alien juvenile who may be legally held for the juvenile's own safety or welfare. This also includes any juvenile who may have initially been contacted for an offense that would not subject an adult to arrest (e.g., fine-only offense) but was taken into custody for the juvenile's protection or for purposes of reuniting the juvenile with a parent, guardian, or other responsible person. Juveniles 11 years of age or younger are considered juvenile non-offenders even if they have committed an offense that would subject an adult to arrest.

**Juvenile offender** - A juvenile 12 to 17 years of age who is alleged to have committed an offense that would subject an adult to arrest (a non-status offense) (Welfare and Institutions Code § 602). It also includes an offense under Penal Code § 29610 for underage possession of a handgun or concealable firearm (28 CFR 31.303).

**Non-secure custody** - When a juvenile is held in the presence of an investigator or other custody employee at all times and is not placed in a locked room, cell, or behind any locked doors. Juveniles in non-secure custody may be handcuffed but not to a stationary or secure object. Personal supervision, through direct visual monitoring and audio two-way communication is maintained. Monitoring through electronic devices, such as video, does not replace direct visual observation (Welfare and Institutions Code § 207.1; 15 CCR 1150).

**Safety checks** - Direct, visual observation personally by a member of this bureau performed at random intervals within time frames prescribed in this policy to provide for the health and welfare of juveniles in temporary custody.

**Secure custody** - When a juvenile offender is held in a locked room, a set of rooms, or a cell. Secure custody also includes being physically secured to a stationary object (15 CCR 1146).

Examples of secure custody include:

- (a) A juvenile left alone in an unlocked room within the secure perimeter of the adult temporary holding area.
- (b) A juvenile handcuffed to a rail.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Juveniles*

---

- (c) A juvenile placed in a room that contains doors with delayed egress devices that have a delay of more than 30 seconds.
- (d) A juvenile being processed in a secure booking area when a non-secure booking area is available.
- (e) A juvenile left alone in a secure booking area after being photographed and fingerprinted.
- (f) A juvenile placed in a cell within the adult temporary holding area, whether or not the cell door is locked.
- (g) A juvenile placed in a room that is capable of being locked or contains a fixed object designed for cuffing or restricting movement.

**Sight and sound separation** - Located or arranged to prevent physical, visual, or auditory contact that is more than brief or inadvertent.

**Status offender** - A juvenile suspected of committing a criminal violation of the law that would not be a criminal violation but for the age of the offender. Examples may include running away, underage possession of tobacco, curfew violation, and truancy. A juvenile in custody on a court order or warrant based upon a status offense is also a status offender. This includes the habitually disobedient or truant juvenile under Welfare and Institutions Code § 601 and any juvenile suspected of an offense that would not subject an adult to arrest (e.g., fine-only offense).

#### **406.2 POLICY**

The Stanislaus County District Attorney's Office is committed to releasing juveniles from temporary custody as soon as reasonably practicable and keeping juveniles safe while they are in temporary custody at the Stanislaus County District Attorney's Office. Juveniles should be held in temporary custody only for as long as reasonably necessary for processing, transfer, or release.

#### **406.3 JUVENILES WHO SHOULD NOT BE HELD**

Juveniles who exhibit any of the following conditions should not be held at the Stanislaus County District Attorney's Office:

- (a) Unconscious
- (b) Seriously injured
- (c) A known suicide risk or obviously severely emotionally disturbed
- (d) Significantly intoxicated except when approved by the Lieutenant. A medical clearance shall be obtained for minors who are under the influence of drugs, alcohol, or any other intoxicating substance to the extent that they are unable to care for themselves (15 CCR 1151).
- (e) Extremely violent or continuously violent

Investigators taking custody of a juvenile who exhibits any of the above conditions should take reasonable steps to provide medical attention or mental health assistance and notify a supervisor of the situation (15 CCR 1142; 15 CCR 1151).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Juveniles*

---

These juveniles should not be held at the Stanislaus County District Attorney's Office unless they have been evaluated by a qualified medical and/or mental health professional (15 CCR 1142).

If the investigator taking custody of the juvenile believes the juvenile may be a suicide risk, the juvenile shall be under continuous direct supervision until evaluation, release, or a transfer is completed (15 CCR 1142).

#### **406.3.1 EMERGENCY MEDICAL CARE OF JUVENILES IN CUSTODY**

When emergency medical attention is required for a juvenile, medical assistance will be called immediately. The Lieutenant shall be notified of the need for medical attention for the juvenile. Bureau members should administer first aid as applicable (15 CCR 1142).

#### **406.3.2 SUICIDE PREVENTION OF JUVENILES IN CUSTODY**

Bureau members should be alert to potential symptoms based upon exhibited behavior that may indicate the juvenile is a suicide risk. These symptoms may include depression, refusal to communicate, verbally threatening to kill themselves, or any unusual behavior which may indicate the juvenile may harm themselves while in either secure or non-secure custody (15 CCR 1142).

#### **406.4 CUSTODY OF JUVENILES**

Investigators should take custody of a juvenile and temporarily hold the juvenile at the Stanislaus County District Attorney's Office when there is no other lawful and practicable alternative to temporary custody. Refer to the Child Abuse Policy for additional information regarding detaining a juvenile that is suspected of being a victim.

No juvenile should be held in temporary custody at the Stanislaus County District Attorney's Office without authorization of the arresting investigator's supervisor or the Lieutenant. Juveniles taken into custody shall be held in non-secure custody unless otherwise authorized by this policy.

Any juvenile taken into custody shall be released to the care of the juvenile's parent or other responsible adult or transferred to a juvenile custody facility or to other authority as soon as practicable and in no event shall a juvenile be held beyond six hours from the time of the juvenile's entry into the Stanislaus County District Attorney's Office (34 USC § 11133; Welfare and Institutions Code § 207.1).

#### **406.4.1 CUSTODY OF JUVENILE NON-OFFENDERS**

Non-offenders taken into protective custody in compliance with the Child Abuse Policy should generally not be held at the Stanislaus County District Attorney's Office. Custodial arrangements should be made for non-offenders as soon as reasonably possible. Juvenile non-offenders shall not be held in secure custody (34 USC § 11133; Welfare and Institutions Code § 206).

Juveniles 11 years of age or younger who have committed an offense that would subject an adult to arrest may be held in non-secure custody for the offenses listed in Welfare and Institutions Code § 602(b) (murder and the sexual assault offenses) and should be referred to a probation officer for a placement determination (Welfare and Institutions Code § 602.1).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Juveniles*

---

#### 406.4.2 CUSTODY OF JUVENILE STATUS OFFENDERS

Status offenders should generally be released by citation or with a warning rather than taken into temporary custody. However, investigators may take custody of a status offender if requested to do so by a parent or legal guardian in order to facilitate reunification (e.g., transported home or to the station to await a parent). Juvenile status offenders shall not be held in secure custody (34 USC § 11133).

#### 406.4.3 CUSTODY OF JUVENILE OFFENDERS

Juvenile offenders should be held in non-secure custody while at the Stanislaus County District Attorney's Office unless another form of custody is authorized by this policy or is necessary due to exigent circumstances.

Generally, a juvenile offender may be taken into custody when authorized by a court order or when there is probable cause to believe the juvenile has committed an offense that would subject an adult to arrest (Welfare and Institutions Code § 625).

A juvenile offender who is 14 years of age or older and taken into custody for committing or attempting to commit a felony with a firearm shall not be released and be transported to a juvenile facility (Welfare and Institutions Code § 625.3).

A juvenile offender suspected of committing murder, a sex offense described in Welfare and Institutions Code § 602(b) that may subject the juvenile to criminal jurisdiction under Welfare and Institutions Code § 707, or a serious or violent felony should be referred to a probation officer for a decision on further detention.

In all other cases the juvenile offender may be:

- (a) Released upon warning or citation.
- (b) Released to a parent or other responsible adult after processing at the Bureau.
- (c) Referred to a probation officer for a decision regarding whether to transport the juvenile offender to a juvenile facility.
- (d) Transported to the juvenile offender's home or to the place where the juvenile offender was taken into custody (Welfare and Institutions Code § 207.2).

In determining which disposition is appropriate, the investigating investigator or supervisor shall prefer the alternative that least restricts the juvenile's freedom of movement, provided that alternative is compatible with the best interests of the juvenile and the community (Welfare and Institutions Code § 626).

Whenever a juvenile offender under the age of 14 is taken into custody, the investigator should take reasonable steps to verify and document the child's ability to differentiate between right and wrong, particularly in relation to the alleged offense (Penal Code § 26).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Juveniles*

---

#### **406.5 ADVISEMENTS**

Investigators shall take immediate steps to notify the juvenile's parent, guardian, or a responsible relative that the juvenile is in custody, the location where the juvenile is being held, and the intended disposition (Welfare and Institutions Code § 627).

Whenever a juvenile is taken into temporary custody, the juvenile shall be given the *Miranda* rights advisement regardless of whether questioning is intended. This does not apply to juvenile non-offenders taken into temporary custody for their safety or welfare (Welfare and Institutions Code § 625).

Anytime a juvenile offender is placed in secure custody, the juvenile offender shall be informed of the purpose of the secure custody, the length of time the secure custody is expected to last, and of the maximum six-hour limitation (Welfare and Institutions Code § 207.1).

Juveniles taken into custody for an offense shall immediately be advised (or at least within one hour from being taken into custody, if possible) that they may make three telephone calls: one call completed to their parent or guardian; one to a responsible relative or their employer; and another call completed to an attorney. The calls shall be at no expense to the juvenile when completed to telephone numbers within the local calling area. Juveniles should be asked whether they are a caregiver and provided two more phone calls in the same manner as provided to adults in the Temporary Custody of Adults Policy (Welfare and Institutions Code § 627; Penal Code § 851.5).

#### **406.6 JUVENILE CUSTODY LOGS**

Any time a juvenile is held in custody at the Bureau, the custody shall be promptly and properly documented in the juvenile custody log, including:

- (a) Identifying information about the juvenile.
- (b) Date and time of arrival and release from the Stanislaus County District Attorney's Office (15 CCR 1150).
- (c) Lieutenant notification and approval to temporarily hold the juvenile.
- (d) Any charges for which the juvenile is being held and classification of the juvenile as a juvenile offender, status offender, or non-offender.
- (e) Any changes in status (e.g., emergency situations, unusual incidents).
- (f) Time of all safety checks.
- (g) Any medical and other screening requested and completed (15 CCR 1142).
- (h) Circumstances that justify any secure custody (Welfare and Institutions Code § 207.1; 15 CCR 1145).
- (i) Any other information that may be required by other authorities, such as compliance inspectors or a local juvenile court authority.

The Lieutenant shall initial the log to approve the custody, including any secure custody, and shall also initial the log when the juvenile is released.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Juveniles*

---

#### **406.7 NO-CONTACT REQUIREMENTS**

Sight and sound separation shall be maintained between all juveniles and adults while in custody at the Bureau (34 USC § 11133; Welfare and Institutions Code § 207.1; Welfare and Institutions Code § 208; 15 CCR 1144). There should also be sight and sound separation between non-offenders and juvenile and status offenders.

In situations where brief or accidental contact may occur (e.g., during the brief time a juvenile is being fingerprinted and/or photographed in booking), a member of the Stanislaus County District Attorney's Office (trained in the supervision of persons in custody) shall maintain a constant, immediate, side-by-side presence with the juvenile or the adult to minimize any contact. If inadvertent or accidental contact does occur, reasonable efforts shall be taken to end the contact (15 CCR 1144).

#### **406.8 TEMPORARY CUSTODY REQUIREMENTS**

Members and supervisors assigned to monitor or process any juvenile at the Stanislaus County District Attorney's Office shall ensure the following:

- (a) The Lieutenant should be notified if it is anticipated that a juvenile may need to remain at the Stanislaus County District Attorney's Office more than four hours. This will enable the Lieutenant to ensure no juvenile is held at the Stanislaus County District Attorney's Office more than six hours.
- (b) A staff member of the same sex shall supervise personal hygiene activities and care, such as changing clothing or using the restroom, without direct observation to allow for privacy.
- (c) Personal safety checks and significant incidents/activities shall be noted on the log.
- (d) Juveniles in custody are informed that they will be monitored at all times, except when using the toilet.
  - 1. There shall be no viewing devices, such as peep holes or mirrors, of which the juvenile is not aware.
  - 2. This does not apply to surreptitious and legally obtained recorded interrogations.
- (e) Juveniles shall have reasonable access to toilets and wash basins (15 CCR 1143).
- (f) Juveniles shall be provided sanitary napkins, panty liners, and tampons as requested (15 CCR 1143).
- (g) Food shall be provided if a juvenile has not eaten within the past four hours or is otherwise in need of nourishment, including any special diet required for the health of the juvenile (15 CCR 1143).
- (h) Juveniles shall have reasonable access to a drinking fountain or water (15 CCR 1143).
- (i) Juveniles shall have reasonable opportunities to stand and stretch, particularly if handcuffed or restrained in any way.
- (j) Juveniles shall have privacy during family, guardian, and/or lawyer visits (15 CCR 1143).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Juveniles*

---

- (k) Juveniles shall be permitted to remain in their personal clothing unless the clothing is taken as evidence or is otherwise unsuitable or inadequate for continued wear while in custody (15 CCR 1143).
- (l) Blankets shall be provided as reasonably necessary (15 CCR 1143).
  - 1. The supervisor should ensure that there is an adequate supply of clean blankets.
- (m) Adequate shelter, heat, light, and ventilation should be provided without compromising security or enabling escape.
- (n) Juveniles shall have adequate furnishings, including suitable chairs or benches.
- (o) Juveniles shall have the right to the same number of telephone calls as an adult in temporary custody.
- (p) Juveniles shall have access to language services (15 CCR 1143).
- (q) Juveniles shall have access to disability services (15 CCR 1143).
- (r) No discipline may be administered to any juvenile, nor may juveniles be subjected to corporal or unusual punishment, humiliation, or mental abuse (15 CCR 1142).

While held in temporary custody, juveniles shall be informed in writing of what is available to them pursuant to 15 CCR 1143 and it shall be posted in at least one conspicuous place to which they have access (15 CCR 1143).

#### **406.9 RELIGIOUS ACCOMMODATION**

Juveniles have the right to the same religious accommodation as adults in temporary custody (see the Temporary Custody of Adults Policy).

#### **406.10 USE OF RESTRAINT DEVICES**

Juvenile offenders may be handcuffed in accordance with the Handcuffing and Restraints Policy. A juvenile offender may be handcuffed at the Stanislaus County District Attorney's Office when the juvenile presents a heightened risk. However, non-offenders and status offenders should not be handcuffed unless they are combative or threatening (15 CCR 1142).

Other restraints shall only be used after less restrictive measures have failed and with the approval of the Lieutenant. Restraints shall only be used so long as it reasonably appears necessary for the juvenile's protection or the protection of others (15 CCR 1142).

Juveniles in restraints shall be kept away from other unrestrained juveniles or monitored in such a way as to protect the juvenile from abuse (15 CCR 1142).

#### **406.11 PERSONAL PROPERTY**

The investigator taking custody of a juvenile offender or status offender at the Stanislaus County District Attorney's Office shall ensure a thorough search of the juvenile's property is made and all property is removed from the juvenile, especially those items that could compromise safety, such as pens, pencils, and belts.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Juveniles*

---

The personal property of a juvenile should be placed in a property bag. The property should be inventoried in the juvenile's presence and sealed into the bag. The property should be kept in a monitored or secure location until the juvenile is released from the custody of the Stanislaus County District Attorney's Office.

#### **406.12 SECURE CUSTODY**

Only juvenile offenders 14 years of age or older may be placed in secure custody (Welfare and Institutions Code § 207; 15 CCR 1145). Lieutenant approval is required before placing a juvenile offender in secure custody.

Secure custody should only be used for juvenile offenders when there is a reasonable belief that the juvenile is a serious risk of harm to themselves or others. Factors to be considered when determining if the juvenile offender presents a serious security risk to themselves or others include the following (15 CCR 1145):

- (a) Age, maturity, and delinquent history
- (b) Severity of offense for which the juvenile was taken into custody
- (c) The juvenile offender's behavior
- (d) Availability of staff to provide adequate supervision or protection of the juvenile offender
- (e) Age, type, and number of other individuals in custody at the facility

Members of this bureau shall not use secure custody for convenience when non-secure custody is, or later becomes, a reasonable option (15 CCR 1145).

When practicable and when no locked enclosure is available, handcuffing one hand of a juvenile offender to a fixed object while otherwise maintaining the juvenile in non-secure custody should be considered as the method of secure custody. An employee must be present at all times to ensure the juvenile's safety while secured to a stationary object (15 CCR 1148).

Juveniles shall not be secured to a stationary object for more than 60 minutes. Supervisor approval is required to secure a juvenile to a stationary object for longer than 60 minutes and every 30 minutes thereafter (15 CCR 1148). Supervisor approval should be documented.

The decision for securing a minor to a stationary object for longer than 60 minutes and every 30 minutes thereafter shall be based upon the best interests of the juvenile offender (15 CCR 1148).

#### **406.12.1 LOCKED ENCLOSURES**

A thorough inspection of the area shall be conducted before placing a juvenile into the enclosure. A second inspection shall be conducted after removing the juvenile. Any damage noted to the room should be photographed and documented in the crime report.

The following requirements shall apply to a juvenile offender who is held inside a locked enclosure:

- (a) The juvenile shall constantly be monitored by an audio/video system during the entire custody.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Juveniles*

---

- (b) Juveniles shall have constant auditory access to bureau members (15 CCR 1147).
- (c) Initial placement into and removal from a locked enclosure shall be logged (Welfare and Institutions Code § 207.1).
- (d) Unscheduled safety checks to provide for the health and welfare of the juvenile by a staff member, no less than once every 15 minutes, shall occur (15 CCR 1147; 15 CCR 1151).
  - 1. All safety checks shall be logged.
  - 2. The safety check should involve questioning the juvenile as to the juvenile's well-being (sleeping juveniles or apparently sleeping juveniles should be awakened).
  - 3. Requests or concerns of the juvenile should be logged.
- (e) Juveniles of different genders shall not be placed in the same locked room (15 CCR 1147).
- (f) Juvenile offenders should be separated according to severity of the crime (e.g., felony or misdemeanor).
- (g) Restrained juveniles shall not be mixed in a cell or room with unrestrained juveniles.

#### **406.13 SUICIDE ATTEMPT, DEATH, OR SERIOUS INJURY OF A JUVENILE**

The Lieutenant will ensure procedures are in place to address the suicide attempt, death, or serious injury of any juvenile held at the Stanislaus County District Attorney's Office (15 CCR 1142; 15 CCR 1047). The procedures will address:

- (a) Immediate notification of the on-duty supervisor, Chief of Investigations, and General Crimes Bureau Supervisor.
- (b) Notification of the parent, guardian, or person standing in loco parentis of the juvenile.
- (c) Notification of the appropriate prosecutor.
- (d) Notification of the County attorney.
- (e) Notification to the coroner.
- (f) Notification of the juvenile court.
- (g) In the case of a death, providing a report to the Attorney General under Government Code § 12525 within 10 calendar days of the death, and forwarding the same report to the Board of State and Community Corrections (BSCC) within the same time frame (15 CCR 1046).
- (h) A medical and operational review of deaths pursuant to 15 CCR 1046.
  - 1. A copy of the review report shall be provided to BSCC within 60 days of the death (15 CCR 1046).
- (i) Evidence preservation.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Juveniles*

---

#### 406.13.1 IN-CUSTODY DEATH PUBLICATION

The Chief of Investigations or the authorized designee should ensure that specified information relating to an in-custody death of a juvenile is posted on the bureau website as prescribed and within the time frames provided in Penal Code § 10008.

#### **406.14 INTERVIEWING OR INTERROGATING JUVENILE SUSPECTS**

No interview or interrogation of a juvenile should occur unless the juvenile has the apparent capacity to consent, and does consent, to an interview or interrogation.

Prior to conducting a custodial interrogation, including the waiver of *Miranda* rights, an investigator shall permit a juvenile 17 years of age or younger to consult with legal counsel in person, by telephone, or by video conference. The consultation may not be waived by the juvenile (Welfare and Institutions Code § 625.6).

Threats, physical harm, deception, or psychologically manipulative interrogation tactics shall not be used by an investigator during a custodial interrogation of a juvenile (Welfare and Institutions Code § 625.7).

The requirements to consult with legal counsel or to refrain from the use of prohibited interrogation techniques do not apply when (Welfare and Institutions Code § 625.6; Welfare and Institutions Code § 625.7):

- (a) Information is necessary to protect life or property from an imminent threat.
  - 1. The questions are limited to what is reasonably necessary to obtain the information relating to the threat.

#### 406.14.1 MANDATORY RECORDINGS OF JUVENILES

Any interrogation of an individual under 18 years of age who is in custody and suspected of committing murder shall be audio and video recorded when the interview takes place at a bureau facility, jail, detention facility, or other fixed place of detention. The recording shall include the entire interview and a *Miranda* advisement preceding the interrogation (Penal Code § 859.5).

This recording is not mandatory when (Penal Code § 859.5):

- (a) Recording is not feasible because of exigent circumstances that are later documented in a report.
- (b) The individual refuses to have the interrogation recorded, including a refusal any time during the interrogation, and the refusal is documented in a report. If feasible, the refusal shall be electronically recorded.
- (c) The custodial interrogation occurred in another state by law enforcement officers of that state, unless the interrogation was conducted with the intent to avoid the requirements of Penal Code § 859.5.
- (d) The interrogation occurs when no member conducting the interrogation has a reason to believe that the individual may have committed murder. Continued custodial interrogation concerning that offense shall be electronically recorded if the interrogating member develops a reason to believe the individual committed murder.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Juveniles*

---

- (e) The interrogation would disclose the identity of a confidential informant or would jeopardize the safety of an investigator, the individual being interrogated, or another individual. Such circumstances shall be documented in a report.
- (f) A recording device fails despite reasonable maintenance and the timely repair or replacement is not feasible.
- (g) The questions are part of a routine processing or booking, and are not an interrogation.
- (h) The suspect is in custody for murder and the interrogation is unrelated to a murder. However, if any information concerning a murder is mentioned during the interrogation, the remainder of the interrogation shall be recorded.

These recordings shall be retained until a conviction is final and all direct and habeas corpus appeals are exhausted, a court no longer has any jurisdiction over the individual, or the prosecution for that offense is barred (Penal Code § 859.5; Welfare and Institutions Code § 626.8).

#### **406.15 FORMAL BOOKING**

Any juvenile 14 years of age or older who is taken into custody for a felony, or any juvenile whose acts amount to a sex crime, shall be booked, fingerprinted, and photographed. For all other acts defined as crimes, juveniles may be booked, fingerprinted or photographed upon the approval from the Lieutenant, giving due consideration to the following:

- (a) The gravity of the offense
- (b) The past record of the offender
- (c) The age of the offender

#### **406.16 RELEASE OF INFORMATION CONCERNING JUVENILES**

Court decisions and legislation have combined to carefully specify situations in which information may be given out or exchanged when a case involves a juvenile. Members of this bureau shall not divulge any information regarding juveniles unless they are certain of the legal authority to do so.

Welfare and Institutions Code § 828 authorizes the release of certain information to other agencies. It shall be the responsibility of the Records Manager and the appropriate Investigative Bureau supervisors to ensure that personnel of those bureaus act within legal guidelines.

#### **406.17 BOARD OF STATE AND COMMUNITY CORRECTIONS CERTIFICATION**

The Training Lieutenant shall coordinate the procedures related to the custody of juveniles held at the Stanislaus County District Attorney's Office and ensure any required certification is maintained (Welfare and Institution Code § 210.2).

## On-Call and Call-Out Policy

### 407.1 PURPOSE AND SCOPE

All law enforcement agencies within Stanislaus County are encouraged to notify the on-call Stanislaus County District Attorney (SCDA) Deputy District Attorney (DDA) who will in turn notify the on-call Bureau of Investigation (BI) Criminal Investigator in the event of any of the following incidents:

- a. Suspicious death investigation
- b. Homicide investigation
- c. Officer involved shooting (OIS) as defined in the County-Wide OIS Protocol
- d. Fatal Fire investigations

#### 407.1.1 INVESTIGATIVE GOALS

The SCDA Office will provide Criminal Investigator(s) and a DDA to any requesting law enforcement agency within Stanislaus County to assist and collaborate in the investigation of any incident that has occurred or is suspected to have occurred as outlined above. This resource is provided to local law enforcement with five primary objectives:

- a. To provide law enforcement with additional investigative resources and legal expertise.
- b. To familiarize the Criminal Investigator and DDA with the crimes scene, evidence and other relevant intelligence for the purposes of follow-up investigation and trial preparation.
- c. To provide neutral and objective perspective to the investigation.
- d. To enhance the integrity of cases where there is a potential for conflict of interest issues.
- e. To insure proper procedures and techniques are utilized in the collection of evidence and statements so that they may be used in court proceedings at a later time.

### 407.2 ON-CALL POLICY

Criminal Investigators who are on call, absent mitigating circumstances, are expected to respond and assist requesting agencies in any capacity that is relevant to an on-going incident as described above. These efforts may include but are not limited to:

- a. Crime scene analysis
- b. Collection of evidence
- c. Suspect or witness interviews
- d. Preparation and execution of search or arrest warrants
- e. Surveillance contemporaneous to the crime
- f. Intelligence gathering functions

# Stanislaus County District Attorney's Office

## Policy Manual

### *On-Call and Call-Out Policy*

---

#### g. Autopsy attendance

In all cases, the scope of the Criminal Investigator's participation in the investigation should be at the discretion of the requesting agency.

Criminal Investigators assigned to this detail are expected to be proficient in the elements of homicide investigation. They are directed to represent the primary interest of the District Attorney in whatever capacity of the investigation that they participate. Similarly, the Criminal Investigator shall conform to the existing policies and procedures of the BI and the SCDA Office and conduct himself/herself in an exemplary manner.

#### 407.2.1 DURATION OF SERVICE

Per the Memorandum of Understanding, all Criminal Investigators are subject to on-call duties, at the discretion of the Chief Investigator or District Attorney. On-call duty will be for a period of seven (7) days, commencing at 0800 hours on each Friday morning. In the event Friday falls on a holiday, the Criminal Investigator will assume the duty at 0800 on the Thursday before the holiday.

#### 407.3 PREPARATION

During the period of on-call duty, Criminal Investigators will take all steps necessary to insure their availability for contact, to include activated and properly functioning home telephones, cellular telephones and issued radios. Criminal Investigators are expected to have their issued equipment readily available. This includes but is not limited to flashlight, firearm, handcuffs, radio, notebook, peace officer identification, business cards, ballistic vest and any other equipment reasonably necessary to carry out the assignment.

#### 407.4 NOTIFICATION

On-call Criminal Investigators will normally be notified by the on-call DDA of an incident requiring a response. In the event the Criminal Investigator is notified by the communications center or in some other manner the Criminal Investigator will notify the on-call DDA and coordinate a respon

- a. Under normal circumstances, the responding DDA will provide an update via email to DA\_187Notification about the known circumstances of the incident and whether a suspect has been identified or arrested.
- b. If the responding Criminal Investigator determines additional resources are needed to adequately assist the requesting law enforcement agency, the Criminal Investigator shall notify his/her Lieutenant and provide details outlining the need for additional resources. The Lieutenant will then evaluate the necessity and determine whether additional Criminal Investigators are needed.
- c. If the call-out involves an incident described within the Stanislaus County Officer Involved Protocol, the Criminal Investigator shall immediately notify their Lieutenant of the incident. The Lieutenant shall immediately notify the Chief Investigator of the incident who will in turn immediately notify the District Attorney. The incidents outlined in the County-Wide OIS Protocol are described as:

# Stanislaus County District Attorney's Office

## Policy Manual

### *On-Call and Call-Out Policy*

---

1. A peace officer, on or off duty, shoots and injures any person;
  2. An individual while in the custody or control of a peace officer(s) or law agency: dies, is seriously injured, or later dies as a result of force used while in the custody or control of a peace officer(s) or law enforcement agency. (This subsection does not apply to custodial deaths as defined in Penal Code section 5021, as there already exists a reporting protocol and procedure in place within the county);
  3. An individual is seriously injured or dies as a result of the operation of a police vehicle by a peace officer.
  4. At the request of any law enforcement agency for the SCDA to investigate any serious incident that said agency may deem appropriate.
- d. In the event the Fire Investigation Unit is called out on an arson investigation and it is determined a death occurred as a result of the fire or other circumstances, the Criminal Investigator assigned to FIU will immediately notify their Lieutenant who will in turn notify the on-call DDA.
- e. In the event of a serious injury or death to a peace officer, the same notification protocol shall be followed.
- f. Once the scene has been stabilized and a determination has been made that there is a need for personnel from the Victims Service Unit (VSU), the on-call DDA or Criminal Investigator will notify the on-call VSU staff member, provide an overview of the incident, and request a response.

#### **407.5 SCENE RESPONSIBILITIES**

It is the role of the SCDA Office to assist our local law enforcement neighbors as we work together to seek justice, service justice, and do justice. DDA's and Criminal Investigators will respond to the incident site to work with and assist our law enforcement partners. The SCDA will work with the investigating agency to ensure the investigation is conducted in a fair and professional manner that will serve the interests of justice, the community and those affected.

- a. As soon as practical after arrival at the scene, the assigned Criminal Investigator should contact the agency supervisor responsible for the investigation. Prior to entering the actual crime scene, the Criminal Investigator should make personal contact with the scribe of the crime scene log and note the exact time of entry.
- b. The primary role of the responding Criminal Investigator is to support the DDA and act as a liaison with law enforcement personnel. Once that mission has been fulfilled, Criminal Investigators are encouraged to seek out the law enforcement scene supervisor and offer assistance where needed. Diplomacy and decorum are essential in communications with the requesting agency.

### *On-Call and Call-Out Policy*

---

- c. The responding Criminal Investigator is responsible for updating his/her supervisor on the status of the case. In the event the Criminal Investigator remains at the scene longer than (4) hours, the Criminal Investigator will contact his/her Lieutenant for approval for additional overtime.
- d. The Criminal Investigator who was called out for the case is responsible to attend the autopsy. If for any reason the Criminal Investigator is unable to attend the autopsy, it will be that Investigators responsibility to contact their Lieutenant and make alternative arrangements in advance so the autopsy is covered by another Criminal Investigator. Criminal Investigators are expected to contact the coroner directly to confirm autopsy dates/times.
- e. The on-call Criminal Investigator will remain assigned to the incident unless the incident is one that falls into a specialty unit such as arson, narcotics or gangs.

#### **407.6 REPORTING**

Criminal Investigators shall document their involvement with any on-call related incident.

- a. As soon as reasonably practical after a call-out, the Criminal Investigator is directed to document their activities and participation in the investigation in the form of an investigative report.
- b. The investigative report should minimally include the time of notification, the time of arrival and departure from the scene. It should outline the Criminal Investigators personal observations and activities they were personally involved with. The report shall not include speculation or conjecture. The reports should not document third party statements related to them by other law enforcement officers.
- c. The report(s) when completed shall be forwarded to the Criminal Investigators Lieutenant for review and approval. Once approved, the report(s) will be loaded into the SCDA Records Management System (RMS). Copies of the Criminal Investigators report(s) will be shared with the primary investigative agency and their lead detective or investigator.



## Stanislaus County Officer Involved Protocol

### 408.1 PURPOSE AND SCOPE

Law enforcement officers perform a vital and often dangerous job in our communities. Situations will occur where peace officers must use deadly force; we expect that such force will be used only when legally necessary and as prescribed by law. When peace officers use deadly force, the public has a right to expect a thorough and neutral examination will be conducted of these incidents and that all parties shall be held legally accountable for their actions.

### 408.2 POLICY

The Stanislaus County District Attorney's Office (SCDA) and participating local law enforcement agencies agree that District Attorney personnel, which means at least one Deputy District Attorney (DDA) and one District Attorney Investigator (DAI) from the Bureau of Investigation (BI) upon notification, will immediately respond to the scene of any specified officer involved shooting, in-custody, or traffic related death as outlined in 611.3. In the event additional DAI's are needed, the responding DAI will coordinate resources through a BI Lieutenant.

### 408.3 INCIDENTS TO BE INVESTIGATED

This policy shall apply when any of the following incidents occur within in Stanislaus County:

- (a) A peace officer, on or off-duty, shoots and injures any person;
- (b) An individual while in the custody or control of a peace officer(s) or law enforcement agency: dies, is seriously injured, or later dies as a result of force used while in the custody or control of a peace officer(s) or law enforcement agency. (This subsection does not apply to custodial deaths as defined in Penal Code § 5021, as there already exists a reporting protocol and procedure in place with the County);
- (c) An individual is seriously injured or dies as a result of the operation of a police vehicle by a peace officer;
- (d) At the request of any law enforcement agency for the SCDA to investigate any serious incident that said agency may deem appropriate.

#### 408.3.1 OTHER USE OF FORCE INCIDENTS

Upon the request of any law enforcement agency, the SCDA will review any officer-involved use of force for criminal violations, even if not covered by this policy. Any case submitted for criminal review pursuant to this policy will be assessed like all other cases submitted to the SCDA and may result in Brady (Brady v. Maryland (1963) 373 U.S. 83) findings depending on the facts established during the investigation.

#### 408.3.2 POLICY JURISDICTION

This policy will also apply to peace officers employed by an agency outside of Stanislaus County if the incident occurs within Stanislaus County and a Stanislaus County agency assumes jurisdiction over the incident. This protocol will not apply where officers or deputies from Stanislaus County are involved in incidents that occur outside the borders of Stanislaus County.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Stanislaus County Officer Involved Protocol*

---

#### **408.4 NOTIFICATION TO DISTRICT ATTORNEY**

For all incidents listed within 611.3, it is the responsibility of the law enforcement agency investigating the incident to immediately notify the assigned on-call SCDA personnel. The law enforcement agency may notify the required SCDA personnel directly by calling the **on-call number 209-652-1296 or may utilize Stanislaus County Regional 911 (SR911)**. The on-call DDA and DAI will respond to the scene.

If a law enforcement agency turns over the investigation to another agency, both agencies shall notify the SCDA as set forth above. Notification should be made as soon as possible. Each agency should notify the SCDA immediately after notification is made to its own investigators.

SCDA personnel should be given a brief summary of all the facts known at the time, including location of the incident, command post location (if applicable), suggested access routes, and any safety concerns. The notification should be made as soon as possible, **preferably no later than 30 minutes after the incident**. An early response to the scene of an investigation is critical so that SCDA personnel may gain first-hand knowledge of lighting conditions, witness demeanor, trajectories, vehicle and pedestrian traffic conditions, etc.

#### **408.5 SUPERVISOR ON SCENE PROCEDURE**

The first field supervisor on scene (from any agency involved) shall obtain a public safety statement from the involved officer(s) as soon as it is safe and practical to do so. It is extremely important to get this information so that the proper investigation can be conducted and that the officers' rights are protected. The public safety questions should be based on and determined by the policy of the law enforcement agency involved.

The first field supervisor on scene should ensure the involved officer(s) secures their weapon until it is requested by the agency investigators handling the incident. There is no need to remove the officer's weapon publicly on scene. For consistency, the following criteria should be followed:

- (a) Handguns used by the involved officer(s) should be secured in his/her holster. The involved officer should be transported to their agency or the investigating agency's office with a buddy officer. The involved officer shall remain in uniform, or how they were dressed during the shooting, if medically appropriate to do so, until their uniform/weapon can be examined, documented, and collected;
- (b) Injured involved officers (taken to a hospital) should have their belt/holster/weapon secured by a field supervisor for later examination/collection by investigators;
- (c) Long guns used by involved officer(s) should be secured by a field supervisor for later examination/collection by investigators.

#### **408.6 JURISDICTION AT THE SCENE**

The investigating law enforcement agency shall be the agency that has primary jurisdiction over where the incident occurred. However, that agency may elect to transfer primary responsibility to another agency that will then have primary jurisdiction. The investigating law enforcement agency shall have the primary responsibility to conduct a thorough, objective and professional investigation of the incident. It shall be responsible for securing the location, collecting all physical

# Stanislaus County District Attorney's Office

## Policy Manual

### *Stanislaus County Officer Involved Protocol*

---

evidence, photographing and/or diagramming the scene and interviewing witnesses in cooperation with the district attorney personnel.

The responsibilities of the on-scene SCDA DAI personnel shall include the following:

- (a) Assist and advise the investigating officers on criminal law issues as they relate to the investigation;
- (b) Observe and participate fully with the investigative agency in the criminal investigation;
- (c) Advise and assist investigating officers as to the collection of evidence and the interview of witnesses, when appropriate.

District Attorney personnel will check in with the officer maintaining the incident scene log upon their arrival. As soon as practical, the officer in charge of the investigation will provide an initial briefing of the incident to District Attorney personnel. The briefing will consist of all relevant information known at the time, including, but not limited to:

- (a) Names and present whereabouts of the officer involved in the incident;
- (b) Names, addresses and present whereabouts of all civilian witnesses to the incident;
- (c) Statements of the officers, if not compelled pursuant to Government Code sections 3300, et.al. (Lybarger);
- (d) A summary of the physical evidence discovered;
- (e) A summary of witness statements and the status of the investigation;
- (f) A "walk through" at the scene, including witnesses' descriptions of the events and the evidence recovered; and
- (g) The medical condition of the injured parties.

If SCDA personnel determine that additional SCDA personnel are needed to assist with the investigation, additional DAI's or DDA's can be called to the scene.

408.6.1 CALIFORNIA DEPARTMENT OF JUSTICE AB 1506 OIS OF AN UNARMED CITIZEN Effective July 1, 2021, pursuant to AB 1506, the Department of Justice (DOJ) is required to investigate "incidents of an officer-involved shooting resulting in the death of an unarmed civilian." (Gov. Code, § 12525.3, subd. (b)(1).) The following is DOJ's understanding of the terms used in this statute, and is to be used as guidance for all law enforcement partners in determining whether a case falls within the ambit of AB 1506. These definitions are meant to apply only in the context of AB 1506, and these terms may have different meanings in other contexts or in different statutes. Notwithstanding these definitions, DOJ may elect to assume jurisdiction in cases where jurisdiction is unclear, or based on other extenuating circumstances, as determined by the Attorney General. (See Cal. Const., art V, § 13 [Attorney General is "chief law officer of the State" and has a duty "to see that the laws of the State are uniformly and adequately enforced"].)

- (a) "Officer-involved" A shooting is "officer-involved" if the death to the unarmed civilian is caused by a California peace officer, within the meaning of Penal Code section 830, acting under color of authority. All shootings committed by officers while on

# Stanislaus County District Attorney's Office

## Policy Manual

### *Stanislaus County Officer Involved Protocol*

---

duty are officer-involved shootings. Shootings committed by officers while off-duty are considered officer-involved shootings only if the officer is acting under color of authority. Officers are acting under "color of authority" when they are performing an act that is made possible only because they are clothed with the authority of law, or when they are acting under pretense of law. Conversely, officers are not acting under "color of authority" when they commit private acts in furtherance of personal pursuits. Shootings by correctional officers as defined in Penal Code section 830.55 are excluded.

- (b) "Shooting" A "shooting" is the discharge of a metal projectile by a firearm. A "firearm" is a "device, designed to be used as a weapon, from which is expelled through a barrel, a projectile by the force of an explosion or other form of combustion." (Pen. Code, § 16520.) A "shooting" does not include incidents involving the use of electronic control devices, stun guns, BB, pellet, air, gas-powered guns, or weapons that discharge rubber bullets or beanbags.
- (c) "Unarmed civilian" An "unarmed civilian" is "anyone who is not in possession of a deadly weapon." (Gov. Code, § 12525.3, subd. (a)(2).)
- (d) "Possession" A civilian is in "possession" if the weapon is under the civilian's dominion and control at the time of the shooting. Possession usually requires that the weapon is available for use. Where a civilian attempts to take control of an officer's firearm, the civilian is not in possession unless the officer loses control of the firearm.
- (e) "Deadly weapon" Deadly weapon includes, but is not limited to, any loaded weapon from which a shot, readily capable of producing death or other serious physical injury, may be discharged, or a switchblade knife, pilum, ballistic knife, metal knuckle knife, dagger, billy, blackjack, plastic knuckles, or metal knuckles." (Gov. Code, § 12525.3, subd. (a)(1).) All firearms, and BB/pellet guns, even if unloaded or inoperable, are deadly weapons. Objects that have a legitimate non-weapon purposes are considered deadly weapons only when, based on all the circumstances, they are actually being used in a manner likely to produce death or great bodily injury. The following are examples of objects that have been considered a deadly weapon when used in that manner: knives, box cutters, screwdrivers, bottles, chains, automobiles, rocks, razor blades, and iron bars. Replica firearms are not considered deadly weapons unless they are used in some particular manner likely to produce death or great bodily injury (e.g., as a bludgeon).
- (f) "Death" Death occurs when "[a]n individual ... has sustained either (1) irreversible cessation of circulatory and respiratory functions, or (2) irreversible cessation of all functions of the entire brain, including the brain stem[.]" (Health & Saf. Code, § 7180.) DOJ may assume responsibility for cases where death appears to be imminent.

Law Enforcement Agency's (LEA) Notification Responsibility Effective July 1, 2021, immediately notify the DOJ when the LEA has an incident of an officer-involved shooting resulting in the death of an unarmed civilian. When situations arise and it is undetermined if the civilian was unarmed, a notification to DOJ is still requested. **The Los Angeles Regional Criminal Information Clearinghouse (LA CLEAR) will be the central point of contact for all officer-involved shooting incident notifications: (800) 522-5327.**

# Stanislaus County District Attorney's Office

## Policy Manual

### *Stanislaus County Officer Involved Protocol*

---

#### **408.7 INTERVIEWS OF CIVILIAN WITNESSES**

SCDA personnel, with the investigating agency will attempt to locate, identify and interview all potential witnesses to an incident. SCDA personnel will be present and participate with the investigating agency in all interviews of civilian witnesses whenever possible. All witnesses shall be interviewed separately to maintain the integrity of their statements. All interviews should be electronically recorded, if possible.

#### **408.8 SEPARATION OF CRIMINAL AND ADMINISTRATIVE INVESTIGATIONS**

Law enforcement agencies may have the responsibility in an officer-involved shooting, in-custody or traffic related death investigation to address several issues, such as: (1) whether any criminal law violations have occurred, (2) whether any participant has incurred or is at risk of incurring civil liability, (3) whether departmental policies have been followed, (4) whether appropriate law enforcement tactics were utilized under the circumstances.

It is the District Attorney's role to determine whether any violation of criminal law may have occurred. However, the law enforcement agency may also administratively investigate other issues as well, and they may sometimes choose to conduct an administrative review concurrently with the criminal investigation.

During the course of an administrative inquiry, law enforcement agencies are authorized by law to compel their officers to give statements regarding matters that are the subjects of administrative investigations. (Public Safety Officer Procedural Bill of Rights Act, Government Code sections 3300 et seq.) However, the law provides that a compelled statement and any evidence derived therefrom shall be inadmissible in a criminal prosecution. Therefore, it is very important from the outset of an investigation to clearly separate the administrative from the criminal investigation. SCDA personnel should not be present during any compelled interview, nor should they receive any information concerning the content of a compelled statement, absent unusual circumstances. Because evidence derived from a compelled statement will be inadmissible in a criminal proceeding, care should be given to keep separate criminal and administrative investigations so as to not taint any findings that are ultimately made after the investigation has been completed.

DDA's and DAI's of the SCDA will respond to assist the investigating agency and, when appropriate, conduct their own independent investigation. The SCDA will work with the investigating agency to ensure that the inquiry is conducted in a fair and professional manner that will serve the interests of justice, the community, the involved officers, those persons injured and the families of those affected. The primary objective is to accurately, thoroughly and objectively investigate all relevant evidence and to determine the potential criminal liability, or lack thereof, of any party.

#### **408.9 INTERVIEWS OF SWORN PEACE OFFICERS**

All peace officer witnesses to the events of the incident shall be separately interviewed. The interviews should take place as soon as is practical and should be recorded. During the pendency of the investigation and prior to the interview, all witnesses or potential witnesses should be kept

# Stanislaus County District Attorney's Office

## Policy Manual

### *Stanislaus County Officer Involved Protocol*

---

apart to maintain the integrity of their individual statements. When appropriate, the interviews may take place at the scene to aid the officer in recalling and explaining the exact location of the parties and the events that took place.

SCDA personnel will be available to participate in interviews of law enforcement personnel. If the involved officer chooses to not make a voluntary statement and the law enforcement agency elects to compel a statement pursuant to the Public Safety Officers Procedural Bill of Rights Act (Government Code sections 3300 et seq.), SCDA personnel will be available to participate in the compelled interview at the request of the investigating agency, and consented to by the peace officer and, if the DDA assigned to the investigation determines, in his or her best judgment, that the presence of SCDA personnel will not compromise any criminal investigation.

The decision of whether to permit officers to view videotape of shooting incidents and, if so, whether this should occur before or after providing a verbal statement or filing a report, remains unresolved. Some argue that allowing an officer to view a videotape before making a statement may allow him or her to adjust the statement to conform to the video. Others contend that this process enhances an officer's memory and allows the officer to better recall actions or events that took place. (Agencies that usually allow viewing prior to making a statement still retain the administrative prerogative to make exceptions.) Videotapes shown following a statement or report avoid, to some degree, the perception that the officer adjusted his or her statement to fit the video recording. An officer who has already given a statement can use the video to clarify discrepancies and to elaborate, where necessary, on actions taken and recorded. Departments should also remember that video recordings have inherent limitations. They generally have a narrow field of view and may vary in quality. In addition, a video recording cannot capture all of the events, actions and surrounding circumstances of which an officer may have been aware; they cannot record all that an officer knew, or reasonably believed, at the time of the incident.

#### **408.10 BODY WORN CAMERAS/PATROL CAR CAMERAS**

It is now common place for agencies to use body worn cameras and/or patrol car cameras (hereafter collectively referred to as BWC video). It is imperative that all videos be immediately collected to assist the investigation. After collection, BWC video should be shared with the responding SCDA personnel to allow them to evaluate the complexity of the issues involved. The BWC video must be provided to the reviewing DDA as soon as possible. It is important to note that 2018 amendments to Penal Code §832. 7 and Government Code §6254 have placed significant restrictions on withholding BWC video from the public during the pendency of the investigation. Due to these amendments, the investigating agency and the SCDA may be required to go to court to protect the investigation - communication between the two agencies will now be more important than ever to ensure an investigation is not compromised by the premature release of BWC videos.

The involved agency may release video footage and provide a brief summary of the events if the agency feels it is in the best interest of the public and the agency exercises reasonable care not to make an extrajudicial statement that a prosecutor would be prohibited from making under State Bar Rule 3.6 or 3.8.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Stanislaus County Officer Involved Protocol*

---

#### **408.11 INVESTIGATIVE REPORTS**

It is the intent of the SCDA and involved law enforcement agencies to complete their review of these matters as quickly as possible, consistent with the primary goal of conducting a thorough and objective review of the facts.

The investigating agency will submit all relevant reports regarding the incident to the SCDA Bureau of Investigation (BI) as soon as possible and absent unusual circumstances within 90 days, depending on the policy of the investigating agency. As the investigation proceeds, reports should be forwarded to the BI as they are completed regardless of whether all reports are completed. This procedure will permit the review process to proceed simultaneously with the investigation. It will also permit timely requests for any additional investigation and clarification of completed reports if required.

#### **408.12 FINAL ACTION**

At the conclusion of the investigation, the SCDA will review and analyze all of the evidence to determine whether the officer acted lawfully. In 2019, the Legislature enacted AB 392 (effective 1/1/2020) which amended Penal Code § 196 and §835a. The amendments were designed to alter the landscape surrounding an officer's use of force.

Contained within amended §835a(a) is a statement that "the Legislature finds and declares" certain items set out in five separate subparts to be of significance. It is unclear if these subparts (§835a(a)(I) to (a)(5)) are actually part of the elements of the use of force defense for peace officers or merely a declarative statement. Subpart (a)(3) has language that a use of force must be "consistent with the law and agency policies." If the intent of the legislature was to graft agency policies into the evaluation of a use of force for criminal purposes, it could be argued that the law would be unconstitutional because an officer might be denied Equal Protection under the law. If the Legislature meant for a department's policies to be considered within the "totality of the circumstance" but not as a substitution for clear legislation, the law may be valid. As stated previously, the District Attorney is required to determine the criminal liability of those involved in proscribed acts and not to evaluate policies or civil liability. The District Attorney may review policies to see if an officer performed as trained which may demonstrate that in the totality of circumstances the officer's conduct was reasonable. The crime charging standards are the same for civilians and peace officers. The District Attorney's policies regarding crime charging are set forth in the District Attorney's Policies Manual, and can be best summarized as follows:

The prosecutor should charge only if the following four basic requirements are satisfied:

- (a) The prosecutor, based on a complete investigation and a thorough consideration of all pertinent facts readily available, is satisfied that the evidence proves that the accused is guilty of the crime to be charged;
- (b) There is legally sufficient, admissible evidence of a corpus delicti;
- (c) There is legally sufficient, admissible evidence of the accused's identity as the perpetrator of the crime charges; and

# Stanislaus County District Attorney's Office

## Policy Manual

### *Stanislaus County Officer Involved Protocol*

---

- (d) The prosecutor has considered the probability of conviction by an objective fact finder and has determined that the admissible evidence is of such convincing force that it would warrant conviction of the crime charged by a reasonable and objective fact finder after hearing all the evidence available to the prosecutor at the time of charging and after considering the most plausible, reasonably foreseeable defense inherent in the prosecution evidence.

If no charges are filed, the SCDA will issue a closing letter summarizing the results of the investigation and analyzing the evidence. This letter will address the question of whether or not there is proof beyond a reasonable doubt that a peace officer, or any other person, committed a crime and whether there was a justification or excuse. It is not the purpose of the SCDA to determine if any officer or deputy violated agency policy or procedure or committed any act which would be subject to civil sanctions. The closing letter shall be sent to the involved law enforcement agencies and, if requested by the involved law enforcement agencies and agreed to by the SCDA, the letter will be sent in accordance with the case of *Rackauckas v. Superior Court*, (2002) 104 Cal.App.4th 169.

#### **408.13 AGENCY PARTICIPATION**

The following Agencies hereby adopt the preceding Stanislaus County Officer Involved Protocol:



# Forensic Genetic Genealogy

## 409.1 PURPOSE AND SCOPE

This policy provides guidance for the use of forensic genetic genealogy (FGG) to generate investigative leads.

### 409.1.1 DEFINITIONS

Definitions related to this policy include:

**Combined DNA Index System (CODIS)** - An FBI computer software program that operates deoxyribonucleic acid (DNA) profile databases for law enforcement use.

**DNA typing laboratory** - A laboratory that analyzes biological samples, including extracted DNA, in order to provide various DNA profile types. State or local crime labs are generally not equipped to provide single nucleotide polymorphism (SNP) DNA profiles; therefore, the use of private DNA typing laboratories is often necessary for FGG.

**Extracted DNA** - The DNA isolated from a biological sample remaining after previous DNA testing has been completed.

**Forensic genetic genealogy (FGG)** - The process of obtaining a SNP DNA profile from a biological sample collected during an investigation; uploading the profile to a genetic genealogy site for comparison to the consumer profiles in the site's database to identify genetic relatives; and using the identified genetic relationships, as well as traditional genealogy research, to generate investigative leads.

**Genetic genealogist** - A genealogist who uses DNA testing with traditional genealogical research methods to assist law enforcement or private clients in identifying biological relatives of an individual.

**Genetic genealogy site** - A database of DNA profiles voluntarily submitted by public consumers for the purpose of identifying genetic relatives. The availability of genetic genealogy sites for law enforcement use varies depending on their terms of service.

**Short tandem repeat (STR) DNA profile** - The results of DNA typing in a format that can be processed through CODIS and state DNA databases. This is the type of DNA used in conventional non-FGG law enforcement investigations.

**Single nucleotide polymorphism (SNP) DNA profile** - The results of DNA typing in a format that enables an unknown DNA sample to be compared to the DNA profiles maintained by a genetic genealogy site. This is the DNA type used in FGG.

## 409.2 POLICY

The Stanislaus County District Attorney's Office's use of FGG will be in coordination with prosecutors, the Coroner, and other appropriate resources only in qualifying cases after reasonable conventional investigative methods have been pursued. Members will take reasonable

# Stanislaus County District Attorney's Office

## Policy Manual

### *Forensic Genetic Genealogy*

---

steps to maintain the integrity of the FGG process and safeguard the privacy rights of individuals whose DNA profiles are analyzed.

#### **409.3 CRITERIA FOR FGG USE**

Before using FGG, the lead investigator should coordinate with the supervisor to determine whether the case meets the following requirements:

- (a) Biological evidence collected as part of the underlying investigation (or extracted DNA from the biological evidence) is available for additional testing and is reasonably believed to be attributable to:
  - 1. The perpetrator of an unsolved violent felony.
  - 2. The unidentified human remains of a suspected homicide victim.
- (b) All reasonable conventional investigative methods have been utilized and all reasonable investigative leads have been pursued (e.g., relevant case information entered in the National Missing and Unidentified Persons System (NamUs) and the Violent Criminal Apprehension Program (ViCAP) national database).
- (c) An STR DNA profile has been developed from the biological evidence collected in the case and, absent unusual circumstances, has been uploaded to CODIS and any applicable state DNA database for comparison with negative results.

#### **409.4 COORDINATION**

Once a preliminary determination has been made that a case may qualify for the use of FGG, the lead investigating member should consult with the appropriate prosecutor to address current and prospective legal issues and determine if a search warrant is required.

In the case of unidentified human remains, the lead investigator should also consult with the Coroner.

#### **409.5 SUBMISSION OF SAMPLE**

The biological evidence or extracted DNA should be submitted to a DNA typing laboratory approved by the Bureau in order to obtain a SNP DNA profile.

Once a SNP DNA profile has been obtained from the biological evidence or extracted DNA, the lead investigating member should arrange for it to be compared to the SNP DNA profiles contained in one or more genetic genealogy sites to identify possible genetic relatives. The lead investigator should work with a qualified genetic genealogist as needed during this process.

When submitting a SNP DNA profile for comparison, the lead investigator or the authorized designee (e.g., assigned genetic genealogist) shall notify the genetic genealogy site that the request for comparison is from a law enforcement agency and confirm that the site's terms of service permit FGG for the type of case being investigated. The use of the SNP DNA profile and any subsequent comparison shall be limited to the original underlying investigation.

If at any time during the FGG process the case no longer meets the criteria for FGG use, the lead investigator should promptly notify the DNA typing laboratory, genetic genealogy site, and/or

### *Forensic Genetic Genealogy*

---

genetic genealogist to cease any further analysis and to return all evidence, data, and materials to the Bureau.

#### **409.6 ANALYSIS OF FGG DATA**

Once results of a comparison are received from a genetic genealogy site, the information should be evaluated by a genetic genealogist, who will assist the lead investigator in identifying potential investigative leads.

The lead investigator should promptly and diligently pursue each viable lead identified through the FGG process using traditional investigative methods, as appropriate, to:

- (a) Eliminate an individual as a potential suspect in the case.
- (b) Link an individual to the case as a potential suspect.
- (c) Identify human remains.

#### **409.7 COLLECTION OF THIRD-PARTY DNA SAMPLE**

If it is determined that a third-party DNA sample (i.e., from a person not likely to be a suspect in the investigation) should be collected and analyzed for FGG, consent from the third party should be obtained prior to collection.

If there is a reasonable belief that the integrity of the investigation would be compromised by seeking consent from the third party prior to collection, the lead investigator should consult with the prosecutor regarding applicable laws and procedures in both the jurisdiction of the investigation and the jurisdiction where the collection will occur, if different.

The use of a third-party DNA sample shall be limited to the original underlying investigation.

#### **409.8 POST-IDENTIFICATION**

Members shall not rely solely on FGG identification of a potential suspect for probable cause to make an arrest or obtain an arrest warrant. Unless there is sufficient evidence independent of the FGG data to support an arrest, a potential suspect identified through FGG should not be arrested until the suspect's identity is confirmed.

Members shall not rely solely on FGG to identify human remains unless there is sufficient evidence independent of the FGG data to declare the identification or confirmation testing has been completed.

Confirmatory DNA testing should be conducted by collecting a known DNA sample from the potential suspect or, in the case of unidentified human remains, from a close biological relative. This known DNA sample should be submitted for comparison to the original unknown STR DNA profile through conventional methods (e.g., in CODIS).

The lead investigator should consult with the prosecutor to determine the appropriate method of obtaining a known DNA sample.

Once the identity of a suspect or the identity of unidentified human remains has been confirmed through conventional DNA testing, the lead investigator should:

### *Forensic Genetic Genealogy*

---

- (a) Consult with the prosecutor to evaluate the entire investigative file for consideration of criminal charges or further investigation.
- (b) If applicable, consult with the Coroner for an amendment to a certificate of death.

#### **409.9 PRIVACY CONSIDERATIONS**

Members should make reasonable efforts to respect and protect the privacy of non-suspect genetic relatives identified through the FGG process. The names and identifying information of any non-suspect genetic relatives should not be included in official reports, probable cause declarations, or affidavits for search warrants and should not be disclosed unless otherwise required by law or court order.

The lead investigator should formally request that the SNP DNA profile be removed from all genetic genealogy sites upon identity confirmation and should retain a copy of the request for bureau records. The lead investigator should request that all case-related records and data provided to, or generated by, a genetic genealogist during the FGG process be returned to the Bureau.

#### **409.10 RETENTION OF DNA SAMPLES AND RELATED RECORDS**

Genetic information, including any derivative profiles and genetic genealogy site user information, should be retained in accordance with the established records retention schedule. The lead investigator should coordinate with the Lieutenant and provide adequate notice to the appropriate prosecutor's office before destroying any profiles or data obtained from the FGG process.

See the Property and Evidence Policy for guidelines regarding biological evidence, including DNA samples.

# Suspicious Activity Reporting

## 410.1 PURPOSE AND SCOPE

This policy provides guidelines for reporting and investigating suspicious and criminal activity.

### 410.1.1 DEFINITIONS

Definitions related to this policy include:

**Involved party** - An individual who has been observed engaging in suspicious activity, as defined in this policy, when no definitive criminal activity can be identified, thus precluding the person's identification as a suspect.

**Suspicious activity** - Any reported or observed activity that a member reasonably believes may have a nexus to any criminal act or attempted criminal act, or to foreign or domestic terrorism. Actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions). Examples of suspicious activity may include but are not limited to:

- Suspected pre-operational surveillance or intelligence gathering (e.g., photographing security features, asking questions about sensitive security-related subjects).
- Tests of security measures and response to incidents (e.g., "dry run," creating false alarms, attempts to enter secure areas without authorization).
- Suspicious purchases (e.g., purchasing large quantities of otherwise legal items, such as fertilizer, that could be used to create an explosive or other dangerous device).
- An individual in possession of such things as a hoax explosive or dispersal device, sensitive materials (e.g., passwords, access codes, classified government information), or coded or ciphered literature or correspondence.

**Suspicious Activity Report (SAR)** - An incident report used to document suspicious activity.

## 410.2 POLICY

The Stanislaus County District Attorney's Office recognizes the need to protect the public from criminal conduct and acts of terrorism and shall lawfully collect, maintain and disseminate information regarding suspicious activities, while safeguarding civil liberties and privacy protections.

## 410.3 RESPONSIBILITIES

The General Crimes Lieutenant and authorized designees will manage SAR activities. Authorized designees should include supervisors who are responsible for bureau participation in criminal intelligence systems as outlined in the Criminal Organizations Policy.

The responsibilities of the General Crimes Lieutenant include, but are not limited to:

- (a) Remaining familiar with those databases available to the Bureau that would facilitate the purpose of this policy.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Suspicious Activity Reporting*

---

- (b) Maintaining adequate training in the area of intelligence gathering to ensure no information is being maintained that would violate the law or civil rights of any individual.
- (c) Ensuring a process is available that would allow members to report relevant information. The process should be designed to promote efficient and quick reporting, and should not be cumbersome, duplicative or complicated.
- (d) Ensuring that members are made aware of the purpose and value of documenting information regarding suspicious activity, as well as the databases and other information resources that are available to the Bureau.
- (e) Ensuring that SAR information is appropriately disseminated to members in accordance with their job responsibilities.
- (f) Coordinating investigative follow-up, if appropriate.
- (g) Coordinating with any appropriate agency or fusion center.
- (h) Ensuring that, as resources are available, the Bureau conducts outreach that is designed to encourage members of the community to report suspicious activity and that outlines what they should look for and how they should report it (e.g., website, public service announcements).

#### **410.4 REPORTING AND INVESTIGATION**

Any bureau member receiving information regarding suspicious activity should take any necessary immediate and appropriate action, including a request for tactical response or immediate notification of specialized entities, when applicable. Any non-sworn member who receives such information should ensure that it is passed on to an investigator in a timely manner.

If the suspicious activity is not directly related to a reportable crime, the member should prepare a SAR and include information about involved parties and the circumstances of the incident. If, during any investigation, an investigator becomes aware of suspicious activity that is unrelated to the current investigation, the information should be documented separately in a SAR and not included in the original incident report. The report number of the original incident should be included in the SAR as a cross reference. A SAR should be processed as any other incident report.

#### **410.5 HANDLING INFORMATION**

The Records Bureau will forward copies of SARs, in a timely manner, to the following:

- Investigative Bureau supervisor
- Crime Analysis Unit
- Other authorized designees

# Generative Artificial Intelligence Use

## 411.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for bureau use of generative artificial intelligence (GenAI). This policy does not apply to artificial intelligence that is integrated into facial recognition applications, voice recognition applications, biometric access controls, or software that redacts documents or video or similar applications.

Additional guidelines for the use of bureau information technology resources are found in the Information Technology Use Policy.

### 411.1.1 DEFINITIONS

Definitions related to this policy include:

**Generative artificial intelligence (GenAI)** - A type of artificial intelligence that is algorithmically trained on one or more large data sets and designed to generate new and unique data (e.g., text, pictures, video) in response to a prompt (generally questions, instructions, images, or video) input by the user.

## 411.2 POLICY

The use of GenAI systems carries unique benefits within a law enforcement agency, providing ways to increase operational efficiency, enhance bureau procedures, and improve the overall effectiveness of the Stanislaus County District Attorney's Office.

However, the prompts input into GenAI systems can present risks to both individuals and law enforcement agencies by making accessible to the public information such as bureau tactics, investigative and training techniques, confidential information (e.g., confidential informants, protected information), active investigations, and security procedures. In addition, without safeguards in place, GenAI can produce unintended discriminatory or biased output as well as content that is inaccurate, misleading, or copyrighted.

It is the policy of the Bureau to develop, implement, and use GenAI ethically and responsibly in a way that minimizes potential risk and harm in accordance with the guidelines set forth below.

Any function carried out by a member of the Bureau using GenAI is subject to the same laws, rules, and policies as if carried out without the use of GenAI. The use of GenAI does not permit any law, rule, or policy to be bypassed or ignored.

## 411.3 RESPONSIBILITIES

### 411.3.1 CHIEF OF INVESTIGATIONS

The Chief of Investigations or an authorized designee shall approve all GenAI systems, their acceptable uses, and their authorized user groups prior to the use, implementation, or development for any bureau functions.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Generative Artificial Intelligence Use*

---

#### 411.3.2 AI COORDINATOR

The Chief of Investigations shall appoint the Information and Technology Manager as the AI coordinator.

The responsibilities of the AI coordinator include but are not limited to:

- (a) Evaluating potential GenAI systems and recommending those GenAI systems that appear to be appropriate and trustworthy to the Chief of Investigations or the authorized designee. The trustworthiness of GenAI systems should be evaluated by balancing the following characteristics:
  - 1. Validity and reliability - The system's apparent ability to meet the intended purpose and fulfill the needs of the Bureau consistently over time.
  - 2. Safety - Any apparent risk to human life, health, property, or the environment that could result from the bureau's use of the system.
  - 3. Security and resiliency - The system's capability to prevent unauthorized access and misuse and its ability to return to normal function should misuse occur.
  - 4. Accountability and transparency - The ability to track and measure the system's use and activity through histories, audit logs, and other processes to provide insight about the system and identify potential sources of error, bias, or vulnerability.
  - 5. Explainability and interpretability - The ability of the user to understand the purpose and impact of the system, how and why the system reached the resulting output, and what the output means for the user.
  - 6. Privacy - The ability of the system to protect confidentiality and meet applicable privacy standards for the types of data intended to be input into the system (e.g., state privacy laws, Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA)).
  - 7. Fairness - The ability of the system to operate in a way that avoids or minimizes bias and discrimination.
- (b) Ensuring appropriate contractual safeguards are in place to manage third-party use of bureau data and to restrict the use of input in AI training data sets. If the input of protected information is necessary for the proper use of the GenAI system, an information-exchange agreement in compliance with applicable rules and standards (e.g., CJIS requirements) should be used to outline the roles, responsibilities, and data ownership between the Bureau and third-party vendor.
- (c) Coordinating with others within the Bureau and County, such as the information technology or legal departments, as appropriate to ensure GenAI systems are procured, implemented, and used appropriately.
- (d) Maintaining a list or inventory of bureau-approved GenAI systems and, when appropriate for bureau transparency, making the list or inventory available to the public.
- (e) Developing and maintaining appropriate procedures related to the use of GenAI systems, including procedures for editing and fact-checking output.



### *Generative Artificial Intelligence Use*

---

- (f) Ensuring any public-facing GenAI systems notify the user that GenAI is being used.
- (g) Developing and updating training for the authorized users of each bureau-approved GenAI system.
- (h) Ensuring access to bureau GenAI systems is limited to authorized users and establishing requirements for user credentials such as two-factor authentication and appropriate password parameters.
- (i) Conducting audits at reasonable time intervals for each of the GenAI systems utilized by the Bureau to evaluate the performance and effectiveness of each approved system and to determine if it continues to meet the bureau's needs and expectations of trustworthiness. The coordinator should arrange for audits to be conducted by an external source, as needed.
- (j) Ensuring each GenAI system is updated and undergoes additional training as reasonably appears necessary in an effort to avoid the use of outdated information or technologies.
- (k) Keeping abreast of advancements in GenAI and any GenAI-related legal developments.
- (l) Reviewing this policy and bureau practices and proposing updates as needed to the Chief of Investigations.
- (m) Developing procedures in coordination with the *Brady* information coordinator and the Records Manager for the compilation and potential release of any discovery or records related to the use of GenAI systems consistent with *Brady* and the California Public Records Act.

#### **411.4 USE OF GENERATIVE AI**

The use of bureau GenAI systems by bureau members shall be limited to official work-related purposes, and members shall only access and use GenAI systems for which they have been authorized and received proper training.

Members shall use AI-generated content as an informational tool and not as a substitution for human judgment or decision-making. Members should not represent AI-generated content as their own original work.

AI-generated content should be considered draft material only and shall be thoroughly reviewed prior to use. Before relying on AI-generated content, members should:

- (a) Obtain independent sources for information provided by GenAI and take reasonable steps to verify that the facts and sources provided by GenAI are correct and reliable.
- (b) Review prompts and output for indications of bias and discrimination and take steps to mitigate its inclusion when reasonably practicable (see the Bias-Based Policing Policy).
- (c) Include a statement in the final document or work product that GenAI was used to aid in its production.

### *Generative Artificial Intelligence Use*

---

#### **411.4.1 PRIVACY CONSIDERATIONS**

Information not otherwise available to the public, including data reasonably likely to compromise an investigation, reveal confidential law enforcement techniques, training, or procedures, or risk the safety of any individual if it were to become publicly accessible, should not be input into a GenAI system unless contractual safeguards are in place to prevent such information from becoming publicly accessible. Members should instead use generic unidentifiable inputs, such as "suspect" or "victim," and hypothetical scenarios whenever possible.

Protected information should only be input into GenAI systems that have been approved for such use and comply with applicable privacy laws and standards (see the Protected Information Policy).

#### **411.5 PROHIBITED USE**

Members shall not use GenAI systems to rationalize a law enforcement decision, or as the sole basis of research, interpretation, or analysis of the law or facts related to a law enforcement contact or investigation.

Members shall not create user accounts in their official capacity or input work-related data (including information learned solely in the scope of their employment) into publicly available GenAI systems unless the system has been approved by the Chief of Investigations or the authorized designee for the intended use.

#### **411.6 TRAINING**

The AI coordinator should ensure that all members authorized to use GenAI have received appropriate initial training that is suitable for their role and responsibilities prior to their use of GenAI and receive periodic refresher training. Training should include but is not limited to the following:

- (a) A review of this policy
- (b) The need for human oversight of GenAI outputs
- (c) The interpretation, review, and verification of GenAI output
- (d) Checking GenAI output for bias or protected information
- (e) Ethical use of GenAI technology
- (f) Data security and privacy concerns

## Media Relations

### 412.1 PURPOSE AND SCOPE

This policy provides guidelines for the release of official bureau information to the media. It also addresses coordinating media access to scenes of disasters, criminal investigations, emergencies, and other law enforcement activities.

### 412.2 RESPONSIBILITIES

The ultimate authority and responsibility for the release of information to the media shall remain with the Chief of Investigations. In situations not warranting immediate notice to the Chief of Investigations and in situations where the Chief of Investigations has given prior approval, Lieutenants,, and designated Public Information Officers (PIOs) may prepare and release information to the media in accordance with this policy and the applicable laws regarding confidentiality.

### 412.3 ACCESS

Authorized media representatives shall be provided access to scenes of disasters, criminal investigations, emergencies, and other law enforcement activities as required by law.

Access by the media is subject to the following conditions (Penal Code § 409.5(d)):

- (a) The media representative shall produce valid press credentials that shall be prominently displayed at all times while in areas otherwise closed to the public. Media representatives may not bring or facilitate the transport of an unauthorized person into a closed area unless it is for the safety of the person.
- (b) Media representatives may be prevented from interfering with emergency operations and criminal investigations.
  - 1. Based upon available resources, reasonable effort should be made to provide a safe staging area for the media that is near the incident and that will not interfere with emergency or criminal investigation operations. All information released to the media should be coordinated through the PIO or other designated spokesperson.
- (c) No member of this bureau who is under investigation shall be subjected to media visits or interviews without the consent of the involved member (Government Code § 3303(e)).
- (d) Media interviews with individuals who are in custody should not be permitted without the approval of the Chief of Investigations and the express consent of the person in custody.

#### 412.3.1 CRITICAL OPERATIONS

A critical incident or tactical operation should be handled in the same manner as a crime scene, except the media should not be permitted within the inner perimeter of the incident, subject to any restrictions as determined by the supervisor in charge. Bureau members shall not jeopardize

# Stanislaus County District Attorney's Office

## Policy Manual

### *Media Relations*

---

a critical incident or tactical operation in order to accommodate the media. All comments to the media shall be coordinated through a supervisor or the PIO.

#### **412.3.2 TEMPORARY FLIGHT RESTRICTIONS**

Whenever the presence of media or other aircraft pose a threat to public or member safety or significantly hamper incident operations, the field supervisor should consider requesting a Temporary Flight Restriction (TFR). All requests for a TFR should be routed through the Lieutenant. The TFR request should include specific information regarding the perimeter and altitude necessary for the incident and should be requested through the appropriate control tower. If the control tower is not known, the Federal Aviation Administration (FAA) should be contacted (14 CFR 91.137).

#### **412.4 POLICY**

It is the policy of the Stanislaus County District Attorney's Office to protect the privacy rights of individuals, while releasing non-confidential information to the media regarding topics of public concern. Information that has the potential to negatively affect investigations will not be released.

#### **412.5 PROVIDING ADVANCE INFORMATION**

To protect the safety and rights of bureau members and other persons, advance information about planned actions by law enforcement personnel, such as movement of persons in custody or the execution of an arrest or search warrant, should not be disclosed to the media, nor should media representatives be invited to be present at such actions except with the prior approval of the Chief of Investigations.

Any exceptions to the above should only be considered for the furtherance of legitimate law enforcement purposes. Prior to approving any exception, the Chief of Investigations will consider, at a minimum, whether the release of information or presence of the media would unreasonably endanger any individual, prejudice the rights of any person, or is otherwise prohibited by law.

#### **412.6 MEDIA REQUESTS**

Any media request for information or access to a law enforcement incident shall be referred to the PIO, or if unavailable, to the first available supervisor. Prior to releasing any information to the media, members shall consider the following:

- (a) At no time shall any member of this bureau make any comment or release any official information to the media without prior approval from a supervisor or the PIO.
- (b) In situations involving multiple agencies or government departments, every reasonable effort should be made to coordinate media releases with the authorized representative of each involved agency prior to the release of any information by this bureau.
- (c) Under no circumstance should any member of this bureau make any comments to the media regarding any law enforcement incident not involving this bureau without prior approval of the Chief of Investigations. Under these circumstances the member should direct the media to the agency handling the incident.

### *Media Relations*

---

#### **412.7 CONFIDENTIAL OR RESTRICTED INFORMATION**

It shall be the responsibility of the PIO to ensure that confidential or restricted information is not inappropriately released to the media (see the Records Maintenance and Release and Personnel Records policies). When in doubt, authorized and available legal counsel should be consulted prior to releasing any information.

##### **412.7.1 EMPLOYEE INFORMATION**

The identities of investigators involved in shootings or other critical incidents may only be released to the media upon the consent of the involved investigator or upon a formal request filed.

Any requests for copies of related reports or additional information not contained in the information log (see the Information Log section in this policy), including the identity of investigators involved in shootings or other critical incidents, shall be referred to the PIO.

Requests should be reviewed and fulfilled by the Custodian of Records, or if unavailable, the Lieutenant or the authorized designee. Such requests will be processed in accordance with the provisions of the Records Maintenance and Release Policy and public records laws.

#### **412.8 RELEASE OF INFORMATION**

The Bureau may routinely release information to the media without receiving a specific request. This may include media releases regarding critical incidents, information of public concern, updates regarding significant incidents, or requests for public assistance in solving crimes or identifying suspects. This information may also be released through the bureau website or other electronic data sources.

##### **412.8.1 INFORMATION LOG**

The Bureau will maintain a daily information log of significant law enforcement activities. Log entries shall only contain information that is deemed public information and not restricted or confidential by this policy or applicable law. Upon request, the log entries shall be made available to media representatives through the Lieutenant.

The daily information log will generally include:

- (a) The date, time, location, case number, type of crime, extent of injury or loss, and names of individuals involved in crimes occurring within this jurisdiction, unless the release of such information would endanger the safety of any individual or jeopardize the successful completion of any ongoing investigation, or the information is confidential (e.g., juveniles or certain victims).
- (b) The date, time, location, case number, name, birth date, and charges for each person arrested by this bureau, unless the release of such information would endanger the safety of any individual or jeopardize the successful completion of any ongoing investigation or the information is confidential (e.g., juveniles).
- (c) The time and location of other significant law enforcement activities or requests for service with a brief summary of the incident.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Media Relations*

---

At no time shall identifying information pertaining to a juvenile arrestee (13 years of age and under), victim, or witness be publicly released without prior approval of a competent court. The identity of a minor 14 years of age or older shall not be publicly disclosed unless the minor has been arrested for a serious felony and the release of such information has been approved by the Lieutenant (Welfare and Institutions Code § 827.5).

Identifying information concerning deceased individuals shall not be released to the media until notification of next of kin or otherwise cleared through the Coroner.

Any requests for copies of related reports or additional information not contained in this log shall be referred to the designated bureau media representative, the custodian of records, or if unavailable, to the Lieutenant. Such requests will generally be processed in accordance with the provisions of the Public Records Act (see the Records Maintenance and Release Policy).

# Criminal Organizations

## 413.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure that the Stanislaus County District Attorney's Office appropriately utilizes criminal intelligence systems and temporary information files to support investigations of criminal organizations and enterprises.

### 413.1.1 DEFINITIONS

Definitions related to this policy include:

**Criminal intelligence system** - Any record system that receives, stores, exchanges or disseminates information that has been evaluated and determined to be relevant to the identification of a criminal organization or enterprise, its members or affiliates. This does not include temporary information files.

## 413.2 POLICY

The Stanislaus County District Attorney's Office recognizes that certain criminal activities, including but not limited to gang crimes and drug trafficking, often involve some degree of regular coordination and may involve a large number of participants over a broad geographical area.

It is the policy of this bureau to collect and share relevant information while respecting the privacy and legal rights of the public.

## 413.3 CRIMINAL INTELLIGENCE SYSTEMS

No bureau member may create, submit to or obtain information from a criminal intelligence system unless the Chief of Investigations has approved the system for bureau use.

Any criminal intelligence system approved for bureau use should meet or exceed the standards of 28 CFR 23.20.

A designated supervisor will be responsible for maintaining each criminal intelligence system that has been approved for bureau use. The supervisor or the authorized designee should ensure the following:

- (a) Members using any such system are appropriately selected and trained.
- (b) Use of every criminal intelligence system is appropriately reviewed and audited.
- (c) Any system security issues are reasonably addressed.

### 413.3.1 GANG DATABASES

The Chief of Investigations may approve participation by the gang unit in a shared criminal gang intelligence database, such as CALGANG®. Members must obtain the requisite training before accessing any such database (11 CCR 751.6).

It is the gang unit supervisor's responsibility to determine whether any report or FI contains information that would qualify for entry into the database. Prior to designating any person as

# Stanislaus County District Attorney's Office

## Policy Manual

### *Criminal Organizations*

---

a suspected gang member, associate, or affiliate in a shared gang database; or submitting a document to the Attorney General's office for the purpose of designating a person in a shared gang database; or otherwise identifying the person in a shared gang database, the gang unit supervisor shall provide written notice to the person and, if the person is under the age of 18, to his/her parent or guardian of the designation and the basis for the designation, unless providing that notification would compromise an active criminal investigation or compromise the health or safety of a minor. Notice shall also describe the process to contest the designation (Penal Code § 186.34).

The person, an attorney working on his/her behalf, or his/her parent or guardian (if the person is under 18 years of age) may request, in writing, information as to whether the person is designated as a suspected gang member, associate, or affiliate in a shared gang database accessible by the Bureau, the basis for that designation, and the name of the agency that made the designation. The Bureau shall respond to a valid request in writing within 30 days, and shall provide the information requested unless doing so would compromise an active investigation or compromise the health and safety of the person if he/she is under 18 years of age (Penal Code § 186.34).

The person, or his/her parent or guardian if the person is under 18 years of age, may contest the designation by submitting written documentation, which shall be reviewed by the gang unit supervisor. If it is determined that the person is not a suspected gang member, associate, or affiliate, the person shall be removed from the database. The person and the parent or guardian shall be provided written verification of the bureau's decision within 30 days of receipt of the written documentation contesting the designation and shall include the reason for a denial when applicable (Penal Code § 186.34).

The gang unit supervisor should forward reports or FIs to the Records Bureau after appropriate database entries are made. The supervisor should clearly mark the report/FI as gang intelligence information.

It is the responsibility of the Records Bureau supervisor to retain reports and FIs in compliance with the database rules and any applicable end user agreement.

Records contained in a shared gang database shall not be disclosed for employment or military screening purposes, and shall not be disclosed for the purpose of enforcing federal immigration law unless required by state or federal statute or regulation (Penal Code § 186.36).

#### **413.4 TEMPORARY INFORMATION FILE**

No member may create or keep files on individuals that are separate from the approved criminal intelligence system. However, members may maintain temporary information that is necessary to actively investigate whether a person or group qualifies for entry into the bureau-approved criminal intelligence system only as provided in this section. Once information qualifies for inclusion, it should be submitted to the supervisor responsible for consideration of criminal intelligence system entries.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Criminal Organizations*

---

#### 413.4.1 FILE CONTENTS

A temporary information file may only contain information and documents that, within one year, will have a reasonable likelihood to meet the criteria for entry into an authorized criminal intelligence system.

Information and documents contained in a temporary information file:

- (a) Must only be included upon documented authorization of the responsible bureau supervisor.
- (b) Should not be originals that would ordinarily be retained by the Records Bureau or Evidence Room, but should be copies of, or references to, retained documents such as copies of reports, FI forms, SR 911 records or booking forms.
- (c) Shall not include opinions. No person, organization or enterprise shall be labeled as being involved in crime beyond what is already in the document or information.
- (d) May include information collected from publicly available sources or references to documents on file with another government agency. Attribution identifying the source should be retained with the information.

#### 413.4.2 FILE REVIEW AND PURGING

The contents of a temporary information file shall not be retained longer than one year. At the end of one year, the contents must be purged.

The designated supervisor shall periodically review the temporary information files to verify that the contents meet the criteria for retention. Validation and purging of files is the responsibility of the supervisor.

#### **413.5 INFORMATION RECOGNITION**

Bureau members should document facts that suggest an individual, organization or enterprise is involved in criminal activity and should forward that information appropriately. Examples include, but are not limited to:

- (a) Gang indicia associated with a person or residence.
- (b) Information related to a drug-trafficking operation.
- (c) Vandalism indicating an animus for a particular group.
- (d) Information related to an illegal gambling operation.

Bureau supervisors who utilize an authorized criminal intelligence system should work with the Lieutenant to train members to identify information that may be particularly relevant for inclusion.

#### **413.6 RELEASE OF INFORMATION**

Bureau members shall comply with the rules of an authorized criminal intelligence system regarding inquiries and release of information.

### *Criminal Organizations*

---

Information from a temporary information file may only be furnished to bureau members and other law enforcement agencies on a need-to-know basis and consistent with the Records Maintenance and Release Policy.

When an inquiry is made by the parent or guardian of a juvenile as to whether that juvenile's name is in a temporary information file, such information should be provided by the supervisor responsible for the temporary information file, unless there is good cause to believe that the release of such information might jeopardize an ongoing criminal investigation.

#### **413.7 CRIMINAL STREET GANGS**

The Investigative Bureau supervisor should ensure that there are an appropriate number of bureau members who can:

- (a) Testify as experts on matters related to criminal street gangs, and maintain an above average familiarity with:
  - 1. Any organization, associate or group of three or more persons that meets the definition of a criminal street gang under Penal Code § 186.22(f).
  - 2. Identification of a person as a criminal street gang member and criminal street gang-related crimes.
  - 3. The California Street Terrorism Enforcement and Prevention Act (Penal Code § 186.21 et seq.), associated crimes and what defines a criminal street gang (Penal Code § 186.22).
- (b) Coordinate with other agencies in the region regarding criminal street gang-related crimes and information.
- (c) Train other members to identify gang indicia and investigate criminal street gang-related crimes.

#### **413.8 TRAINING**

The Lieutenant should provide training on best practices in the use of each authorized criminal intelligence system to those tasked with investigating criminal organizations and enterprises. Training should include:

- (a) The protection of civil liberties.
- (b) Participation in a multiagency criminal intelligence system.
- (c) Submission of information into a multiagency criminal intelligence system or the receipt of information from such a system, including any governing federal and state rules and statutes.
- (d) The type of information appropriate for entry into a criminal intelligence system or temporary information file.
- (e) The review and purging of temporary information files.

### *Criminal Organizations*

---

#### 413.8.1 SHARED GANG DATABASE TRAINING

The Lieutenant should ensure that members who are authorized users of a shared gang database receive the required training from the California Department of Justice (DOJ) or an instructor certified by the DOJ that includes comprehensive and standardized training on the use of shared gang databases, and any other associated training required by the Bureau (Penal Code § 186.36; 11 CCR 751.6).

## Crime and Disaster Scene Integrity

### 414.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance in handling a major crime or disaster.

### 414.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to secure crime or disaster scenes so that evidence is preserved, and to identify and mitigate the dangers associated with a major crime or disaster scene for the safety of the community and those required to enter or work near the scene.

### 414.3 SCENE RESPONSIBILITY

The first investigator at the scene of a crime or major incident is generally responsible for the immediate safety of the public and preservation of the scene. Investigators shall also consider officer safety and the safety of those persons entering or exiting the area, including those rendering medical aid to any injured parties. Once an investigator has assumed or been assigned to maintain the integrity and security of the crime or disaster scene, the investigator shall maintain the crime or disaster scene until he/she is properly relieved by a supervisor or other designated person.

### 414.4 FIRST RESPONDER CONSIDERATIONS

The following list generally describes the first responder's function at a crime or disaster scene. This list is not intended to be all-inclusive, is not necessarily in order and may be altered according to the demands of each situation:

- (a) Broadcast emergency information, including requests for additional assistance and resources.
- (b) Provide for the general safety of those within the immediate area by mitigating, reducing or eliminating threats or dangers.
- (c) Locate or identify suspects and determine whether dangerous suspects are still within the area.
- (d) Provide first aid to injured parties if it can be done safely.
- (e) Evacuate the location safely as required or appropriate.
- (f) Secure the inner perimeter.
- (g) Protect items of apparent evidentiary value.
- (h) Secure an outer perimeter.
- (i) Identify potential witnesses.
- (j) Start a chronological log noting critical times and personnel allowed access.

### 414.5 SEARCHES

Investigators arriving at crime or disaster scenes are often faced with the immediate need to search for and render aid to victims, and to determine if suspects are present and continue to pose a

# Stanislaus County District Attorney's Office

## Policy Manual

### *Crime and Disaster Scene Integrity*

---

threat. Once investigators are satisfied that no additional suspects are present and/or there are no injured persons to be treated, those exigent circumstances will likely no longer exist. Investigators should thereafter secure the scene and conduct no further search until additional or alternate authority for the search is obtained, such as consent or a search warrant.

#### **414.5.1 CONSENT**

When possible, investigators should seek written consent to search from authorized individuals. However, in the case of serious crimes or major investigations, it may be prudent to also obtain a search warrant. Consent as an additional authorization may be sought, even in cases where a search warrant has been granted.

#### **414.6 EXECUTION OF HEALTH ORDERS**

Any sworn member of this bureau is authorized to enforce all orders of the local health officer that have been issued for the purpose of preventing the spread of any contagious, infectious or communicable disease (Health and Safety Code § 120155).

# Domestic Violence

## 415.1 PURPOSE AND SCOPE

The purpose of this policy is to provide the guidelines necessary to deter, prevent and reduce domestic violence through vigorous enforcement and to address domestic violence as a serious crime against society. The policy specifically addresses the commitment of this bureau to take enforcement action when appropriate, to provide assistance to victims and to guide investigators in the investigation of domestic violence.

### 415.1.1 DEFINITIONS

Definitions related to this policy include:

**Court order** - All forms of orders related to domestic violence that have been issued by a court of this state or another, whether civil or criminal, regardless of whether service has been made.

## 415.2 POLICY

The Stanislaus County District Attorney's Office's response to incidents of domestic violence and violations of related court orders shall stress enforcement of the law to protect the victim and shall communicate the philosophy that domestic violence is criminal behavior. It is also the policy of this bureau to facilitate victims' and offenders' access to appropriate civil remedies and community resources whenever feasible. When a member of the community reports an incident of domestic violence to the Bureau will take all necessary steps to assist the victim and ensure it is properly reported to the agency having jurisdiction over the investigation. In the unlikely event the Bureau takes an initiating (courtesy report), the following policy will be adhered to.

## 415.3 OFFICER SAFETY

The investigation of domestic violence cases often places investigators in emotionally charged and sometimes highly dangerous environments. No provision of this policy is intended to supersede the responsibility of all investigators to exercise due caution and reasonable care in providing for the safety of any investigators and parties involved.

## 415.4 INVESTIGATIONS

The following guidelines should be followed by investigators when investigating domestic violence cases:

- (a) Calls of reported, threatened, imminent, or ongoing domestic violence and the violation of any court order are of extreme importance and should be considered among the highest response priorities. This includes incomplete 9-1-1 calls.
- (b) When practicable, investigators should obtain and document statements from the victim, the suspect, and any witnesses, including children, in or around the household or location of occurrence.
  - 1. A lethality assessment should be administered to victims of domestic violence to assess the level of danger and/or the severity of the situation and attached to the appropriate report.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Domestic Violence*

---

- (c) Investigators should list the full name and date of birth (and school if available) of each child who was present in the household at the time of the offense. The names of other children who may not have been in the house at that particular time should also be obtained for follow-up.
- (d) When practicable and legally permitted, video or audio record all significant statements and observations.
- (e) All injuries should be photographed, regardless of severity, taking care to preserve the victim's personal privacy. Where practicable, photographs should be taken by a person of the same sex. Victims whose injuries are not visible at the time of the incident should be asked to contact the Investigative Bureau in the event that the injuries later become visible.
- (f) Investigators should request that the victim complete and sign an authorization for release of medical records related to the incident when applicable.
- (g) If the suspect is no longer at the scene, investigators should make reasonable efforts to locate the suspect to further the investigation, provide the suspect with an opportunity to make a statement, and make an arrest or seek an arrest warrant if appropriate.
- (h) Seize any firearms or other dangerous weapons in the home, if appropriate and legally permitted, for safekeeping or as evidence. If the domestic violence involved threats of bodily harm, any firearm discovered in plain view or pursuant to consent or other lawful search must be taken into temporary custody (Penal Code § 18250).
- (i) When completing an incident or arrest report for violation of a court order, investigators should include specific information that establishes that the offender has been served, including the date the offender was served, the name of the agency that served the order, and the provision of the order that the subject is alleged to have violated. When reasonably available, the arresting investigator should attach a copy of the order to the incident or arrest report.
- (j) Investigators should take appropriate enforcement action when there is probable cause to believe an offense has occurred. Factors that should not be used as sole justification for declining to take enforcement action include:
  - 1. Whether the suspect lives on the premises with the victim.
  - 2. Claims by the suspect that the victim provoked or perpetuated the violence.
  - 3. The potential financial or child custody consequences of arrest.
  - 4. The physical or emotional state of either party.
  - 5. Use of drugs or alcohol by either party.
  - 6. Denial that the abuse occurred where evidence indicates otherwise.
  - 7. A request by the victim not to arrest the suspect.
  - 8. Location of the incident (public/private).
  - 9. Speculation that the complainant may not follow through with the prosecution.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Domestic Violence*

---

10. Actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, disability, or marital status of the victim or suspect.
11. The social status, community status, or professional position of the victim or suspect.

#### **415.4.1 IF A SUSPECT IS ARRESTED**

If a suspect is arrested, investigators should:

- (a) Advise the victim that there is no guarantee the suspect will remain in custody.
- (b) Provide the victim's contact information to the jail staff to enable notification of the victim upon the suspect's release from jail.
- (c) Advise the victim whether any type of court order will be in effect when the suspect is released from jail.

#### **415.4.2 IF NO ARREST IS MADE**

If no arrest is made, the investigator should:

- (a) Advise the parties of any options, including but not limited to:
  1. Voluntary separation of the parties.
  2. Appropriate resource referrals (e.g., counselors, friends, relatives, shelter homes, victim witness unit).
- (b) Document the resolution in a report.

#### **415.4.3 ARRESTING INVESTIGATORS' RESPONSIBILITIES REGARDING FIREARMS**

If a suspect is arrested, investigators shall (Penal Code § 273.76):

- (a) Query the Automated Firearms System through the California Law Enforcement Telecommunications System (CLETS) for any firearms owned or possessed by the arrestee.
  1. The investigating or filing investigator shall include a copy of the Automated Firearms System report when filing the case with the district attorney or prosecuting city attorney.
- (b) Ask the arrestee, victim, and any other household members, if applicable, about any firearms owned or possessed by the arrestee.
- (c) Ensure that any firearm or other deadly weapon in plain sight or discovered pursuant to a consensual or other lawful search is taken into temporary custody pursuant to Penal Code § 18250.
- (d) Document in the arrest report the detailed actions taken required by Penal Code § 273.76.

#### **415.5 VICTIM ASSISTANCE**

Because victims may be traumatized or confused, investigators should be aware that a victim's behavior and actions may be affected:



# Stanislaus County District Attorney's Office

## Policy Manual

### *Domestic Violence*

---

- (a) Victims should be provided with the bureau's domestic violence information handout, even if the incident may not rise to the level of a crime.
- (b) Victims should also be alerted to any available victim advocates, shelters, and community resources.
- (c) When an involved person requests law enforcement assistance while removing essential items of personal property, investigators should stand by for a reasonable amount of time.
- (d) If the victim has sustained injury or complaints of pain, investigators should seek medical assistance as soon as practicable.
- (e) Investigators should ask the victim whether the victim has a safe place to stay and assist in arranging transportation to an alternate shelter if the victim expresses a concern for the victim's safety or if the investigator determines that a need exists.
- (f) Investigators should make reasonable efforts to ensure that children or dependent adults who are under the supervision of the suspect or victim are being properly cared for.
- (g) If appropriate, investigators should seek or assist the victim in obtaining an emergency order if appropriate.

An investigator shall advise an individual protected by a Canadian domestic violence protection order of available local victim services (Family Code § 6452).

#### **415.6 FOREIGN COURT ORDERS**

Various types of orders may be issued in domestic violence cases. Any foreign court order properly issued by a court of another state, Indian tribe, or territory shall be enforced by investigators as if it were the order of a court in this state. An order should be considered properly issued when it reasonably appears that the issuing court has jurisdiction over the parties and reasonable notice and opportunity to respond was given to the party against whom the order was issued (18 USC § 2265). An otherwise valid out-of-state court or foreign order shall be enforced, regardless of whether the order has been properly registered with this state (Family Code § 6403).

Canadian domestic violence protection orders shall also be enforced in the same manner as if issued in this state (Family Code § 6452).

#### **415.7 VERIFICATION OF COURT ORDERS**

Determining the validity of a court order, particularly an order from another jurisdiction, can be challenging. Therefore, in determining whether there is probable cause to make an arrest for a violation of any court order, investigators should carefully review the actual order when available, and where appropriate and practicable:

- (a) Ask the subject of the order about his/her notice or receipt of the order, his/her knowledge of its terms and efforts to respond to the order.
  - 1. If a determination is made that a valid foreign order cannot be enforced because the subject has not been notified or served the order, the investigator shall inform the subject of the order, make a reasonable effort to serve the order upon the

# Stanislaus County District Attorney's Office

## Policy Manual

### *Domestic Violence*

---

subject, and allow the subject a reasonable opportunity to comply with the order before enforcing the order. Verbal notice of the terms of the order is sufficient notice (Family Code § 6403).

- (b) Check available records or databases that may show the status or conditions of the order.
  - 1. Registration or filing of an order in California is not required for the enforcement of a valid foreign order (Family Code § 6403).
- (c) Contact the issuing court to verify the validity of the order.
- (d) Contact a law enforcement official from the jurisdiction where the order was issued to verify information.

Investigators should document in an appropriate report their efforts to verify the validity of an order, regardless of whether an arrest is made. Investigators should contact a supervisor for clarification when needed.

#### **415.8 STANDARDS FOR ARRESTS**

Investigators investigating a domestic violence report should consider the following:

- (a) An arrest should be made when there is probable cause to believe that a felony or misdemeanor domestic violence offense has been committed (Penal Code § 13701). Any decision to not arrest an adult when there is probable cause to do so requires supervisor approval.
  - 1. Investigators are only authorized to make an arrest without a warrant for a misdemeanor domestic violence offense if the investigator makes the arrest as soon as probable cause arises (Penal Code § 836).
- (b) An investigator responding to a domestic violence call who cannot make an arrest will advise the victim of the victim's right to make a private person's arrest. The advisement should be made out of the presence of the suspect and shall include advising the victim how to safely execute the arrest. Investigators shall not dissuade victims from making a lawful private person's arrest. Investigators should refer to the provisions in the Private Persons Arrests Policy for options regarding the disposition of private person's arrests (Penal Code § 836(b)).
- (c) Investigators shall not cite and release a person for the following offenses (Penal Code § 853.6(a)(3)):
  - 1. Penal Code § 243(e)(1) (battery against spouse, cohabitant)
  - 2. Penal Code § 273.5 (corporal injury on spouse, cohabitant, fiancé/fiancée, person of a previous dating or engagement relationship, mother/father of the offender's child)
  - 3. Penal Code § 273.6 (violation of protective order) if violence or threats of violence have occurred or the suspect has gone to the workplace or residence of the protected party
  - 4. Penal Code § 646.9 (stalking)

# Stanislaus County District Attorney's Office

## Policy Manual

### *Domestic Violence*

---

5. Other serious or violent felonies specified in Penal Code § 1270.1
- (d) In responding to domestic violence incidents, including mutual protective order violations, investigators should generally be reluctant to make dual arrests. Investigators shall make reasonable efforts to identify the dominant aggressor in any incident. The dominant aggressor is the person who has been determined to be the most significant, rather than the first, aggressor (Penal Code § 13701). In identifying the dominant aggressor, an investigator shall consider:
  1. The intent of the law to protect victims of domestic violence from continuing abuse.
  2. The threats creating fear of physical injury.
  3. The history of domestic violence between the persons involved.
  4. Whether either person acted in self-defense.
- (e) An arrest shall be made when there is probable cause to believe that a violation of a domestic violence court order has been committed (Penal Code § 13701; Penal Code § 836), regardless of whether the offense was committed in the investigator's presence. After arrest, the investigator shall confirm that a copy of the order has been registered, unless the victim provides a copy (Penal Code § 836)

#### **415.9 REPORTS AND RECORDS**

- (a) A written report shall be completed on all incidents of domestic violence. All such reports should be documented on the appropriate form, which includes information and notations specific to domestic violence incidents as required by Penal Code § 13730.
  1. [See attachment: Addendum A\\_Countywide DV Form.pdf](#)
  2. [See attachment: Addendum B\\_Countywide Strangulation Form.pdf](#)
  3. [See attachment: epo001.pdf](#)
- (b) Reporting investigators should provide the victim with the case number of the report. The case number may be placed in the space provided on the domestic violence victim information handout provided to the victim. If the case number is not immediately available, an explanation should be given regarding how the victim can obtain the information at a later time.
- (c) Investigators who seize any firearm, ammunition, or other deadly weapon in a domestic violence incident shall issue the individual possessing such weapon a receipt that includes the name and residential mailing address of the owner or person who possessed the weapon and notice of where the weapon may be recovered, along with the applicable time limit for recovery (Penal Code § 18250; Penal Code § 18255; Penal Code § 33800; Family Code § 6389(c)).

#### **415.10 SERVICE OF COURT ORDERS**

- (a) An investigator who obtains an emergency protective order from the court shall serve it on the restrained person if the person can be reasonably located and shall provide

# Stanislaus County District Attorney's Office

## Policy Manual

### *Domestic Violence*

---

the person protected or the person's parent/guardian with a copy of the order. The investigator shall file a copy with the court as soon as practicable and shall have the order entered into the computer database system for protective and restraining orders maintained by the Department of Justice (Family Code § 6271; Penal Code § 646.91).

- (b) A temporary restraining order, emergency protective order, or an order issued after a hearing shall, at the request of the petitioner, be served on the restrained person by an investigator who is present at the scene of a reported domestic violence incident or when the investigator receives a request from the petitioner to provide service of the order (Family Code § 6383; Penal Code § 13710).
- (c) Any investigator serving a protective order that indicates that the respondent possesses weapons or ammunition shall request that the firearm/ammunition be immediately surrendered (Family Code § 6389(c)).
- (d) During the service of a protective order any firearm discovered in plain view or pursuant to consent or other lawful search shall be taken into temporary custody (Penal Code § 18250).
  - 1. An investigator should ensure that the Records Bureau is notified of any firearm obtained for entry into the Automated Firearms System (Family Code § 6383) (see the Records Bureau Policy for additional guidance).
- (e) If a valid Canadian order cannot be enforced because the person subject to the order has not been notified or served with the order, the investigator shall notify the protected individual that reasonable efforts shall be made to contact the person subject to the order. The investigator shall make a reasonable effort to inform the person subject to the order of the existence and terms of the order and provide the person with a record of the order, if available, and shall allow the person a reasonable opportunity to comply with the order before taking enforcement action (Family Code § 6452).

#### **415.11 PUBLIC ACCESS TO POLICY**

A copy of this domestic violence policy will be provided to members of the public upon request (Penal Code § 13701).

#### **415.12 DECLARATION IN SUPPORT OF BAIL INCREASE**

Any investigator who makes a warrantless arrest for a felony or misdemeanor violation of a domestic violence restraining order shall evaluate the totality of the circumstances to determine whether reasonable cause exists to seek an increased bail amount. If there is reasonable cause to believe that the scheduled bail amount is insufficient to assure the arrestee's appearance or to protect the victim or family member of a victim, the investigator shall prepare a declaration in support of increased bail (Penal Code § 1269c).

[See attachment: Bail increase affidavit and order 2023B Template-Final.pdf](#)

#### **415.13 DOMESTIC VIOLENCE DEATH REVIEW TEAM**

This bureau should cooperate with any interagency domestic violence death review team investigation. Written and oral information relating to a domestic violence death that would

# Stanislaus County District Attorney's Office

## Policy Manual

### *Domestic Violence*

---

otherwise be subject to release restrictions may be disclosed to the domestic violence death review team upon written request and approval of a supervisor (Penal Code § 11163.3).

# Gun Violence Restraining Orders

## 416.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for petitioning and serving gun violence restraining orders and accounting for the firearms obtained pursuant to those orders (Penal Code § 18108).

### 416.1.1 DEFINITIONS

Definitions related to this policy include:

**Gun violence restraining order** - Civil restraining order prohibiting a named person from controlling, owning, purchasing, possessing, receiving, or otherwise having custody of any firearms or ammunition, including an ammunition magazine (Penal Code § 18100).

## 416.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to petition for and serve gun violence restraining orders in compliance with state law and to properly account for firearms and ammunition obtained by the Bureau pursuant to such orders.

## 416.3 GUN VIOLENCE RESTRAINING ORDERS

An investigator who reasonably believes a person is a present danger to self or another person by controlling, owning, purchasing, possessing, receiving, or otherwise having custody of a firearm may request permission from the investigator's supervisor to petition the court for a gun violence restraining order.

Investigators petitioning the court should use the forms established by the Judicial Council (Penal Code § 18105). The petition should describe the number, types, and locations of any firearms and ammunition that the investigator believes to be possessed or controlled by the person (Penal Code § 18107). The petition should also describe why less-restrictive alternatives are ineffective or inadequate for the circumstances (Penal Code § 18125; Penal Code § 18150; Penal Code § 18175).

If it is not practical under the circumstances to submit a written petition, an investigator may submit the petition electronically or orally request a temporary order (Penal Code § 18122; Penal Code § 18140).

### 416.3.1 ADDITIONAL CONSIDERATIONS

Investigators should also consider requesting permission to petition the court for a gun violence restraining order (Penal Code § 18108):

- (a) When responding to a residence that is associated with a firearm registration or record.
- (b) When responding to any call or incident when a firearm is present or when one of the involved parties owns, possesses, or expresses an intent to acquire a firearm.
- (c) During a contact with a person exhibiting mental health issues, including suicidal thoughts, statements, or actions, if that person owns or possesses a firearm.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Gun Violence Restraining Orders*

---

Investigators should consider obtaining a mental health evaluation if the encounter involves a situation where there is a reasonable cause to believe that the person poses an immediate and present danger of causing personal injury to themselves or another person by having custody or control of a firearm or expresses intent to obtain a firearm (see the Mental Illness Commitments Policy) (Penal Code § 18108).

#### **416.4 SERVICE OF GUN VIOLENCE RESTRAINING ORDERS**

An investigator serving any gun violence restraining order shall:

- (a) Verbally ask the subject of the order if he/she has any firearm, ammunition, or magazine in his/her possession or under his/her custody or control (Penal Code § 18160).
- (b) Request that any firearms or ammunition be immediately surrendered and issue a receipt for the surrendered items (Penal Code § 18120).
- (c) Take into temporary custody any firearm or other deadly weapon discovered in plain view or pursuant to consent or other lawful search (Penal Code § 18250).
- (d) Inform the restrained person of any scheduled hearing regarding the order (Penal Code § 18160).
- (e) Transmit the original proof of service form to the issuing court as soon as practicable but within one business day (Penal Code § 18115).
- (f) As soon as practicable, but by the end of his/her shift, submit proof of service to their supervisor for prompt entry into the California Restraining and Protective Order System (Penal Code § 18115).

The investigator should also inform the restrained person that he/she is required, within 24 hours, to surrender to a law enforcement agency any other firearms and ammunition he/she owns or that are in his/her custody or control or sell them to a firearms dealer. This notification should be documented.

All firearms and ammunition collected shall be handled and booked in accordance with the Property and Evidence Policy.

##### **416.4.1 SERVICE OF ORAL GUN VIOLENCE RESTRAINING ORDERS**

If a gun violence restraining order is obtained orally, the investigator shall (Penal Code § 18140):

- (a) Serve the order on the restrained person in the manner outlined above, if the restrained person can reasonably be located.
- (b) File a copy of the order with the court as soon as practicable after issuance.
- (c) Ensure the order is provided to a supervisor for entry into the computer database system for protective and restraining orders maintained by the Department of Justice.

#### **416.5 SEARCH WARRANTS**

If a person who has been served with a gun violence restraining order refuses to surrender any firearm or ammunition, the investigator should consider whether to seek a search warrant. If a

# Stanislaus County District Attorney's Office

## Policy Manual

### *Gun Violence Restraining Orders*

---

search warrant is to be obtained, the preparation and service of the search warrant shall be done in accordance with the Warrant Service Policy. Additionally, (Penal Code § 1542.5):

- (a) The investigator serving the warrant shall take custody of any firearm or ammunition that is controlled, possessed or owned by the person who is the subject of the gun violence restraining order, including any discovered pursuant to the warrant, a consensual search or other lawful search.
- (b) If the location being searched is jointly occupied and the firearm or ammunition is owned by a person other than the restrained person, the firearm or ammunition should not be seized if the following conditions are met:
  - 1. The firearm or ammunition can be stored in a manner that does not allow the restrained person to have control or access.
  - 2. There is no evidence that the owner unlawfully possesses the firearm or ammunition.
- (c) If a locked gun safe belonging to someone other than the subject of a gun violence restraining order is discovered, the investigator shall not search the contents of the safe unless the owner consents or there is a valid search warrant for the safe. Any search of the safe must be done in the owner's presence.

#### **416.6 BUREAU SUPERVISING LEGAL CLERK RESPONSIBILITIES**

The Supervising Legal Clerk is responsible for ensuring:

- (a) Proof of service of any gun violence restraining order served by an investigator or received from the clerk of the court is entered in the computer database system for protective and restraining orders maintained by the Department of Justice within one business day of service if served by an investigator, or within one business day of receipt of proof of service if served by a person other than a law enforcement officer (Penal Code § 18115).
- (b) Oral orders are entered into the California Restraining and Protective Order System (Penal Code § 18140).
- (c) Copies of receipts of surrendered firearms or ammunition issued by other agencies for gun violence restraining orders issued by the Bureau are properly maintained and scanned into ICJIS (Penal Code § 18120).
- (d) Any relinquishment of firearm rights form received from the court is entered into the California Restraining and Protective Order System within one business day of receipt (Penal Code § 18115).

#### **416.7 COURT-ORDERED FIREARMS AND AMMUNITION SURRENDERS**

Authorized members shall accept firearms and ammunition from any individual who is the subject of a gun violence restraining order. The member receiving any firearm or ammunition shall:

- (a) Record the individual's name, address and telephone number.
- (b) Record the serial number of the firearm.
- (c) Prepare an incident report and property report.



*Gun Violence Restraining Orders*

---

- (d) Provide a property receipt to the individual who surrendered the firearms and ammunition.
- (e) Package and submit the firearms and ammunition in accordance with the Property and Evidence Policy.

**416.8 STORAGE AND RELEASE OF FIREARMS AND AMMUNITION**

Firearms and ammunition that were taken into temporary custody or surrendered pursuant to a gun violence restraining order shall be stored in accordance with the Property and Evidence Policy.

Firearms and ammunition shall be returned to the restrained person upon the expiration of the order in accordance with Penal Code § 18120 and the Property and Evidence Policy (Penal Code § 18108).

**416.9 RENEWAL OF GUN VIOLENCE RESTRAINING ORDERS**

The Investigative Bureau supervisor is responsible for the review of a gun violence restraining order (including temporary or ex parte orders) obtained by the Bureau to determine if renewal should be requested within the time prescribed by law (Penal Code § 18190).

**416.10 POLICY AVAILABILITY**

The Chief of Investigations or the authorized designee shall be responsible for making this policy available to the public upon request (Penal Code § 18108).

**416.11 TRAINING**

The Lieutenant should ensure that members receive periodic training on the requirements of this policy (Penal Code § 18108).

# Hate Crimes

## 417.1 PURPOSE AND SCOPE

This policy is designed to assist in identifying and handling crimes motivated by hate or other bias toward individuals and groups with legally defined protected characteristics, to define appropriate steps for assisting victims, and to provide a guide to conducting related investigations. It outlines the general policy framework for prevention, response, accessing assistance, victim assistance and follow-up, and reporting as related to law enforcement's role in handling hate crimes. It also serves as a declaration that hate crimes are taken seriously and demonstrates how the Stanislaus County District Attorney's Office may best use its resources to investigate and solve an offense, in addition to building community trust and increasing police legitimacy (Penal Code § 13519.6; Penal Code § 422.87).

### 417.1.1 DEFINITION AND LAWS

In accordance with Penal Code § 422.55; Penal Code § 422.56; Penal Code § 422.6; and Penal Code § 422.87, for purposes of all other state law, unless an explicit provision of law or the context clearly requires a different meaning, the following shall apply:

**Bias motivation** - Bias motivation is a pre-existing negative attitude toward actual or perceived characteristics referenced in Penal Code § 422.55. Depending on the circumstances of each case, bias motivation may include but is not limited to hatred, animosity, discriminatory selection of victims, resentment, revulsion, contempt, unreasonable fear, paranoia, callousness, thrill-seeking, desire for social dominance, desire for social bonding with those of one's "own kind," or a perception of the vulnerability of the victim due to the victim being perceived as being weak, worthless, or fair game because of a protected characteristic, including but not limited to disability or gender.

**Disability** - Disability includes mental disability and physical disability as defined in Government Code § 12926, regardless of whether those disabilities are temporary, permanent, congenital, or acquired by heredity, accident, injury, advanced age, or illness.

**Disability bias** - In recognizing suspected disability-bias hate crimes, investigators should consider whether there is any indication that the perpetrator was motivated by hostility or other bias, occasioned by factors such as but not limited to dislike of persons who arouse fear or guilt, a perception that persons with disabilities are inferior and therefore "deserving victims," a fear of persons whose visible traits are perceived as being disturbing to others, or resentment of those who need, demand, or receive alternative educational, physical, or social accommodations.

In recognizing suspected disability-bias hate crimes, investigators should consider whether there is any indication that the perpetrator perceived the victim to be vulnerable and, if so, if this perception is grounded, in whole or in part, in anti-disability bias. This includes but is not limited to situations where a perpetrator targets a person with a particular perceived disability while avoiding other vulnerable-appearing persons, such as inebriated persons or persons with perceived disabilities different from those of the victim. Such circumstances could be evidence

# Stanislaus County District Attorney's Office

## Policy Manual

### *Hate Crimes*

---

that the perpetrator's motivations included bias against persons with the perceived disability of the victim and that the crime must be reported as a suspected hate crime and not a mere crime of opportunity.

**Gender** - Gender means sex and includes a person's gender identity and gender expression.

**Gender expression** - Gender expression means a person's gender-related appearance and behavior, regardless of whether it is stereotypically associated with the person's assigned sex at birth.

**Gender identity** - Gender identity means each person's internal understanding of their gender, or the perception of a person's gender identity, which may include male, female, a combination of male and female, neither male nor female, a gender different from the person's sex assigned at birth, or transgender (2 CCR § 11030).

**Hate crime** - "Hate crime" includes but is not limited to a violation of Penal Code § 422.6, and means a criminal act committed, in whole or in part, because of one or more of the following actual or perceived characteristics of the victim:

- (a) Disability
- (b) Gender
- (c) Nationality
- (d) Race or ethnicity
- (e) Religion
- (f) Sexual orientation
- (g) Association with a person or group with one or more of these actual or perceived characteristics:
  - 1. "Association with a person or group with one or more of these actual or perceived characteristics" includes advocacy for, identification with, or being on the premises owned or rented by, or adjacent to, any of the following: a community center, educational facility, family, individual, office, meeting hall, place of worship, private institution, public agency, library, or other entity, group, or person that has, or is identified with people who have, one or more of the characteristics listed in the definition of "hate crime" under paragraphs 1 to 6, inclusive, of Penal Code § 422.55(a).

Note: A "hate crime" need not be motivated by hate but may be motivated by any bias against a protected characteristic.

**Hate incident** - A hate incident is an action or behavior motivated by hate or bias but legally protected by the First Amendment right to freedom of expression. Examples of hate incidents include:

- Name-calling
- Insults and epithets

# Stanislaus County District Attorney's Office

## Policy Manual

### *Hate Crimes*

---

- Distributing hate material in public places
- Displaying hate material on your own property

**Hate speech** - The First Amendment to the U.S. Constitution protects most speech, even when it is disagreeable, offensive, or hurtful. The following types of speech are generally not protected:

- Fighting words
- True threats
- Perjury
- Blackmail
- Incitement to lawless action
- Conspiracy
- Solicitation to commit any crime

**In whole or in part** - "In whole or in part because of" means that the bias motivation must be a cause in fact of the offense whether or not other causes also exist. When multiple concurrent motives exist, the prohibited bias must be a substantial factor in bringing about the particular result. There is no requirement that the bias be a main factor, or that a crime would not have been committed but for the actual or perceived characteristic.

**Nationality** - Nationality means country of origin, immigration status, including citizenship, and national origin.

**Race or ethnicity** - Race or ethnicity includes ancestry, color, and ethnic background.

**Religion** - Religion includes all aspects of religious belief, observance, and practice and includes agnosticism and atheism.

**Religious bias** - In recognizing suspected religion-bias hate crimes, investigators should consider whether there were targeted attacks on, or biased references to, symbols of importance to a particular religion or articles considered of spiritual significance in a particular religion (e.g., crosses, hijabs, Stars of David, turbans, head coverings, statues of the Buddha).

**Sexual orientation** - Sexual orientation means heterosexuality, homosexuality, or bisexuality.

**Victim** - Victim includes but is not limited to:

- Community center
- Educational facility
- Entity
- Family
- Group
- Individual

### *Hate Crimes*

---

- Office
- Meeting hall
- Person
- Place of worship
- Private institution
- Public agency
- Library
- Other victim or intended victim of the offense

#### **417.2 POLICY**

It is the policy of this bureau to safeguard the rights of all individuals irrespective of their disability, gender, nationality, race or ethnicity, religion, sexual orientation, and/or association with a person or group with one or more of these actual or perceived characteristics. Any acts or threats of violence, property damage, harassment, intimidation, or other crimes motivated by hate or bias should be viewed very seriously and given high priority.

When necessary, this bureau will assist local law enforcement agencies employing reasonably available resources and vigorous law enforcement action to identify and arrest hate crime perpetrators. Also, recognizing the particular fears and distress typically suffered by victims, the potential for reprisal and escalation of violence, and the far-reaching negative consequences of these crimes on the community, this bureau should take all reasonable steps to attend to the security and related concerns of the immediate victims and their families as feasible.

All investigators are required to be familiar with the policy and use reasonable diligence to carry out the policy.

#### **417.3 PLANNING AND PREVENTION**

In order to facilitate the guidelines contained within this policy, bureau members will continuously work to build and strengthen relationships with the community, engage in dialogue, and provide education to the community about this policy. Bureau personnel are also encouraged to learn about the inherent issues concerning their communities in relation to hate crimes.

Although hate incidents are not criminal events, they can be indicators of, or precursors to, hate crimes. Hate incidents should be investigated and documented as part of an overall strategy to prevent hate crimes.

##### **417.3.1 RELEASE OF INFORMATION**

Establishing a relationship with stakeholders, before any incident occurs, to develop a network and protocol for disclosure often assists greatly in any disclosure.

The benefit of public disclosure of hate crime incidents includes:

- (a) Dissemination of correct information.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Hate Crimes*

---

- (b) Assurance to affected communities or groups that the matter is being properly and promptly investigated.
- (c) The ability to request information regarding the commission of the crimes from the victimized community.

Information or records relating to hate crimes subject to public disclosure shall be released as provided by the Records Maintenance and Release Policy or as allowed by law. In accordance with the Media Relations Policy, the supervisor, public information officer, or the authorized designee should be provided with information that can be responsibly reported to the media. When appropriate, the bureau spokesperson should reiterate that hate crimes will not be tolerated, will be investigated seriously, and will be prosecuted to the fullest extent of the law.

The Bureau should consider the following when releasing information to the public regarding hate crimes and hate incidents that have been reported within the jurisdiction:

- Inform community organizations in a timely manner when a community group has been the target of a hate crime.
- Inform the community of the impact of these crimes on the victim, the victim's family, and the community, and of the assistance and compensation available to victims.
- Inform the community regarding hate crime law and the legal rights of, and remedies available to, victims of hate crimes.
- Provide the community with ongoing information regarding hate crimes and/or hate incidents.

#### **417.4 RESPONSE, VICTIM ASSISTANCE, AND FOLLOW-UP**

##### **417.4.1 INVESTIGATION**

Investigators at the scene of, or performing follow-up investigation on, a suspected hate or bias crime or hate incident should take all actions deemed reasonably necessary, including but not limited to the following:

- (a) Consider typologies of perpetrators of hate crimes and incidents, including but not limited to thrill, reactive/defensive, and mission (hard core).
- (b) Utilize investigative techniques and methods to handle hate crimes or hate incidents in a professional manner.
- (c) Utilize proper techniques for interviewing people with disabilities and be aware of and provide appropriate accommodations (e.g., ADA standards, Braille, visuals, translators for the deaf or hard of hearing).
- (d) Properly investigate any report of a hate crime committed under the color of authority per Penal Code § 422.6 and Penal Code § 13519.6.
- (e) Document physical evidence or indicators of hate crimes, in accordance with the provisions of the Property and Evidence Policy, such as:
  - 1. Hate literature.
  - 2. Spray paint cans.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Hate Crimes*

---

3. Threatening letters.
4. Symbols used by hate groups.
5. Desecration of religious symbols, objects, or buildings.
- (f) Request the assistance of translators or interpreters when needed to establish effective communication.
- (g) Conduct a preliminary investigation and record information regarding:
  1. Identity of suspected perpetrators.
  2. Identity of witnesses, including those no longer at the scene.
  3. Offer of victim confidentiality per Government Code § 7923.615.
  4. Prior occurrences, in this area or with this victim.
  5. Statements made by suspects; exact wording is critical.
  6. Document the victim's protected characteristics.
- (h) Provide victim assistance and follow-up.
- (i) Canvass the area for additional witnesses.
- (j) Examine suspect's social media activity for potential evidence of bias motivation.
- (k) Coordinate the investigation with bureau, state, and regional intelligence operations. These sources can provide the investigator with an analysis of any patterns, organized hate groups, and suspects potentially involved in the offense.
- (l) Coordinate the investigation with the crime scene investigation unit (if applicable) or other appropriate units of the Bureau.
- (m) Determine if the incident should be classified as a hate crime.
- (n) Take reasonable steps to provide appropriate assistance to hate crime victims, including the following measures:
  1. Contact victims periodically to determine whether they are receiving adequate and appropriate assistance.
  2. Provide ongoing information to victims about the status of the criminal investigation.
  3. Provide victims and any other interested persons the brochure on hate crimes per Penal Code § 422.92 and information on any local advocacy groups (if asked).
- (o) Document any suspected multi-mission extremist crimes.
- (p) Coordinate with other law enforcement agencies in the area to assess patterns of hate crimes and/or hate incidents, and determine if organized hate groups are involved.

#### **417.5 TRAINING**

All members of this bureau will receive POST-approved training on hate crime recognition and investigation (Penal Code § 13519.6).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Hate Crimes*

---

Training should include (Penal Code § 422.87):

- (a) Recognition of bias motivators such as ranges of attitudes and perceptions toward a specific characteristic or group, including disability bias, gender bias, and religion bias.
- (b) Accurate reporting by investigators, including information on the general underreporting of hate crimes.
- (c) Distribution of hate crime brochures.
- (d) When a gun violence restraining order may be appropriate for prevention of hate crimes (Penal Code § 13519.6).

#### **417.6 APPENDIX**

See attachments:

[Statutes and Legal Requirements.pdf](#)

[Hate Crime Checklist.pdf](#)

[Supplemental Hate Crime Report.pdf](#)



# Foreign Diplomatic and Consular Representatives

## 418.1 PURPOSE AND SCOPE

This policy provides guidelines to ensure that members of the Stanislaus County District Attorney's Office extend appropriate privileges and immunities to foreign diplomatic and consular representatives in accordance with international law.

## 418.2 POLICY

The Stanislaus County District Attorney's Office respects international laws related to the special privileges and immunities afforded foreign diplomatic and consular representatives assigned to the United States.

All foreign diplomatic and consular representatives shall be treated with respect and courtesy, regardless of any privileges or immunities afforded them.

## 418.3 CLAIMS OF IMMUNITY

If a member comes into contact with a person where law enforcement action may be warranted and the person claims diplomatic or consular privileges and immunities, the member should, without delay:

- (a) Notify a supervisor.
- (b) Advise the person that his/her claim will be investigated and he/she may be released in accordance with the law upon confirmation of the person's status.
- (c) Request the person's identification card, either issued by the U.S. Department of State (DOS), Office of the Chief of Protocol, or in the case of persons accredited to the United Nations, by the U.S. Mission to the United Nations. These are the only reliable documents for purposes of determining privileges and immunities.
- (d) Contact the DOS Diplomatic Security Command Center at 571-345-3146 or toll free at 866-217-2089, or at another current telephone number and inform the center of the circumstances.
- (e) Verify the immunity status with DOS and follow any instructions regarding further detention, arrest, prosecution and/or release, as indicated by the DOS representative. This may require immediate release, even if a crime has been committed.

Identity or immunity status should not be presumed from the type of license plates displayed on a vehicle. If there is a question as to the status or the legitimate possession of a Diplomat or Consul license plate, a query should be run via the National Law Enforcement Telecommunications System (NLETS), designating "US" as the state.

## 418.4 ENFORCEMENT

If the DOS is not immediately available for consultation regarding law enforcement action, members shall be aware of the following:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Foreign Diplomatic and Consular Representatives*

---

- (a) Generally, all persons with diplomatic and consular privileges and immunities may be issued a citation or notice to appear. However, the person may not be compelled to sign the citation.
- (b) All persons, even those with a valid privilege or immunity, may be reasonably restrained in exigent circumstances for purposes of self-defense, public safety or the prevention of serious criminal acts.
- (c) An impaired foreign diplomatic or consular representative may be prevented from driving a vehicle, even if the person may not be arrested due to privileges and immunities.
  - 1. Investigations, including the request for field sobriety tests, chemical tests and any other tests regarding impaired driving may proceed but they shall not be compelled.
- (d) The following persons may not be detained or arrested, and any property or vehicle owned by these persons may not be searched or seized:
  - 1. Diplomatic-level staff of missions to international organizations and recognized family members
  - 2. Diplomatic agents and recognized family members
  - 3. Members of administrative and technical staff of a diplomatic mission and recognized family members
  - 4. Career consular officers, unless the person is the subject of a felony warrant
- (e) The following persons may generally be detained and arrested:
  - 1. International organization staff; however, some senior officers are entitled to the same treatment as diplomatic agents.
  - 2. Support staff of missions to international organizations
  - 3. Diplomatic service staff and consular employees; however, special bilateral agreements may exclude employees of certain foreign countries.
  - 4. Honorary consular officers
  - 5. Whenever an investigator arrests and incarcerates, or detains for investigation for over two hours, a person with diplomatic and consular privileges and immunities, the investigator shall promptly advise the person that he/she is entitled to have his/her government notified of the arrest or detention (Penal Code § 834c). If the individual wants his/her government notified, the investigator shall begin the notification process.

#### **418.5 DOCUMENTATION**

All contacts with persons who have claimed privileges and immunities afforded foreign diplomatic and consular representatives should be thoroughly documented and the related reports forwarded to DOS.

#### **418.6 DIPLOMATIC IMMUNITY TABLE**

Reference table on diplomatic immunity:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Foreign Diplomatic and Consular Representatives*

Category	Arrested or Detained	Enter Residence Subject to Ordinary Procedures	Issued Traffic Citation	Subpoenaed as Witness	Prosecuted	Recognized Family Members
<b>Diplomatic Agent</b>	No (note (b))	No	Yes	No	No	Same as sponsor (full immunity & inviolability)
<b>Member of Admin and Tech Staff</b>	No (note (b))	No	Yes	No	No	Same as sponsor (full immunity & inviolability)
<b>Service Staff</b>	Yes (note (a))	Yes	Yes	Yes	No for official acts. Yes otherwise (note (a))	No immunity or inviolability (note (a))
<b>Career Consul Officer</b>	Yes if for a felony and pursuant to a warrant (note (a))	Yes (note (d))	Yes	No for official acts Testimony may not be compelled in any case	No for official acts. Yes otherwise (note (a))	No immunity or inviolability
<b>Honorable Consul Officer</b>	Yes	Yes	Yes	No for official acts Yes otherwise.	No for official acts Yes otherwise	No immunity or inviolability
<b>Consulate Employees</b>	Yes (note (a))	Yes	Yes	No for official acts Yes otherwise.	No for official acts. Yes otherwise (note (a))	No immunity or inviolability (note (a))
<b>Int'l Org Staff (note (b))</b>	Yes (note (c))	Yes (note (c))	Yes	Yes (note (c))	No for official acts. Yes otherwise (note (c))	No immunity or inviolability
<b>Diplomatic-Level Staff of Missions to Int'l Org</b>	No (note (b))	No	Yes	No	No	Same as sponsor (full immunity & inviolability)
<b>Support Staff of Missions to Int'l Orgs</b>	Yes	Yes	Yes	Yes	No for official acts Yes otherwise	No immunity or inviolability

Notes for diplomatic immunity table:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Foreign Diplomatic and Consular Representatives*

---

- (a) This table presents general rules. The employees of certain foreign countries may enjoy higher levels of privileges and immunities on the basis of special bilateral agreements.
- (b) Reasonable constraints, however, may be applied in emergency circumstances involving self-defense, public safety, or in the prevention of serious criminal acts.
- (c) A small number of senior officers are entitled to be treated identically to diplomatic agents.
- (d) Note that consul residences are sometimes located within the official consular premises. In such cases, only the official office space is protected from police entry.

# Sexual Assault Investigations

## 419.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the investigation of sexual assaults. These guidelines will address some of the unique aspects of such cases and the effects that these crimes have on the victims.

Mandatory notifications requirements are addressed in the Child Abuse and Senior and Disability Victimization policies.

### 419.1.1 DEFINITIONS

Definitions related to this policy include:

**Sexual assault** - Any crime or attempted crime of a sexual nature, to include but not limited to offenses defined in Penal Code § 243.4, Penal Code § 261 et seq., and Penal Code § 285 et seq.

**Sexual Assault Response Team (SART)** - A multidisciplinary team generally comprised of advocates; law enforcement officers; forensic medical examiners, including sexual assault forensic examiners (SAFEs) or sexual assault nurse examiners (SANEs) if possible; forensic laboratory personnel; and prosecutors. The team is designed to coordinate a broad response to sexual assault victims.

## 419.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office that its members, when investigating reports of sexual assaults, will strive to minimize the trauma experienced by the victims, and will aggressively investigate sexual assaults, pursue expeditious apprehension and conviction of perpetrators, and protect the safety of the victims and the community. Bureau Investigators typically do not respond to take initial reports of sexual assault. The initial report is usually taken by the law enforcement agency having jurisdiction over where the sexual assault occurred. However, if a situation arises in which a criminal investigator is made aware of a sexual assault, the following shall apply.

## 419.3 QUALIFIED INVESTIGATORS

Qualified investigators should be available for assignment of sexual assault investigations. These investigators should:

- (a) Have specialized training in, and be familiar with, interview techniques and the medical and legal issues that are specific to sexual assault investigations.
- (b) Conduct follow-up interviews and investigation.
- (c) Present appropriate cases of alleged sexual assault to the prosecutor for review.
- (d) Coordinate with other enforcement agencies, social service agencies and medical personnel as needed.
- (e) Provide referrals to therapy services, victim advocates and support for the victim.
- (f) Participate in or coordinate with SART.

### *Sexual Assault Investigations*

---

#### **419.4 REPORTING**

In all reported or suspected cases of sexual assault, a report will be written and assigned for follow-up investigation. This includes incidents in which the allegations appear unfounded or unsubstantiated.

#### **419.5 VICTIM INTERVIEWS**

The primary considerations in sexual assault investigations should be the health and safety of the victim, the preservation of evidence, and preliminary interviews to determine if a crime has been committed and to attempt to identify the suspect.

Whenever possible, a member of SART should be included in the initial victim interviews. An in-depth follow-up interview should not be conducted until after the medical and forensic examinations are completed and the personal needs of the victim have been met (e.g., change of clothes, bathing). The follow-up interview may be delayed to the following day based upon the circumstances. Whenever practicable, the follow-up interview should be conducted by a qualified investigator.

No opinion of whether the case is unfounded shall be included in the report.

Victims shall not be asked or required to take a polygraph examination (34 USC § 10451; Penal Code § 637.4).

Victims should be apprised of applicable victim's rights provisions, as outlined in the Victim and Witness Assistance Policy.

##### **419.5.1 VICTIM RIGHTS**

Whenever there is an alleged sexual assault, the assigned investigator shall accomplish the following:

- (a) Prior to the commencement of the initial interview, advise the victim in writing of the right to have a victim advocate and a support person of the victim's choosing present at any interview or contact by law enforcement, about any other rights of a sexual assault victim pursuant to the sexual assault victim card described in Penal Code § 680.2, and the right to have a person of the same or opposite gender present in the room during any interview with a law enforcement official unless no such person is reasonably available (Penal Code § 679.04).
- (b) If the victim is transported to a hospital for any medical evidentiary or physical examination, the investigator shall immediately cause the local rape victim counseling center to be notified (Penal Code § 264.2).
  1. The investigator shall not discourage a victim from receiving a medical evidentiary or physical examination (Penal Code § 679.04).
  2. A support person may be excluded from the examination by the investigator or the medical provider if the support person's presence would be detrimental to the purpose of the examination (Penal Code § 264.2).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Sexual Assault Investigations*

---

#### 419.5.2 VICTIM CONFIDENTIALITY

Investigators investigating or receiving a report of an alleged sex offense shall inform the victim, or the victim's parent or guardian if the victim is a minor, that his/her name will become a matter of public record unless the victim requests that his/her name not be made public. The reporting investigator shall document in his/her report that the victim was properly informed and shall include any related response made by the victim, or if a minor, any response made by the victim's parent or guardian (Penal Code § 293).

Except as authorized by law, members of this bureau shall not publicly disclose the name of any victim of a sex crime who has exercised his/her right to confidentiality (Penal Code § 293).

#### **419.6 COLLECTION AND TESTING OF BIOLOGICAL EVIDENCE**

Whenever possible, a SART member should be involved in the collection of forensic evidence from the victim.

When the facts of the case indicate that collection of biological evidence is warranted, it should be collected regardless of how much time has elapsed since the reported assault.

If a drug-facilitated sexual assault is suspected, urine and blood samples should be collected from the victim as soon as practicable.

Subject to requirements set forth in this policy, biological evidence from all sexual assault cases, including cases where the suspect is known by the victim, should be submitted for testing.

Victims who choose not to assist with an investigation, do not desire that the matter be investigated, or wish to remain anonymous may still consent to the collection of evidence under their control. In these circumstances, the evidence should be collected and stored appropriately (Penal Code § 680).

##### 419.6.1 STANDARDIZED SEXUAL ASSAULT FORENSIC MEDICAL EVIDENCE KIT

California standardized sexual assault forensic medical evidence (SAFE) kits are available to members who may investigate sexual assault cases. Members investigating a sexual assault should use these SAFE kits when appropriate and follow related usage guidelines issued by the California Clinical Forensic Medical Training Center (Penal Code § 13823.14).

##### 419.6.2 COLLECTION AND TESTING REQUIREMENTS

Members investigating a sexual assault offense should take every reasonable step to ensure that DNA testing of such evidence is performed in a timely manner and within the time periods prescribed by Penal Code § 803(g). SAFE kits should be submitted to the crime lab within 20 days after being booked into evidence (Penal Code § 680).

In order to maximize the effectiveness of such testing and identify the perpetrator of any sexual assault, the assigned investigator shall ensure that an information profile for the SAFE kit evidence has been created in the California Department of Justice (DOJ) SAFE-T database within 120 days of collection and should further ensure that the results of any such test have been timely entered

# Stanislaus County District Attorney's Office

## Policy Manual

### *Sexual Assault Investigations*

---

into and checked against both the DOJ Cal-DNA database and the Combined DNA Index System (CODIS) (Penal Code § 680.3).

If the assigned investigator determines that a SAFE kit submitted to a private vendor laboratory for analysis has not been tested within 120 days after submission, the investigator shall update the SAFE-T database to reflect the reason for the delay in testing. The assigned investigator shall continue to update the status every 120 days thereafter until the testing is complete, the statute of limitations has run, or the SAFE kit is exempt from the update requirement (Penal Code § 680.3).

If, for any reason, DNA evidence in a sexual assault case in which the identity of the perpetrator is in issue and is not going to be analyzed within 18 months of the crime, the assigned investigator shall notify the victim of such fact in writing no less than 60 days prior to the expiration of the 18-month period (Penal Code § 680).

Additional guidance regarding evidence retention and destruction is found in the Property and Evidence Policy.

#### 419.6.3 DNA TEST RESULTS

A SART member should be consulted regarding the best way to deliver biological testing results to a victim so as to minimize victim trauma, especially in cases where there has been a significant delay in getting biological testing results (e.g., delays in testing the evidence or delayed DNA databank hits). Members should make reasonable efforts to assist the victim by providing available information on local assistance programs and organizations as provided in the Victim and Witness Assistance Policy.

- (a) Upon receipt of a written request from a sexual assault victim or the victim's authorized designee, members investigating sexual assault cases shall inform the victim of the status of the DNA testing of any evidence from the victim's case (Penal Code § 680).
  - 1. Although such information may be communicated orally, the assigned investigator should thereafter follow-up with and retain a copy of confirmation by either written or electronic mail.
  - 2. Absent a written request, no member of this bureau is required to, but may, communicate with the victim or the victim's authorized designee regarding the status of any DNA testing.
- (b) Sexual assault victims shall further have the following rights (Penal Code § 680):
  - 1. To be informed if a DNA profile of the assailant was obtained from the testing of the SAFE kit or other crime scene evidence from their case.
  - 2. To be informed if there is a confirmed match between the DNA profile of the assailant developed from the evidence and a DNA profile contained in the DOJ Convicted Offender DNA Database, providing that disclosure would not impede or compromise an ongoing investigation.
  - 3. To be informed if the DNA profile of the assailant developed from the evidence has been entered into the DOJ Databank or the federal Department of Justice or Federal Bureau of Investigation CODIS database of case evidence.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Sexual Assault Investigations*

---

4. To access the DOJ SAFE-T database portal consistent with Penal Code § 680.3(e) for information involving their own forensic kit and the status of the kit.
- (c) Provided that the sexual assault victim or the victim's authorized designee has kept the assigned investigator informed with regard to current address, telephone number, and email address (if available), any victim or the victim's authorized designee shall, upon request, be advised of any known significant changes regarding the victim's case (Penal Code § 680).
  1. Although such information may be communicated orally, the assigned investigator should thereafter follow-up with and retain a copy of confirmation by either written or electronic mail.
  2. No investigator shall be required or expected to release any information which might impede or compromise any ongoing investigation.

#### **419.6.4 COLLECTION OF DNA REFERENCE SAMPLES**

Reference samples of DNA collected directly from a victim of sexual assault, and reference samples of DNA collected from any individual that were voluntarily provided for the purpose of exclusion, shall be protected as provided in Penal Code § 679.12 (Penal Code § 680).

#### **419.7 DISPOSITION OF CASES**

If the assigned investigator has reason to believe the case is without merit, the case may be classified as unfounded only upon review and approval of the Investigative Bureau supervisor.

Classification of a sexual assault case as unfounded requires the Investigative Bureau supervisor to determine that the facts have significant irregularities with reported information and that the incident could not have happened as it was reported. When a victim has recanted his/her original statement, there must be corroborating evidence that the allegations were false or baseless (i.e., no crime occurred) before the case should be determined as unfounded.

#### **419.8 CASE REVIEW**

The Investigative Bureau supervisor should ensure case dispositions are reviewed on a periodic basis, at least annually, using an identified group that is independent of the investigation process. The reviews should include an analysis of:

- Case dispositions.
- Decisions to collect biological evidence.
- Submissions of biological evidence for lab testing.

The SART and/or victim advocates should be considered for involvement in this audit. Summary reports on these reviews should be forwarded through the chain of command to the Chief of Investigations.

#### **419.9 RELEASING INFORMATION TO THE PUBLIC**

In cases where the perpetrator is not known to the victim, and especially if there are multiple crimes where more than one appear to be related, consideration should be given to releasing

### *Sexual Assault Investigations*

---

information to the public whenever there is a reasonable likelihood that doing so may result in developing helpful investigative leads. The Investigative Bureau supervisor should weigh the risk of alerting the suspect to the investigation with the need to protect the victim and the public, and to prevent more crimes.

#### **419.10 TRAINING**

Subject to available resources, periodic training should be provided to:

- (a) Members who are first responders. Training should include:
  - 1. Initial response to sexual assaults.
  - 2. Legal issues.
  - 3. Victim advocacy.
  - 4. Victim's response to trauma.
  - 5. Proper use and handling of the California standardized SAFE kit (Penal Code § 13823.14).
- (b) Qualified investigators, who should receive advanced training on additional topics. Advanced training should include:
  - 1. Interviewing sexual assault victims.
  - 2. SART.
  - 3. Medical and legal aspects of sexual assault investigations.
  - 4. Serial crimes investigations.
  - 5. Use of community and other federal and state investigative resources, such as the Violent Criminal Apprehension Program (ViCAP).
  - 6. Techniques for communicating with victims to minimize trauma.

# Child Abuse

## 420.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the investigation of suspected child abuse. This policy also addresses when Stanislaus County District Attorney's Office members are required to notify the county Child Protective Services (CPS) of suspected child abuse.

### 420.1.1 DEFINITIONS

Definitions related to this policy include:

**Child** - Unless otherwise specified by a cited statute, a child is any person under the age of 18 years.

**Child abuse** - Any offense or attempted offense involving violence or neglect with a child victim when committed by a person responsible for the child's care or any other act that would mandate notification to a social service agency or law enforcement (Penal Code § 11165.9; Penal Code § 11166).

## 420.2 POLICY

The Stanislaus County District Attorney's Office will investigate all reported incidents of alleged criminal child abuse and ensure CPS is notified as required by law.

## 420.3 MANDATORY NOTIFICATION

The child protection agency shall be notified when (Penal Code § 11166):

- (a) There is a known or suspected instance of child abuse or neglect reported, which is alleged to have occurred as a result of the action of a person responsible for the child's welfare, or
- (b) A person responsible for the child's welfare fails to adequately protect the child from abuse when the person knew or reasonably should have known that the child was in danger of abuse.

The District Attorney's office shall be notified in all instances of known or suspected child abuse or neglect reported to this bureau. Notification of the District Attorney is not required for reports only involving neglect by a person, who has the care or custody of a child, to provide adequate food, clothing, shelter, medical care, or supervision where no physical injury to the child has occurred (Penal Code § 11166).

When the abuse or neglect occurs at a licensed facility or is alleged to have resulted from the actions of a person who is required to have a state license (e.g., foster homes, group homes, day care), notification shall also be made to the California Department of Social Services or other applicable licensing authority. When the alleged abuse or neglect involves a child of a minor parent or a dependent adult, notification shall also be made to the attorney of the minor or the dependent adult within 36 hours (Penal Code 11166.1; Penal Code 11166.2).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Child Abuse*

---

For purposes of notification, the abuse or neglect includes physical injury or death inflicted by other than accidental means upon a child by another person; sexual abuse (Penal Code § 11165.1); neglect (Penal Code § 11165.2); the willful harming or injuring of a child or the endangering of the person or health of a child (Penal Code § 11165.3); and unlawful corporal punishment or injury (Penal Code § 11165.4). Child abuse or neglect does not include a mutual affray between minors, nor does it include an injury caused by the reasonable and necessary force used by a peace officer acting within the course and scope of the peace officer's employment as a peace officer.

#### **420.3.1 NOTIFICATION PROCEDURE**

Notification should occur as follows (Penal Code § 11166):

- (a) Notification shall be made immediately, or as soon as practicable, by telephone, fax or electronic transmission.
- (b) A written follow-up report should be forwarded within 36 hours of receiving the information concerning the incident.

#### **420.4 QUALIFIED INVESTIGATORS**

Qualified investigators should be available for child abuse investigations. These investigators should:

- (a) Conduct interviews in child appropriate interview facilities.
- (b) Be familiar with forensic interview techniques specific to child abuse investigations.
- (c) Present all cases of alleged child abuse to the prosecutor for review.
- (d) Coordinate with other enforcement agencies, social service agencies and school administrators as needed.
- (e) Provide referrals to therapy services, victim advocates, guardians and support for the child and family as appropriate.
- (f) Participate in or coordinate with multidisciplinary investigative teams as applicable (Welfare and Institutions Code § 18961.7).

#### **420.5 INVESTIGATIONS AND REPORTING**

In all reported or suspected cases of child abuse, a report will be written. Investigators shall write a report even if the allegations appear unfounded or unsubstantiated.

Investigations and reports related to suspected cases of child abuse should address, as applicable:

- (a) The overall basis for the contact. This should be done by the investigating investigator in all circumstances where a suspected child abuse victim was contacted.
- (b) The exigent circumstances that existed if investigators interviewed the child victim without the presence of a parent or guardian.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Child Abuse*

---

- (c) Any relevant statements the child may have made and to whom he/she made the statements.
- (d) If a child was taken into protective custody, the reasons, the name and title of the person making the decision, and why other alternatives were not appropriate.
- (e) Documentation of any visible injuries or any injuries identified by the child. This should include photographs of such injuries, if practicable.
- (f) Whether the child victim was transported for medical treatment or a medical examination.
- (g) Whether the victim identified a household member as the alleged perpetrator, and a list of the names of any other children who may reside in the residence.
- (h) Identification of any prior related reports or allegations of child abuse, including other jurisdictions, as reasonably known.
- (i) Previous addresses of the victim and suspect.
- (j) Other potential witnesses who have not yet been interviewed, such as relatives or others close to the victim's environment.

All cases of the unexplained death of a child should be investigated as thoroughly as if it had been a case of suspected child abuse (e.g., a sudden or unexplained death of an infant).

#### 420.5.1 EXTRA JURISDICTIONAL REPORTS

If a report of known or suspected child abuse or neglect that is alleged to have occurred outside this jurisdiction is received, bureau members shall ensure that the caller is immediately transferred to the agency with proper jurisdiction for the investigation of the case. If the caller cannot be successfully transferred to the appropriate agency, a report shall be taken and immediately referred by telephone, fax, or electronic transfer to the agency with proper jurisdiction (Penal Code § 11165.9).

#### 420.5.2 INITIAL REPORTS OF ABUSE FROM A NONMANDATED REPORTER

Members who receive a report of child abuse or neglect shall request the following information from the reporter (Penal Code § 11167):

- (a) Name and telephone number
- (b) Information and the source of information that gives rise to the knowledge or reasonable suspicion of child abuse or neglect

If the reporter refuses to provide their name and telephone number, the member should make a reasonable effort to determine the basis for the refusal and inform them that their information will remain confidential.

### *Child Abuse*

---

#### **420.6 PROTECTIVE CUSTODY**

Before taking any child into protective custody, the investigator should make reasonable attempts to contact CPS. Generally, removal of a child from the child's family, guardian, or other responsible adult should be left to the child welfare authorities when they are present or have become involved in an investigation.

Generally, members of this bureau should remove a child from the child's parent or guardian without a court order only when no other effective alternative is reasonably available and immediate action reasonably appears necessary to protect the child. Prior to taking a child into protective custody, the investigator should take reasonable steps to deliver the child to another qualified parent or legal guardian, unless it reasonably appears that the release would endanger the child or result in abduction. If this is not a reasonable option, the investigator shall ensure that the child is delivered to CPS.

Whenever practicable, the investigator should inform a supervisor of the circumstances prior to taking a child into protective custody. If prior notification is not practicable, investigators should contact a supervisor promptly after taking a child into protective custody.

Children may only be removed from a parent or guardian in the following situations when a court order cannot reasonably be obtained in a timely manner (Welfare and Institutions Code § 305):

- (a) The investigator reasonably believes the child is a person described in Welfare and Institutions Code § 300, and further has good cause to believe that any of the following conditions exist:
  - 1. The child has an immediate need for medical care.
  - 2. The child is in immediate danger of physical or sexual abuse.
  - 3. The physical environment or the fact that the child is left unattended poses an immediate threat to the child's health or safety. In the case of a child left unattended, the investigator shall first attempt to locate and determine if a responsible parent or guardian is available and capable of assuming custody before taking the child into protective custody.
- (b) The investigator reasonably believes the child requires protective custody under the provisions of Penal Code § 279.6, in one of the following circumstances:
  - 1. It reasonably appears to the investigator that a person is likely to conceal the child, flee the jurisdiction with the child or, by flight or concealment, evade the authority of the court.
  - 2. There is no lawful custodian available to take custody of the child.
  - 3. There are conflicting custody orders or conflicting claims to custody and the parties cannot agree which party should take custody of the child.
  - 4. The child is an abducted child.
- (c) The child is in the company of, or under the control of, a person arrested for Penal Code § 278 (Detainment or concealment of child from legal custodian) or Penal Code § 278.5 (Deprivation of custody of a child or right to visitation) (Penal Code § 279.6).

### *Child Abuse*

---

A child taken into protective custody shall be delivered to CPS unless otherwise directed by court order.

#### **420.6.1 CALIFORNIA SAFELY SURRENDERED BABY LAW**

An individual having lawful custody of an infant less than 72 hours old is not guilty of abandonment if the individual voluntarily surrenders physical custody of the infant to personnel on-duty at a safe-surrender site, such as a hospital or fire department (Penal Code § 271.5). The law requires the surrender site to notify CPS.

#### **420.6.2 NEWBORNS TESTING POSITIVE FOR DRUGS**

Under certain circumstances, investigators can be prohibited from taking a newborn who is the subject of a proposed adoption into protective custody, even when the newborn has tested positive for illegal drugs or the birth mother tested positive for illegal drugs.

Investigators shall instead follow the provisions of Welfare and Institutions Code § 305.6 to ensure that the newborn is placed with the adoptive parents when it is appropriate.

### **420.7 INTERVIEWS**

#### **420.7.1 PRELIMINARY INTERVIEWS**

Absent extenuating circumstances or impracticality, investigators should record the preliminary interview with suspected child abuse victims. Investigators should avoid multiple interviews with a child victim and should attempt to gather only the information necessary to begin an investigation. When practicable, investigating investigators should defer interviews until a person who is specially trained in such interviews is available. Generally, child victims should not be interviewed in the home or location where the alleged abuse occurred.

#### **420.7.2 DETAINING SUSPECTED CHILD ABUSE VICTIMS FOR AN INTERVIEW**

An investigator should not detain a child involuntarily who is suspected of being a victim of child abuse solely for the purpose of an interview or physical exam without the consent of a parent or guardian unless one of the following applies:

- (a) Exigent circumstances exist, such as:
  - 1. A reasonable belief that medical issues of the child need to be addressed immediately.
  - 2. A reasonable belief that the child is or will be in danger of harm if the interview or physical exam is not immediately completed.
  - 3. The alleged offender is the custodial parent or guardian and there is reason to believe the child may be in continued danger.
- (b) A court order or warrant has been issued.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Child Abuse*

---

#### 420.7.3 INTERVIEWS AT A SCHOOL

Any student at school who is a suspected victim of child abuse shall be afforded the option of being interviewed in private or selecting any qualified available adult member of the school staff to be present. The purpose of the staff member's presence is to provide comfort and support. The staff member shall not participate in the interview. The selection of a staff member should be such that it does not burden the school with costs or hardship (Penal Code § 11174.3).

#### 420.8 MEDICAL EXAMINATIONS

If the child has been the victim of abuse that requires a medical examination, the investigating investigator should obtain consent for such examination from the appropriate parent, guardian or agency having legal custody of the child. The investigator should also arrange for the child's transportation to the appropriate medical facility.

In cases where the alleged offender is the custodial parent or guardian and is refusing consent for the medical examination, investigators should notify a supervisor before proceeding. If exigent circumstances do not exist or if state law does not provide for investigators to take the child for a medical examination, the notified supervisor should consider obtaining a court order for such an examination.

#### 420.9 DRUG-ENDANGERED CHILDREN

A coordinated response by law enforcement and social services agencies is appropriate to meet the immediate and longer-term medical and safety needs of children exposed to the manufacturing, trafficking or use of narcotics.

##### 420.9.1 SUPERVISOR RESPONSIBILITIES

The Investigative Bureau supervisor should:

- (a) Work with professionals from the appropriate agencies, including CPS, other law enforcement agencies, medical service providers and local prosecutors to develop community specific procedures for responding to situations where there are children endangered by exposure to methamphetamine labs or the manufacture and trafficking of other drugs.
- (b) Activate any available interagency response when an investigator notifies the Investigative Bureau supervisor that the investigator has responded to a drug lab or other narcotics crime scene where a child is present or where evidence indicates that a child lives there.
- (c) Develop a report format or checklist for use when investigators respond to drug labs or other narcotics crime scenes. The checklist will help investigators document the environmental, medical, social and other conditions that may affect the child.

##### 420.9.2 INVESTIGATOR RESPONSIBILITIES

Investigators responding to a drug lab or other narcotics crime scene where a child is present or where there is evidence that a child lives should:



# Stanislaus County District Attorney's Office

## Policy Manual

### *Child Abuse*

---

- (a) Document the environmental, medical, social and other conditions of the child using photography as appropriate and the checklist or form developed for this purpose.
- (b) Notify the Investigative Bureau supervisor so an interagency response can begin.

#### **420.10 STATE MANDATES AND OTHER RELEVANT LAWS**

California requires or permits the following:

##### **420.10.1 RELEASE OF REPORTS**

Information related to incidents of child abuse or suspected child abuse shall be confidential and may only be disclosed pursuant to state law and the Records Maintenance and Release Policy (Penal Code § 841.5; Penal Code § 11167.5).

##### **420.10.2 REQUESTS FOR REMOVAL FROM THE CHILD ABUSECENTRAL INDEX (CACI)**

Any person whose name has been forwarded to the California Department of Justice (DOJ) for placement in California's CACI, as a result of an investigation, may request that his/her name be removed from the CACI list. Requests shall not qualify for consideration if there is an active case, ongoing investigation or pending prosecution that precipitated the entry to CACI (Penal Code § 11169). All requests for removal shall be submitted in writing by the requesting person and promptly routed to the CACI hearing officer.

##### **420.10.3 CACI HEARING OFFICER**

The Investigative Bureau supervisor will normally serve as the hearing officer but must not be actively connected with the case that resulted in the person's name being submitted to CACI. Upon receiving a qualified request for removal, the hearing officer shall promptly schedule a hearing to take place during normal business hours and provide written notification of the time and place of the hearing to the requesting party.

##### **420.10.4 CACI HEARING PROCEDURES**

The hearing is an informal process where the person requesting removal from the CACI list will be permitted to present relevant evidence (e.g., certified copy of an acquittal, factual finding of innocence) as to why his/her name should be removed. The person requesting the hearing may record the hearing at his/her own expense.

Formal rules of evidence will not apply and the hearing officer may consider, in addition to evidence submitted by the person requesting the hearing, any relevant information including, but not limited to, the following:

- (a) Case reports including any supplemental reports
- (b) Statements by investigators
- (c) Statements from representatives of the District Attorney's Office
- (d) Statements by representatives of a child protective agency who may be familiar with the case

### *Child Abuse*

---

After considering all information presented, the hearing officer shall make a determination as to whether the requesting party's name should be removed from the CACI list. Such determination shall be based on a finding that the allegations in the investigation are not substantiated (Penal Code § 11169).

If, after considering the evidence, the hearing officer finds that the allegations are not substantiated, he/she shall cause a request to be completed and forwarded to the DOJ that the person's name be removed from the CACI list. A copy of the hearing results and the request for removal will be attached to the case reports.

The findings of the hearing officer shall be considered final and binding.

#### **420.11 TRAINING**

The Bureau should provide training on best practices in child abuse investigations to members tasked with investigating these cases. The training should include:

- (a) Participating in multidisciplinary investigations, as appropriate.
- (b) Conducting forensic interviews.
- (c) Availability of therapy services for children and families.
- (d) Availability of specialized forensic medical exams.
- (e) Cultural competence (including interpretive services) related to child abuse investigations.
- (f) Availability of victim advocate or guardian ad litem support.

# Immigration Violations

## 421.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines to members of the Stanislaus County District Attorney's Office relating to immigration and interacting with federal immigration officials.

### 421.1.1 DEFINITIONS

The following definitions apply to this policy (Government Code § 7284.4):

**Criminal immigration violation** - Any federal criminal immigration violation that penalizes a person's presence in, entry, or reentry to, or employment in, the United States. This does not include any offense where a judicial warrant already has been issued.

**Immigration enforcement** - Any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal civil immigration law, including any and all efforts to investigate, enforce, or assist in the investigation or enforcement of any federal criminal immigration law that penalizes a person's presence in, entry or reentry to, or employment in the United States.

**Judicial warrant** - An arrest warrant for a violation of federal criminal immigration law and issued by a federal judge or a federal magistrate judge.

## 421.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office that all members make personal and professional commitments to equal enforcement of the law and equal service to the public. Confidence in this commitment will increase the effectiveness of this bureau in protecting and serving the entire community and recognizing the dignity of all persons, regardless of their national origin or immigration status.

## 421.3 VICTIMS AND WITNESSES

To encourage crime reporting and cooperation in the investigation of criminal activity, all individuals, regardless of their immigration status, must feel secure that contacting or being addressed by members of law enforcement will not automatically lead to immigration inquiry and/or deportation. While it may be necessary to determine the identity of a victim or witness, members shall treat all individuals equally and not in any way that would violate the United States or California constitutions.

## 421.4 IMMIGRATION INQUIRIES PROHIBITED

Investigators shall not inquire into an individual's immigration status for immigration enforcement purposes (Government Code § 7284.6).

### 421.4.1 CALIFORNIA LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (CLETS)

Members shall not use information transmitted through CLETS for immigration enforcement purposes except for criminal history information and only when consistent with the California Values Act (Government Code § 15160).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Immigration Violations*

---

Members shall not use the system to investigate immigration violations of 8 USC § 1325 (improper entry) if that violation is the only criminal history in an individual's record (Government Code § 15160).

#### 421.4.2 CALIFORNIA DEPARTMENT OF MOTOR VEHICLES

Members shall not obtain, access, use, or otherwise disclose noncriminal history information maintained by the DMV for immigration enforcement (Vehicle Code § 1808.48).

#### **421.5 DETENTIONS AND ARRESTS**

An investigator shall not detain any individual, for any length of time, for a civil violation of federal immigration laws or a related civil warrant (Government Code § 7284.6).

An investigator who has a reasonable suspicion that an individual already lawfully contacted or detained has committed a criminal violation of 8 USC § 1326(a) (unlawful reentry) that may be subject to an enhancement due to a previous conviction of an aggravated felony under 8 USC § 1326(b)(2), may detain the person for a reasonable period of time to contact federal immigration officials to verify whether the United States Attorney General has granted the individual permission for reentry and whether the violation is subject to enhancement (Government Code § 7284.6). No individual who is otherwise ready to be released should continue to be detained only because questions about the individual's status are unresolved.

If the investigator has facts that establish probable cause to believe that a person already lawfully detained has violated 8 USC § 1326(a) and the penalty may be subject to enhancement due to prior conviction for specified aggravated felonies, he/she may arrest the individual for that offense (Government Code § 7284.6).

An investigator shall not detain any individual, for any length of time, for any other criminal immigration violation of federal immigration laws (Government Code § 7284.6).

An investigator should notify a supervisor as soon as practicable whenever an individual is arrested for violation of 8 USC § 1326(a).

##### 421.5.1 SUPERVISOR RESPONSIBILITIES

When notified that an investigator has arrested an individual for violation of 8 USC § 1326(a) or under the authority of a judicial warrant, the supervisor should determine whether it is appropriate to:

- (a) Transfer the person to federal authorities.
- (b) Transfer the person to jail.

#### **421.6 FEDERAL REQUESTS FOR ASSISTANCE**

Absent an urgent issue of officer safety or other emergency circumstances, requests by federal immigration officials for assistance from this bureau should be directed to a supervisor. The supervisor is responsible for determining whether the requested assistance would be permitted under the California Values Act (Government Code § 7284.2 et seq.).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Immigration Violations*

---

#### **421.7 INFORMATION SHARING**

No member of this bureau will prohibit, or in any way restrict, any other member from doing any of the following regarding the citizenship or immigration status, lawful or unlawful, of any individual (8 USC § 1373; Government Code § 7284.6):

- (a) Sending information to, or requesting or receiving such information from federal immigration officials
- (b) Maintaining such information in bureau records
- (c) Exchanging such information with any other federal, state, or local government entity

Nothing in this policy restricts sharing information that is permissible under the California Values Act.

##### **421.7.1 IMMIGRATION DETAINERS**

No individual should be held based solely on a federal immigration detainer under 8 CFR 287.7 (Government Code § 7284.6).

Notification to a federal authority may be made prior to release of an individual who is the subject of a notification request only if the individual meets one of the following conditions (Government Code § 7282.5; Government Code § 7284.6):

- (a) The individual has been arrested and had a judicial probable cause determination for a serious or violent felony identified in Penal Code § 667.5(c) or Penal Code § 1192.7(c).
- (b) The individual has been arrested and had a judicial probable cause determination for a felony punishable by time in a state prison.
- (c) The individual has been convicted of an offense as identified in Government Code § 7282.5(a).
- (d) The individual is a current registrant on the California Sex and Arson Registry.
- (e) The individual is identified by the U.S. Department of Homeland Security's Immigration and Customs Enforcement as the subject of an outstanding federal felony arrest warrant.

##### **421.7.2 NOTICE TO INDIVIDUALS**

Individuals in custody shall be given a copy of documentation received from U.S. Immigration and Customs Enforcement (ICE) regarding a hold, notification, or transfer request along with information as to whether the Stanislaus County District Attorney's Office intends to comply with the request (Government Code § 7283.1).

If the Stanislaus County District Attorney's Office provides ICE with notification that an individual is being, or will be, released on a certain date, the same notification shall be provided in writing to the individual and to his/her attorney or to one additional person who the individual may designate (Government Code § 7283.1).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Immigration Violations*

---

#### **421.7.3 ICE INTERVIEWS**

Before any interview regarding civil immigration violations takes place between ICE personnel and an individual in custody, the Stanislaus County District Attorney's Office shall provide the individual with a written consent form that explains the purpose of the interview, that the interview is voluntary, and that he/she may decline to be interviewed or may choose to be interviewed only with his/her attorney present. The consent form must be available in the languages specified in Government Code § 7283.1.

#### **421.7.4 TRANSFERS TO IMMIGRATION AUTHORITIES**

Members shall not transfer an individual to immigration authorities unless one of the following circumstances exist (Government Code § 7282.5; Government Code § 7284.6):

- (a) Transfer is authorized by a judicial warrant or judicial probable cause determination.
- (b) The individual has been convicted of an offense as identified in Government Code § 7282.5(a).
- (c) The individual is a current registrant on the California Sex and Arson Registry.
- (d) The individual is identified by the U.S. Department of Homeland Security's Immigration and Customs Enforcement as the subject of an outstanding federal felony arrest warrant.

#### **421.7.5 REPORTING TO CALIFORNIA DEPARTMENT OF JUSTICE**

The Investigative Bureau supervisor shall ensure that data regarding the number of transfers of an individual to immigration authorities, as permitted by Government Code § 7284.6(a)(4), and the offense that allowed for the transfer is collected and provided to the Records Manager for required reporting to the DOJ (Government Code § 7284.6(c)(2)(see the Records Bureau Policy)).

#### **421.8 U VISA AND T VISA NONIMMIGRANT STATUS**

Under certain circumstances, federal law allows temporary immigration benefits, known as a U visa, to victims and witnesses of certain qualifying crimes (8 USC § 1101(a)(15)(U)).

Similar immigration protection, known as a T visa, is available for certain qualifying victims of human trafficking (8 USC § 1101(a)(15)(T)).

Any request for assistance in applying for U visa or T visa status should be forwarded in a timely manner to the Investigative Bureau supervisor assigned to oversee the handling of any related case. The Investigative Bureau supervisor should:

- (a) Consult with the assigned investigator to determine the current status of any related case and whether further documentation is warranted.
- (b) Contact the appropriate prosecutor assigned to the case, if applicable, to ensure the certification or declaration has not already been completed and whether a certification or declaration is warranted.
- (c) Address the request and complete the certification or declaration, if appropriate, in a timely manner.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Immigration Violations*

---

1. The instructions for completing certification and declaration forms can be found on the U.S. Department of Homeland Security (DHS) website.
  2. Form I-918 Supplement B certification shall be completed if the victim qualifies under Penal Code § 679.10 (multiple serious offenses). The certification shall be completed and not refused for the specified reasons in Penal Code § 679.10(k)(3).
  3. Form I-914 Supplement B declaration shall be completed if the victim qualifies under Penal Code § 236.5 or Penal Code § 679.11 (human trafficking). The declaration shall be completed and not refused for completion for the specified reasons in Penal Code § 679.11(j)(3).
  4. Forward the completed Form I-918 Supplement B certification or completed Form I-914 declaration B to the victim, family member, or authorized representative (as defined in Penal Code § 679.10 and Penal Code § 679.11) without requiring the victim to provide government-issued identification (Penal Code § 679.10; Penal Code § 679.11)
- (d) Ensure that any decision to complete, or not complete, a certification or declaration form is documented in the case file and forwarded to the appropriate prosecutor. Include a copy of any completed form in the case file.
1. If Form I-918 Supplement B is not certified, a written explanation of denial shall be provided to the victim or authorized representative. The written denial shall include specific details of any reasonable requests for cooperation and a detailed description of how the victim refused to cooperate (Penal Code § 679.10).
- (e) Inform the victim liaison of any requests and their status.

#### 421.8.1 TIME FRAMES FOR COMPLETION

Investigators and their supervisors who are assigned to investigate a case of human trafficking as defined by Penal Code § 236.1 shall complete the above process and the documents needed for indicating the individual is a victim for the T visa application within 15 business days of the first encounter with the victim, regardless of whether it is requested by the victim (Penal Code § 236.5).

Investigators and their supervisors shall complete the above process and the documents needed certifying victim cooperation for a U visa or T visa application pursuant to Penal Code § 679.10 and Penal Code § 679.11 within 30 days of a request from the victim, victim's family, or authorized representative related to one of their assigned cases. If the victim is in removal proceedings, the certification shall be processed within seven days of the first business day following the day the request was received.

#### 421.8.2 REPORTING TO LEGISLATURE

The Investigative Bureau supervisor or the authorized designee should ensure that certification requests are reported to the Legislature in January of each year and include the number of certifications signed and the number denied. The report shall comply with Government Code § 9795 (Penal Code § 679.10; Penal Code § 679.11).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Immigration Violations*

---

#### 421.8.3 POLICE REPORTS

Upon request, an investigator or supervisor should provide a victim or authorized representative with a copy of the report filed by the victim within seven days of the request (Penal Code § 679.10).

#### **421.9 TRAINING**

The training Lieutenant should ensure that all appropriate members receive training on immigration issues.

Training should include:

- (a) Identifying civil versus criminal immigration violations.
- (b) Factors that may be considered in determining whether a criminal immigration violation has been committed.
- (c) Prohibitions contained in the California Values Act (Government Code § 7284 et seq.).



# Missing Persons

## 422.1 PURPOSE AND SCOPE

This policy provides guidance for handling missing person investigations.

### 422.1.1 DEFINITIONS

Definitions related to this policy include:

**At risk** - Includes but is not limited to (Penal Code § 14215):

- A victim of a crime or foul play
- A person missing and in need of medical attention
- A missing person with no pattern of running away or disappearing
- A missing person who may be the victim of parental abduction
- A mentally impaired missing person, including cognitively impaired or developmentally disabled

**Missing person** - Any person who is reported missing to law enforcement when the person's location is unknown. This includes a child who has been taken, detained, concealed, enticed away, or kept by a parent in violation of the law (Penal Code § 277 et seq.). It also includes any child who is missing voluntarily, involuntarily, or under circumstances that do not conform to their ordinary habits or behavior, and who may be in need of assistance (Penal Code § 14215).

**Missing person networks** - Databases or computer networks that are available to law enforcement and that are suitable for obtaining information related to missing persons investigations. This includes the National Crime Information Center (NCIC), the National Missing and Unidentified Persons System (NamUs), the California Law Enforcement Telecommunications System (CLETS), the Missing Person System (MPS), and the Unidentified Persons System (UPS).

## 422.2 POLICY

The Stanislaus County District Attorney's Office does not consider any report of a missing person to be routine and assumes that the missing person is in need of immediate assistance until an investigation reveals otherwise. The Stanislaus County District Attorney's Office gives missing person cases priority and will not require any time frame to pass before assisting a citizen wishing to make a missing person report. Sworn investigators of the bureau shall accept any missing person report and immediately, without delay assist the reporting party by contacting the jurisdiction having authority (police or sheriff) to initiate a missing person investigation (Penal Code § 14211).

## 422.3 REPORT PROCEDURES AND ROUTING

Employees should complete all missing person reports and forms promptly and advise the appropriate supervisor as soon as a missing person report is ready for review. Once approved by a Bureau Lieutenant or Chief Investigator, the Investigator receiving the report, will seek the

### *Missing Persons*

---

assistance from a Records Supervisor at the Sheriff's Office or local police department to ensure the missing person report is entered into the correct law enforcement databases.

#### **422.4 WHEN A MISSING PERSON IS FOUND**

When any person reported missing is found, the assigned investigator shall document the location of the missing person in the appropriate report, notify the relatives and/or reporting party, as appropriate, and other involved agencies and refer the case for additional investigation if warranted. Likewise, the investigator will seek the assistance of a Records Supervisor at the Sheriff's Office or local police department to ensure the proper notifications as listed below are accomplished.

The Records Manager shall ensure that, upon receipt of information that a missing person has been located, the following occurs (Penal Code § 14213):

- (a) Notification is made to California DOJ.
- (b) The missing person's school is notified.
- (c) Entries are made in the applicable missing person networks.
- (d) Immediately notify the Attorney General's Office.
- (e) Notification shall be made to any other law enforcement agency that took the initial report or participated in the investigation within 24 hours.

## Mental Illness Commitments

### 423.1 PURPOSE AND SCOPE

This policy provides guidelines for when investigators may take a person into custody for psychiatric evaluation and treatment (5150 commitment) (Welfare and Institutions Code § 5150).

### 423.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to protect the public and individuals through legal and appropriate use of the 72-hour treatment and evaluation commitment (5150 commitment) process.

### 423.3 AUTHORITY

An investigator having probable cause may take a person into custody and place the person in an approved mental health facility for 72-hour treatment and evaluation when the investigator believes that, as a result of a mental disorder, the person is a danger to him/herself or others or the person is gravely disabled (Welfare and Institutions Code § 5150; Welfare and Institutions Code § 5585.50).

When determining whether to take a person into custody, investigators are not limited to determining the person is an imminent danger and shall consider reasonably available information about the historical course of the person's mental disorder, which may include evidence presented from any of the following (Welfare and Institutions Code § 5150; Welfare and Institutions Code § 5150.05):

- (a) An individual who is providing or has provided mental health treatment or related support services to the person
- (b) A family member
- (c) The person subject to the determination or anyone designated by the person

#### 423.3.1 VOLUNTARY EVALUATION

If an investigator encounters an individual who may qualify for a 5150 commitment, the investigator may inquire as to whether the person desires to voluntarily be evaluated at an appropriate facility. If the person so desires, the investigators should:

- (a) Transport the person to an appropriate facility that is able to conduct the evaluation and admit the person pursuant to a 5150 commitment.
- (b) Document the circumstances surrounding the individual's desire to pursue voluntary evaluation and/or admission.

If at any point the person changes their mind regarding voluntary evaluation, investigators should proceed with the 5150 commitment, if appropriate.

### 423.4 CONSIDERATIONS AND RESPONSIBILITIES

Any investigator handling a call involving an individual who may qualify for a 5150 commitment should consider, as time and circumstances reasonably permit:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Mental Illness Commitments*

---

- (a) Available information that might assist in determining the cause and nature of the person's action or stated intentions.
- (b) Community or neighborhood mediation services.
- (c) Conflict resolution and de-escalation techniques.
- (d) Community or other resources available to assist in dealing with mental health issues.

While these steps are encouraged, nothing in this section is intended to dissuade investigators from taking reasonable action to ensure the safety of the investigators and others.

Investigators should consider a 5150 commitment over arrest when mental health issues appear to be a mitigating factor for people who are suspected of committing minor crimes or creating other public safety issues.

#### **423.4.1 SECURING OF PROPERTY**

When a person is taken into custody for evaluation, or within a reasonable time thereafter, and unless a responsible relative, guardian or conservator is in possession of the person's personal property, the investigator shall take reasonable precautions to safeguard the individual's personal property in his/her possession or on the premises occupied by the person (Welfare and Institutions Code § 5150).

The investigator taking the person into custody shall provide a report to the court that describes the person's property and its disposition in the format provided in Welfare and Institutions Code § 5211, unless a responsible person took possession of the property, in which case the investigator shall only include the name of the responsible person and the location of the property (Welfare and Institutions Code § 5150).

#### **423.5 TRANSPORTATION**

When transporting any individual for a 5150 commitment, the transporting investigator should have SR 911 notify the receiving facility of the estimated time of arrival, the level of cooperation of the individual and whether any special medical care is needed.

Investigators should request assistance from a patrol unit to transport individuals in a patrolcar with a cage and seatbelts and shall secure them in accordance with the Handcuffing and Restraints Policy. In some circumstances, Investigators may request a medical transport unit to take the individual to a medial facility. In any case, whomever transports, the Investigator shall respond to the facility and complete the required 72 hour hold paperwork to the appropriate medical staff.

#### **423.6 TRANSFER TO APPROPRIATE FACILITY**

Upon arrival at the facility, the investigator will escort the individual into a treatment area designated by a facility staff member. If the individual is not seeking treatment voluntarily, the investigator should provide the staff member with the written application for a 5150 commitment and remain present to provide clarification of the grounds for detention, upon request.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Mental Illness Commitments*

---

Absent exigent circumstances, the transporting investigator should not assist facility staff with the admission process, including restraint of the individual. However, if the individual is transported and delivered while restrained, the investigator may assist with transferring the individual to facility restraints and will be available to assist during the admission process, if requested. Under normal circumstances, investigators will not apply facility-ordered restraints.

#### **423.7 DOCUMENTATION**

The investigator shall complete an application for a 72-Hour detention for evaluation and treatment, provide it to the facility staff member assigned to that patient and retain a copy of the application for inclusion in the case report.

The application shall include the circumstances for investigator involvement; the probable cause to believe the person is, as a result of a mental health disorder, a danger to others or him/herself or gravely disabled; and all information used for the determination of probable cause (Welfare and Institutions Code § 5150; Welfare and Institutions Code § 5150.05).

The investigator should also provide a verbal summary to any evaluating staff member regarding the circumstances leading to the involuntary detention.

##### **423.7.1 ADVISEMENT**

The investigator taking a person into custody for evaluation shall advise the person of:

- (a) The investigator's name and agency.
- (b) The fact that the person is not under criminal arrest but is being taken for examination by mental health professionals and the mental health staff will advise him/her of their rights.
- (c) The name of the facility to which the person is being taken.
- (d) If the person is being taken into custody at his/her residence, he/she should also be advised that he/she may take a few personal items, which the investigator must approve, and may make a telephone call or leave a note indicating where he/she is being taken. The investigator should also ask if the person needs assistance turning off any appliance or water.

The advisement shall be given in a language the person understands. If the person cannot understand an oral advisement, the information shall be provided in writing (Welfare and Institutions Code § 5150).

#### **423.8 CRIMINAL OFFENSES**

Investigators investigating an individual who is suspected of committing a minor criminal offense and who is being taken on a 5150 commitment should resolve the criminal matter by issuing a warning or a Notice to Appear as appropriate.

When an individual who may qualify for a 5150 commitment has committed a serious criminal offense that would normally result in an arrest and transfer to a jail facility, the investigator should:

- (a) Arrest the individual when there is probable cause to do so.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Mental Illness Commitments*

---

- (b) Notify the appropriate supervisor of the facts supporting the arrest and the facts that would support the 5150 commitment.
- (c) Facilitate the individual's transfer to jail.
- (d) Thoroughly document in the related reports the circumstances that indicate the individual may qualify for a 5150 commitment.

In the supervisor's judgment, the individual may instead be arrested or booked and transported to the appropriate mental health facility. The supervisor should consider the seriousness of the offense, the treatment options available, the ability of this bureau to regain custody of the individual, bureau resources (e.g., posting a guard) and other relevant factors in making this decision.

#### **423.9 FIREARMS AND OTHER WEAPONS**

Whenever a person is taken into custody for a 5150 commitment, the handling investigators should seek to determine if the person owns or has access to any firearm or other deadly weapon defined in Welfare and Institutions Code § 8100. Investigators should consider whether it is appropriate and consistent with current search and seizure law under the circumstances to seize any such firearms or other dangerous weapons (e.g., safekeeping, evidence, consent).

Investigators are cautioned that a search warrant may be needed before entering a residence or other place to search, unless lawful, warrantless entry has already been made (e.g., exigent circumstances, consent). A search warrant may also be needed before searching for or seizing weapons

The handling investigators shall issue a receipt describing the deadly weapon or any firearm seized, and list any serial number or other identification that is on the firearm. Investigators shall advise the person of the procedure for the return of any firearm or other weapon that has been taken into custody (Welfare and Institutions Code § 8102 (b)) (see the Evidence Room Policy).

##### **423.9.1 PETITION FOR RETURN OF FIREARMS AND OTHER WEAPONS**

Whenever the handling investigator has cause to believe that the future return of any confiscated weapon might endanger the person or others, the investigator shall detail those facts and circumstances in a report. The report shall be forwarded to the Investigative Bureau, which shall be responsible for initiating a petition to the Superior Court for a hearing in accordance with Welfare and Institutions Code § 8102(c), to determine whether the weapon will be returned.

The petition to the Superior Court shall be initiated within 30 days of the release of the individual from whom such weapon has been confiscated, unless the Bureau makes an ex parte application to the court to extend the time to file such a petition, up to a maximum of 60 days. At the time any such petition is initiated, the Bureau shall send written notice to the individual informing him/her of the right to a hearing on the issue, that he/she has 30 days to confirm with the court clerk any desire for a hearing and that the failure to do so will result in the forfeiture of any confiscated weapon.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Mental Illness Commitments*

---

#### **423.10 TRAINING**

This bureau will endeavor to provide Peace Officer Standards and Training (POST)-approved advanced officer training on interaction with persons with mental disabilities, 5150 commitments and crisis intervention.

## Public Recording of Law Enforcement Activity

### 424.1 PURPOSE AND SCOPE

This policy provides guidelines for handling situations in which members of the public photograph or audio/video record law enforcement actions and other public activities that involve members of this bureau. In addition, this policy provides guidelines for situations where the recordings may be evidence.

### 424.2 POLICY

The Stanislaus County District Attorney's Office recognizes the right of persons to lawfully record members of this bureau who are performing their official duties. Members of this bureau will not prohibit or intentionally interfere with such lawful recordings. Any recordings that are deemed to be evidence of a crime or relevant to an investigation will only be collected or seized lawfully.

Investigators should exercise restraint and should not resort to highly discretionary arrests for offenses such as interference, failure to comply or disorderly conduct as a means of preventing someone from exercising the right to record members performing their official duties.

### 424.3 RECORDING LAW ENFORCEMENT ACTIVITY

Members of the public who wish to record law enforcement activities are limited only in certain aspects.

- (a) Recordings may be made from any public place or any private property where the individual has the legal right to be present (Penal Code § 69; Penal Code § 148).
- (b) Beyond the act of photographing or recording, individuals may not interfere with the law enforcement activity. Examples of interference include, but are not limited to:
  - 1. Tampering with a witness or suspect.
  - 2. Inciting others to violate the law.
  - 3. Being so close to the activity as to present a clear safety hazard to the investigators.
  - 4. Being so close to the activity as to interfere with an investigator's effective communication with a suspect or witness.
- (c) The individual may not present an undue safety risk to the investigators, him/herself or others.

### 424.4 INVESTIGATOR RESPONSE

Investigators should promptly request that a supervisor respond to the scene whenever it appears that anyone recording activities may be interfering with an investigation or it is believed that the recording may be evidence. If practicable, investigators should wait for the supervisor to arrive before taking enforcement action or seizing any cameras or recording media.

Whenever practicable, investigators or supervisors should give clear and concise warnings to individuals who are conducting themselves in a manner that would cause their recording or



# Stanislaus County District Attorney's Office

## Policy Manual

### *Public Recording of Law Enforcement Activity*

---

behavior to be unlawful. Accompanying the warnings should be clear directions on what an individual can do to be compliant; directions should be specific enough to allow compliance. For example, rather than directing an individual to clear the area, an investigator could advise the person that he/she may continue observing and recording from the sidewalk across the street.

If an arrest or other significant enforcement activity is taken as the result of a recording that interferes with law enforcement activity, investigators shall document in a report the nature and extent of the interference or other unlawful behavior and the warnings that were issued.

#### **424.5 SUPERVISOR RESPONSIBILITIES**

A supervisor should respond to the scene when requested or any time the circumstances indicate a likelihood of interference or other unlawful behavior.

The supervisor should review the situation with the investigator and:

- (a) Request any additional assistance as needed to ensure a safe environment.
- (b) Take a lead role in communicating with individuals who are observing or recording regarding any appropriate limitations on their location or behavior. When practical, the encounter should be recorded.
- (c) When practicable, allow adequate time for individuals to respond to requests for a change of location or behavior.
- (d) Ensure that any enforcement, seizure or other actions are consistent with this policy and constitutional and state law.
- (e) Explain alternatives for individuals who wish to express concern about the conduct of Bureau members, such as how and where to file a complaint.

#### **424.6 SEIZING RECORDINGS AS EVIDENCE**

Investigators should not seize recording devices or media unless (42 USC § 2000aa):

- (a) There is probable cause to believe the person recording has committed or is committing a crime to which the recording relates, and the recording is reasonably necessary for prosecution of the person.
  - 1. Absent exigency or consent, a warrant should be sought before seizing or viewing such recordings. Reasonable steps may be taken to prevent erasure of the recording.
- (b) There is reason to believe that the immediate seizure of such recordings is necessary to prevent serious bodily injury or death of any person.
- (c) The person consents.
  - 1. To ensure that the consent is voluntary, the request should not be made in a threatening or coercive manner.
  - 2. If the original recording is provided, a copy of the recording should be provided to the recording party, if practicable. The recording party should be permitted to be present while the copy is being made, if feasible. Another way to obtain

# Stanislaus County District Attorney's Office

## Policy Manual

### *Public Recording of Law Enforcement Activity*

---

the evidence is to transmit a copy of the recording from a device to a bureau-owned device.

Recording devices and media that are seized will be submitted within the guidelines of the Property and Evidence Policy.

# Informants

## 425.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use of informants.

### 425.1.1 DEFINITIONS

Definitions related to this policy include:

**Informant** - A person who covertly interacts with other individuals or suspects at the direction of, request of, or by agreement with, the Stanislaus County District Attorney's Office for law enforcement purposes. This also includes a person agreeing to supply information to the Stanislaus County District Attorney's Office for a benefit (e.g., a quid pro quo in the form of a reduced criminal penalty, money).

## 425.2 POLICY

The Stanislaus County District Attorney's Office recognizes the value of informants to law enforcement efforts and will strive to protect the integrity of the informant process. It is the policy of this bureau that all funds related to informant payments will be routinely audited and that payments to informants will be made according to the criteria outlined in this policy.

## 425.3 USE OF INFORMANTS

### 425.3.1 INITIAL APPROVAL

Before using an individual as an informant, an investigator must receive approval from his/her supervisor. The investigator shall compile sufficient information through a background investigation and experience with the informant in order to determine the suitability of the individual, including age, maturity and risk of physical harm, as well as any indicators of his/her reliability and credibility.

Members of this bureau should not guarantee absolute safety or confidentiality to an informant.

### 425.3.2 JUVENILE INFORMANTS

The use of informants under the age of 13 is prohibited.

Except for the enforcement of laws related to the commercial sale of alcohol, marijuana or tobacco products, a juvenile 13 years of age or older may only be used as an informant with the written consent of each of the following:

- (a) The juvenile's parents or legal guardians
- (b) The juvenile's attorney, if any
- (c) The court in which the juvenile's case is being handled, if applicable (Penal Code § 701.5)
- (d) The Chief of Investigations or the authorized designee

# Stanislaus County District Attorney's Office

## Policy Manual

### *Informants*

---

#### **425.3.3 INFORMANT AGREEMENTS**

All informants are required to sign and abide by the provisions of the designated bureau informant agreement and/or any informant agreement designated from a specialized Task Force unit where a District Attorney Criminal Investigator is assigned. The investigator using the informant shall discuss each of the provisions of the agreement with the informant.

Details of the agreement are to be approved in writing by a supervisor before being finalized with the informant.

#### **425.4 INFORMANT INTEGRITY**

To maintain the integrity of the informant process, the following must be adhered to:

- (a) The identity of an informant acting in a confidential capacity shall not be withheld from the Chief of Investigations, Lieutenant, supervisor or their authorized designees.
  - 1. Identities of informants acting in a confidential capacity shall otherwise be kept confidential.
- (b) Criminal activity by informants shall not be condoned.
- (c) Informants shall be told they are not acting as investigators, employees or agents of the Stanislaus County District Attorney's Office, and that they shall not represent themselves as such.
- (d) The relationship between bureau members and informants shall always be ethical and professional.
  - (a) Members shall not become intimately involved with an informant.
  - (b) Social contact shall be avoided unless it is necessary to conduct an official investigation, and only with prior approval of the supervisor.
  - (c) Members shall neither solicit nor accept gratuities or engage in any private business transaction with an informant.
- (e) Investigators shall not meet with informants in a private place unless accompanied by at least one additional investigator or with prior approval of the supervisor.
  - 1. Investigators may meet informants alone in an occupied public place, such as a restaurant.
- (f) When contacting informants for the purpose of making payments, investigators shall arrange for the presence of another investigator.
- (g) In all instances when bureau funds are paid to informants, a voucher shall be completed in advance, itemizing the expenses.
- (h) Since the decision rests with the appropriate prosecutor, investigators shall not promise that the informant will receive any form of leniency or immunity from criminal prosecution.

#### **425.4.1 UNSUITABLE INFORMANTS**

The suitability of any informant should be considered before engaging him/her in any way in a covert or other investigative process. Members who become aware that an informant may

# Stanislaus County District Attorney's Office

## Policy Manual

### *Informants*

---

be unsuitable will notify the supervisor, who will initiate a review to determine suitability. Until a determination has been made by a supervisor, the informant should not be used by any member. The supervisor shall determine whether the informant should be used by the Bureau and, if so, what conditions will be placed on his/her participation or any information the informant provides. The supervisor shall document the decision and conditions in file notes and mark the file "unsuitable" when appropriate.

Considerations for determining whether an informant is unsuitable include, but are not limited to, the following:

- (a) The informant has provided untruthful or unreliable information in the past.
- (b) The informant behaves in a way that may endanger the safety of an investigator.
- (c) The informant reveals to suspects the identity of an investigator or the existence of an investigation.
- (d) The informant appears to be using his/her affiliation with this bureau to further criminal objectives.
- (e) The informant creates officer-safety issues by providing information to multiple law enforcement agencies simultaneously, without prior notification and approval of each agency.
- (f) The informant engages in any other behavior that could jeopardize the safety of investigators or the integrity of a criminal investigation.
- (g) The informant commits criminal acts subsequent to entering into an informant agreement.

#### **425.5 INFORMANT FILES**

Informant files shall be utilized as a source of background information about the informant, to enable review and evaluation of information provided by the informant, and to minimize incidents that could be used to question the integrity of bureau members or the reliability of the informant.

Informant files shall be maintained in a secure area within the Bureau of Investigation. The Chief Investigator will assign a bureau lieutenant or an authorized designee to be responsible for maintaining informant files. Access to the informant files shall be restricted to the Chief of Investigations, Lieutenant, supervisor or their authorized designees.

The Lieutenant should arrange for an audit using a representative sample of randomly selected informant files on a periodic basis, but no less than one time per year. If the supervisor is replaced, the files will be audited before the new supervisor takes over management of the files. The purpose of the audit is to ensure compliance with file content and updating provisions of this policy. The audit should be conducted by a supervisor who does not have normal access to the informant files.

##### **425.5.1 FILE SYSTEM PROCEDURE**

A separate file shall be maintained on each informant and shall be coded with an assigned informant control number. An informant history that includes the following information shall be prepared for each file:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Informants*

---

- (a) Name and aliases
- (b) Date of birth
- (c) Physical description: sex, race, height, weight, hair color, eye color, scars, tattoos or other distinguishing features
- (d) Photograph
- (e) Current home address and telephone numbers
- (f) Current employers, positions, addresses and telephone numbers
- (g) Vehicles owned and registration information
- (h) Places frequented
- (i) Briefs of information provided by the informant and his/her subsequent reliability
  - 1. If an informant is determined to be unsuitable, the informant's file is to be marked "unsuitable" and notations included detailing the issues that caused this classification.
- (j) Name of the investigator initiating use of the informant
- (k) Signed informant agreement
- (l) Update on active or inactive status of informant

#### **425.6 INFORMANT PAYMENTS**

No informant will be told in advance or given an exact amount or percentage for his/her service. The amount of funds to be paid to any informant will be evaluated against the following criteria:

- The extent of the informant's personal involvement in the case
- The significance, value or effect on crime
- The value of assets seized
- The quantity of the drugs or other contraband seized
- The informant's previous criminal activity
- The level of risk taken by the informant

The Investigator will discuss the above factors with the Lieutenant and/or Task Force Supervisor and recommend the type and level of payment subject to approval by the Chief of Investigations.

##### **425.6.1 PAYMENT PROCESS**

Approved payments to an informant should be in cash using the following process:

- (a) Payments of \$500 and under may be paid in cash.
  - (a) The investigator and supervisor shall sign the paid voucher.
- (b) Payments exceeding \$500 shall be made by issuance of a check, payable to the investigator who will be delivering the payment.
  - (a) The check shall list the case numbers related to and supporting the payment.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Informants*

---

- (b) A written statement of the informant's involvement in the case shall be placed in the informant's file.
- (c) The statement shall be signed by the informant verifying the statement as a true summary of his/her actions in the case.
- (d) Authorization signatures from the Chief of Investigations and the District Attorney are required for disbursement of the funds.
- (c) To complete the payment process for any amount, the investigator delivering the payment shall complete a cash transfer form.
  - 1. The cash transfer form shall include the following:
    - (a) Date
    - (b) Payment amount
    - (c) Stanislaus County District Attorney's Office case number
    - (d) A statement that the informant is receiving funds in payment for information voluntarily rendered.
  - 2. The cash transfer form shall be signed by the informant.
  - 3. The cash transfer form will be kept in the informant's file.

#### 425.6.2 REPORTING OF PAYMENTS

Each informant receiving a cash payment shall be advised of his/her responsibility to report the cash to the Internal Revenue Service (IRS) as income. If funds distributed exceed \$600 in any reporting year, the informant should be provided IRS Form 1099 (26 CFR 1.6041-1). If such documentation or reporting may reveal the identity of the informant and by doing so jeopardize any investigation, the safety of investigators or the safety of the informant (26 CFR 1.6041-3), then IRS Form 1099 should not be issued.

In such cases, the informant shall be provided a letter identifying the amount he/she must report on a tax return as "other income" and shall be required to provide a signed acknowledgement of receipt of the letter. The completed acknowledgement form and a copy of the letter shall be retained in the informant's file.

#### 425.6.3 AUDIT OF PAYMENTS

The supervisor or the authorized designee shall be responsible for compliance with any audit requirements associated with grant provisions and applicable state and federal law.

At least once every six months, the Chief of Investigations or the authorized designee should conduct an audit of all informant funds for the purpose of accountability and security of the funds. The funds and related documents (e.g., buy/expense fund records, cash transfer forms, invoices, receipts and logs) will assist with the audit process.

## Senior and Disability Victimization

### 426.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the investigation and reporting of suspected abuse of certain adults who may be more vulnerable than others. This policy also addresses mandatory notification for Stanislaus County District Attorney's Office members as required by law (Penal Code § 368.6).

The Stanislaus County District Attorney's Office is committed to providing equal protection and demonstrating respect for all persons regardless of age or disabilities, and to conscientiously enforcing all criminal laws protecting elders, and adults and children with disabilities, regardless of whether these crimes also carry civil penalties (Penal Code § 368.6) (see Child Abuse Policy for child abuse investigations and reporting).

#### 426.1.1 DEFINITIONS

Definitions related to this policy include:

**Abuse of an elder (age 65 or older) or dependent adult** - Physical abuse, neglect, financial abuse, abandonment, isolation, abduction, or other treatment with resulting physical harm or pain or mental suffering; or the deprivation by a care custodian of goods or services that are necessary to avoid physical harm or mental suffering. Neglect includes self-neglect (Welfare and Institutions Code § 15610.05 et seq.; Penal Code § 368.5).

**Bureau protocols (or protocols)** - A procedure adopted by a local law enforcement agency consistent with the agency's organizational structure and stated in a policy adopted pursuant to this section, to effectively and accountably carry out a particular agency responsibility.

**Dependent adult** - An individual, regardless of whether the individual lives independently, between 18 and 64 years of age who has physical or mental limitations that restrict their ability to carry out normal activities or to protect their rights, including but not limited to persons who have physical or developmental disabilities or whose physical or mental abilities have diminished because of age. This also includes those admitted as inpatients to a 24-hour health facility, as defined in state law (Penal Code § 368; Welfare and Institutions Code § 15610.23).

**Elder and dependent adult abuse** - Any offense or attempted offense involving violence or neglect of an adult victim when committed by a person responsible for the adult's care, or any other act that would mandate reporting or notification to a social service agency or law enforcement (Penal Code § 368).

**Senior and disability victimization** - Means any of the following (Penal Code § 368.6):

- (a) Elder and dependent adult abuse
- (b) Unlawful interference with a mandated report
- (c) Homicide of an elder, dependent adult, or other adult or child with a disability



# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

- (d) Sex crimes against elders, dependent adults, or other adults and children with disabilities
- (e) Child abuse of children with disabilities
- (f) Violation of relevant protective orders
- (g) Hate crimes against persons with actual or perceived disabilities, including but not limited to disabilities caused by advanced age, or those associated with them
- (h) Domestic violence against elders, dependent adults, and adults and children with disabilities, including disabilities caused by advanced age

#### **426.2 POLICY**

The Stanislaus County District Attorney's Office will investigate all reported incidents of alleged elder and dependent adult abuse and ensure proper reporting and notification as required by law.

##### **426.2.1 ADHERENCE TO POLICY**

All investigators are required to be familiar with the policy and carry out the policy at all times, except in the case of an unusual compelling circumstance as determined and approved by a supervisor (Penal Code § 368.6).

Any supervisor who determines and approves an investigator's deviation from this policy shall provide a written report to the Chief of Investigations that states the unusual compelling circumstances regarding the deviation. A copy of this report will be made available to the alleged victim and reporting party pursuant to bureau protocols (Penal Code § 368.6(c)(27)).

The Chief of Investigations shall retain the report for a minimum of five years and shall make it available to the state protection and advocacy agency upon request (Penal Code § 368.6(c)(27)).

#### **426.3 INVESTIGATIONS AND REPORTING**

All reported or suspected cases of elder and dependent adult abuse require investigation and a report, even if the allegations appear unfounded or unsubstantiated (Penal Code § 368.6).

Investigations and reports related to suspected cases of elder and dependent adult abuse should address, as applicable:

- (a) The overall basis for the contact. This should be done by the investigating investigator in all circumstances where a suspected elder and dependent adult abuse victim is contacted.
- (b) Any relevant statements the victim may have made and to whom he/she made the statements.
- (c) If a person is taken into protective custody, the reasons, the name and title of the person making the decision, and why other alternatives were not appropriate.
- (d) Documentation of any visible injuries or any injuries identified by the victim. This should include photographs of such injuries, if practicable.
- (e) Whether the victim was transported for medical treatment or a medical examination.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

- (f) Whether the victim identified a household member as the alleged perpetrator, and a list of the names of any other potential victims or witnesses who may reside in the residence.
- (g) Identification of any prior related reports or allegations of abuse, including other jurisdictions, as reasonably known.
- (h) Previous addresses of the victim and suspect.
- (i) Other potential witnesses who have not yet been interviewed, such as relatives or others close to the victim's environment.
- (j) Witness and suspect statements if available.
- (k) Review of all portable audio/video recorders, devices, and other available video.
- (l) Call history related to the elder or dependent adult including calls from mandated reporters or other individuals.
- (m) Whether the abuse is related to a disability-bias hate crime and related bias motivations (Penal Code § 368.6) (see the Hate Crimes Policy for additional guidance).
- (n) Results of investigations shall be provided to those agencies (Adult Protective Services (APS), long-term ombudsman) that referred or reported the elder or dependent adult abuse (Welfare and Institutions Code § 15640(f)).
- (o) Whether a death involved the End of Life Option Act:
  - 1. Whether or not assistance was provided to the person beyond that allowed by law (Health and Safety Code § 443.14).
  - 2. Whether an individual knowingly altered or forged a request for an aid-in-dying drug to end a person's life without his/her authorization, or concealed or destroyed a withdrawal or rescission of a request for an aid-in-dying drug (Health and Safety Code § 443.17).
  - 3. Whether coercion or undue influence was exerted on the person to request or ingest an aid-in-dying drug or to destroy a withdrawal or rescission of a request for such medication (Health and Safety Code § 443.17).
  - 4. Whether an aid-in-dying drug was administered to a person without his/her knowledge or consent (Health and Safety Code § 443.17).

Any unexplained death of an adult who was in the care of a guardian or caretaker should be considered as potential elder or dependent adult abuse and investigated similarly.

An unexplained or suspicious death of an elder, dependent adult, or other adult or child with a disability should be treated as a potential homicide until a complete investigation including an autopsy is completed, and it should not be assumed that the death of an elder or person with a disability is natural simply because of the age or disability of the deceased (Penal Code § 368.6(c)(18)).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

#### 426.3.1 ADDITIONAL INVESTIGATIVE CONSIDERATIONS

The following factors as provided in Penal Code § 368.6 should be considered when investigating incidents of elder and dependent adult abuse:

- (a) Elder and dependent adult abuse, sex crimes, child abuse, domestic violence, and any other criminal act, when committed in whole or in part because of the victim's actual or perceived disability, including disability caused by advanced age, is also a hate crime (Penal Code § 368.6) (see the Hate Crimes Policy for additional guidance).
- (b) Senior and disability victimization crimes are also domestic violence subject to the mandatory arrest requirements of Penal Code § 836 if they meet the elements described in Penal Code § 273.5, including but not limited to a violation by a caretaker or other person who is or was a cohabitant of the victim, regardless of whether the cohabitant is or was a relative of, or in an intimate personal relationship with, the victim (Penal Code § 368.6(c)(10)).
- (c) Many victims of sexual assault and other sex crimes delay disclosing the crimes for reasons including but not limited to shame, embarrassment, self-doubt, fear of being disbelieved, and fear of retaliation by the perpetrator or others (Penal Code § 368.6(c)(11)).
- (d) Victims and witnesses with disabilities, including cognitive and communication disabilities, can be highly credible witnesses when interviewed appropriately by trained officers or other trained persons (Penal Code § 368.6(c)(14)).

#### 426.4 QUALIFIED INVESTIGATORS

Qualified investigators should be available to investigate cases of elder and dependent adult abuse. These investigators should:

- (a) Conduct interviews in appropriate interview facilities.
- (b) Be familiar with forensic interview techniques specific to elder and dependent adult abuse investigations.
- (c) Present all cases of alleged elder and dependent adult abuse to the prosecutor for review.
- (d) Coordinate with other enforcement agencies, social service agencies, and facility administrators as needed (Welfare and Institutions Code § 15650).
- (e) Provide referrals to therapy services, victim advocates, guardians, and support for the victim and family as appropriate (see the Victim and Witness Assistance Policy for additional guidance).
  - 1. Ensure victims of sex crimes know their right to have a support person of their choice present at all times during an interview or contact (Penal Code § 368.6) (see the Sexual Assault Investigations Policy for additional guidance).
  - 2. Referrals to the crime victim liaison as appropriate for victims requiring further assistance or information regarding benefits from crime victim resources.
- (f) Participate in or coordinate with multidisciplinary investigative teams as applicable (Welfare and Institutions Code § 15610.55).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

- (g) Make reasonable efforts to determine whether any person committed unlawful interference in a mandated report.

#### **426.5 MANDATORY NOTIFICATION**

Members of the Stanislaus County District Attorney's Office shall notify the local office of the California Department of Social Services (CDSS) APS agency of known, suspected, or alleged instances of abuse when they reasonably suspect, have observed, or have knowledge of an incident that reasonably appears to be abuse of an elder or dependent adult, or are told by an elder or dependent adult that the person has experienced abuse (Welfare and Institutions Code § 15630(b)).

Notification shall be made by telephone or through a confidential internet reporting tool as soon as practicable. If notification is made by telephone, a written report shall be sent or internet report shall be made through the confidential internet reporting tool within two working days, as provided in Welfare and Institutions Code § 15630(b).

Notification shall also be made to the following agencies as soon as practicable or as provided below (Welfare and Institutions Code § 15630):

- (a) If the abuse occurred in a long-term care facility (not a state mental health hospital or a state developmental center), notification shall be made as follows (Welfare and Institutions Code § 15630(b)(1)):
  - 1. If there is serious bodily injury, notification shall be made by telephone and, within two hours, a written report shall be made to the local ombudsman and the corresponding licensing agency.
  - 2. If the abuse is allegedly caused by a resident with dementia and there is no serious bodily injury, notification shall be made by a written report to the local ombudsman within 24 hours.
  - 3. If there is any other abuse in a long-term care facility (not a state mental health or a state developmental center), a written report shall be made to the local ombudsman and corresponding state licensing agency within 24 hours.
- (b) The California Department of Public Health (DPH) shall be notified of all known or suspected abuse in a long-term care facility.
- (c) The CDSS shall be notified of all known or suspected abuse occurring in a residential care facility for the elderly or in an adult day program.
- (d) If the abuse occurred in an adult day health care center, DPH and the California Department of Aging shall be notified.
- (e) The Division of Medi-Cal Fraud and Elder Abuse shall be notified of all abuse that constitutes criminal activity in a long-term care facility.
- (f) The District Attorney's office shall be notified of all cases of physical abuse and financial abuse in a long-term care facility.
- (g) If the abuse occurred at a state mental hospital or a state developmental center, notification shall be made to the designated investigators of the California Department

# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

of State Hospitals or the California Department of Developmental Services as soon as practicable but no later than two hours after law enforcement becomes aware of the abuse (Welfare and Institutions Code § 15630(b)).

1. When a report of abuse is received by the Bureau, investigation efforts shall be coordinated with the designated investigators of the California Department of State Hospitals or the California Department of Developmental Services (Welfare and Institutions Code § 15630(b)).
- (h) If during an investigation it is determined that the elder or dependent adult abuse is being committed by a licensed health practitioner as identified in Welfare and Institutions Code § 15640(b), the appropriate licensing agency shall be immediately notified (Welfare and Institutions Code 15640(b)).
- (i) When the Bureau receives a report of abuse, neglect, or abandonment of an elder or dependent adult alleged to have occurred in a long-term care facility, the licensing agency shall be notified by telephone as soon as practicable (Welfare and Institutions Code § 15640(e)).

The Investigative Bureau supervisor is responsible for ensuring that proper notifications have occurred to the District Attorney's Office and any other regulatory agency that may be applicable based upon where the abuse took place (e.g., care facility, hospital) per Welfare and Institutions Code § 15630(b).

Notification is not required for a person who was merely present when a person self-administered a prescribed aid-in-dying drug or a person prepared an aid-in-dying drug so long as the person did not assist the individual in ingesting the aid-in-dying drug (Health and Safety Code § 443.14; Health and Safety Code § 443.18).

Failure to report or impeding or inhibiting a report of abuse of an elder or dependent adult is a misdemeanor (Welfare and Institutions Code §15630(h)).

#### 426.5.1 NOTIFICATION PROCEDURE

Notification should include the following information, if known (Welfare and Institutions Code § 15630(e)):

- (a) The name of the person making the report.
- (b) The name and age of the elder or dependent adult.
- (c) The present location of the elder or dependent adult.
- (d) The names and addresses of family members or any other adult responsible for the care of the elder or dependent adult.
- (e) The nature and extent of the condition of the elder or dependent adult.
- (f) The date of incident.
- (g) Any other information, including information that led the person to suspect elder or dependent adult abuse.

### *Senior and Disability Victimization*

---

#### **426.6 PROTECTIVE CUSTODY**

Before taking an elder or dependent adult abuse victim into protective custody when facts indicate the adult may not be able to care for him/herself, the investigator should make reasonable attempts to contact APS. Generally, removal of an adult abuse victim from his/her family, guardian, or other responsible adult should be left to the welfare authorities when they are present or have become involved in an investigation.

Generally, members of this bureau should remove an elder or dependent adult abuse victim from his/her family or guardian without a court order only when no other effective alternative is reasonably available and immediate action reasonably appears necessary to protect the victim. Prior to taking an elder or dependent adult abuse victim into protective custody, the investigator should take reasonable steps to deliver the adult to another qualified legal guardian, unless it reasonably appears that the release would endanger the victim or result in abduction. If this is not a reasonable option, the investigator shall ensure that the adult is delivered to APS.

Whenever practicable, the investigator should inform a supervisor of the circumstances prior to taking an elder or dependent adult abuse victim into protective custody. If prior notification is not practicable, investigators should contact a supervisor promptly after taking the adult into protective custody.

When elder or dependent adult abuse victims are under state control, have a state-appointed guardian, or there are other legal holdings for guardianship, it may be necessary or reasonable to seek a court order on behalf of the adult victim to either remove the adult from a dangerous environment (protective custody) or restrain a person from contact with the adult.

##### **426.6.1 EMERGENCY PROTECTIVE ORDERS**

In any situation which an investigator reasonably believes that an elder or dependent adult is in immediate and present danger of abuse based on an allegation of a recent incident of abuse or threat of abuse (other than financial abuse alone), the investigator may seek an emergency protective order against the person alleged to have committed or threatened such abuse (Family Code § 6250(d)).

##### **426.6.2 VERIFICATION OF PROTECTIVE ORDER**

Whenever an investigator verifies that a relevant protective order has been issued, the investigator shall make reasonable efforts to determine if the order prohibits the person from possession of firearms or requires the relinquishment of firearms, and if the order does so, the investigator shall make reasonable efforts to (Penal Code § 368.6(c)(19)):

- (a) Inquire whether the restrained person possesses firearms. The investigator should make this effort by asking the restrained person and the protected person.
- (b) Query the California Law Enforcement Telecommunications System to determine if any firearms are registered to the restrained person.
- (c) Receive or seize prohibited firearms located in plain view or pursuant to a consensual or other lawful search in compliance with Penal Code § 18250 et seq. and in accordance with bureau procedures.

### *Senior and Disability Victimization*

---

#### **426.7 INTERVIEWS**

##### **426.7.1 PRELIMINARY INTERVIEWS**

Absent extenuating circumstances or impracticality, investigators should audio record the preliminary interview with a suspected elder or dependent adult abuse victim. Investigators should avoid multiple interviews with the victim and should attempt to gather only the information necessary to begin an investigation. When practicable, investigating investigators should defer interviews until a person who is specially trained in such interviews is available.

##### **426.7.2 DETAINING VICTIMS FOR INTERVIEWS**

An investigator should not detain an adult involuntarily who is suspected of being a victim of abuse solely for the purpose of an interview or physical exam without his/her consent or the consent of a guardian unless one of the following applies:

- (a) Exigent circumstances exist, such as:
  - 1. A reasonable belief that medical issues of the adult need to be addressed immediately.
  - 2. A reasonable belief that the adult is or will be in danger of harm if the interview or physical exam is not immediately completed.
  - 3. The alleged offender is a family member or guardian and there is reason to believe the adult may be in continued danger.
- (b) A court order or warrant has been issued.

##### **426.7.3 INTERVIEWS WITH A PERSON WITH DEAFNESS OR HEARING LOSS**

An investigator who is interviewing a victim or witness who reports or demonstrates deafness or hearing loss should secure the services of a qualified interpreter (as defined by Evidence Code § 754) prior to the start of the interview (Penal Code § 368.6) (see the Communications with Persons with Disabilities Policy for additional guidance).

#### **426.8 MEDICAL EXAMINATIONS**

When an elder or dependent adult abuse investigation requires a medical examination, the investigating investigator should obtain consent for such examination from the victim, guardian, agency, or entity having legal custody of the adult. The investigator should also arrange for the adult's transportation to the appropriate medical facility.

In cases where the alleged offender is a family member, guardian, agency, or entity having legal custody and is refusing to give consent for the medical examination, investigators should notify a supervisor before proceeding. If exigent circumstances do not exist or if state law does not provide for investigators to take the adult for a medical examination, the supervisor should consider other government agencies or services that may obtain a court order for such an examination.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

#### **426.9 DRUG-ENDANGERED VICTIMS**

A coordinated response by law enforcement and social services agencies is appropriate to meet the immediate and longer-term medical and safety needs of an elder or dependent adult abuse victim who has been exposed to the manufacturing, trafficking, or use of narcotics.

##### **426.9.1 INVESTIGATOR RESPONSIBILITIES**

Investigators responding to a drug lab or other narcotics crime scene where an elder or dependent adult abuse victim is present or where there is evidence that an elder or dependent adult abuse victim lives should:

- (a) Document the environmental, medical, social, and other conditions of the adult, using photography as appropriate and the checklist or form developed for this purpose.
- (b) Notify the Investigative Bureau supervisor so an interagency response can begin.

##### **426.9.1 SUPERVISOR RESPONSIBILITIES**

The Investigative Bureau supervisor should:

- (a) Work with professionals from the appropriate agencies, including APS, other law enforcement agencies, medical service providers, and local prosecutors, to develop community specific procedures for responding to situations where there are elder or dependent adult abuse victims endangered by exposure to methamphetamine labs or the manufacture and trafficking of other drugs.
- (b) Activate any available interagency response when an investigator notifies the Investigative Bureau supervisor that he/she has responded to a drug lab or other narcotics crime scene where an elder or dependent adult abuse victim is present or where evidence indicates that an elder or dependent adult abuse victim lives.
- (c) Develop a report format or checklist for use when investigators respond to drug labs or other narcotics crime scenes. The checklist will help investigators document the environmental, medical, social, and other conditions that may affect the adult.

#### **426.10 RECORDS BUREAU RESPONSIBILITIES**

The Records Bureau is responsible for:

- (a) Providing a copy of the elder or dependent adult abuse report to the APS, ombudsman, or other agency as applicable within two working days or as required by law (Welfare and Institutions Code § 15630; Welfare and Institutions Code § 15640(c)).
- (b) Retaining the original elder or dependent adult abuse report with the initial case file.

#### **426.11 JURISDICTION**

The Stanislaus County District Attorney's Office has concurrent jurisdiction with state law enforcement agencies when investigating elder and dependent adult abuse and all other crimes against elder victims and victims with disabilities (Penal Code § 368.5).

Adult protective services agencies and local long-term care ombudsman programs also have jurisdiction within their statutory authority to investigate elder and dependent adult abuse and criminal neglect and may assist in criminal investigations upon request, if consistent with federal



# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

law, in such cases. However, this bureau will retain responsibility for the criminal investigations (Penal Code § 368.5).

Additional jurisdiction responsibilities for investigations of abuse involving various facilities and agencies may be found in Welfare and Institutions Code § 15650.

#### **426.12 TRAINING**

The Bureau should provide training on best practices in elder and dependent adult abuse investigations to members tasked with investigating these cases. The training should include:

- (a) Participating in multidisciplinary investigations, as appropriate.
- (b) Conducting interviews.
- (c) Availability of therapy services for adults and families.
- (d) Availability of specialized forensic medical exams.
- (e) Cultural competence (including interpretive services) related to elder and dependent adult abuse investigations.
- (f) Availability of victim advocates or other support.

##### **426.12.1 MANDATORY TRAINING**

The Lieutenant shall ensure that appropriate personnel receive the required training, including:

- (a) Materials from POST as described in Penal Code § 368.6(c)(5)(A).
- (b) Advanced training on senior and disability victimization available from POST, the United States Department of Justice, the Disability and Abuse Project of the Spectrum Institute, or other sources as provided by Penal Code § 368.6(c)(16)(A).
  - 1. Training should include the following:
    - (a) Information on the wide prevalence of elder and dependent adult abuse, sexual assault, other sex crimes, hate crimes, domestic violence, human trafficking, and homicide against adults and children with disabilities, including disabilities caused by advanced age, and including those crimes often committed by caretakers (Penal Code § 368.6(c)(1)).
    - (b) Information on the history of elder and dependent adult abuse and crimes against individuals with disabilities (see the POST Senior and Disability Victimization Policy Guidelines).

#### **426.13 RELEVANT STATUTES**

##### **Penal Code § 288 (a) and Penal Code § 288 (b)(2)**

(a) Except as provided in subdivision (i), a person who willfully and lewdly commits any lewd or lascivious act, including any of the acts constituting other crimes provided for in Part 1 (Of Crimes and Punishments of the Penal Code) upon or with the body, or any part or member thereof, of a child who is under the age of 14 years, with the intent of arousing, appealing to, or gratifying the lust, passions, or sexual desires of that person or the child, is guilty of a felony and shall be punished by imprisonment in the state prison for three, six, or eight years.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

(b)(2) A person who is a caretaker and commits an act described in subdivision (a) upon a dependent person by use of force, violence, duress, menace, or fear of immediate and unlawful bodily injury on the victim or another person, with the intent described in subdivision (a), is guilty of a felony and shall be punished by imprisonment in the state prison for 5, 8, or 10 years.

#### **Penal Code § 368 (c)**

A person who knows or reasonably should know that a person is an elder or dependent adult and who, under circumstances or conditions other than those likely to produce great bodily harm or death, willfully causes or permits any elder or dependent adult to suffer, or inflicts thereon unjustifiable physical pain or mental suffering, or having the care or custody of any elder or dependent adult, willfully causes or permits the person or health of the elder or dependent adult to be injured or willfully causes or permits the elder or dependent adult to be placed in a situation in which their person or health may be endangered, is guilty of a misdemeanor.

#### **Penal Code § 368 (f)**

A person who commits the false imprisonment of an elder or a dependent adult by the use of violence, menace, fraud, or deceit is punishable by imprisonment pursuant to subdivision (h) of Section 1170 for two, three, or four years.

Protections provided by the above Penal Code § 288 and Penal Code § 368 protect many persons with disabilities regardless of the fact they live independently.

#### **Welfare and Institutions Code § 15610.05**

"Abandonment" means the desertion or willful forsaking of an elder or a dependent adult by anyone having care or custody of that person under circumstances in which a reasonable person would continue to provide care and custody.

#### **Welfare and Institutions Code § 15610.06**

"Abduction" means the removal from this state and the restraint from returning to this state, or the restraint from returning to this state, of any elder or dependent adult who does not have the capacity to consent to the removal from this state and the restraint from returning to this state, or the restraint from returning to this state, as well as the removal from this state or the restraint from returning to this state, of any conservatee without the consent of the conservator or the court.

#### **Welfare and Institutions Code § 15610.30**

- (a) "Financial abuse" of an elder or dependent adult occurs when a person or entity does any of the following:
  - 1. Takes, secretes, appropriates, obtains, or retains real or personal property of an elder or dependent adult for a wrongful use or with intent to defraud, or both.
  - 2. Assists in taking, secreting, appropriating, obtaining, or retaining real or personal property of an elder or dependent adult for a wrongful use or with intent to defraud, or both.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

3. Takes, secretes, appropriates, obtains, or retains, or assists in taking, secreting, appropriating, obtaining, or retaining, real or personal property of an elder or dependent adult by undue influence, as defined in Section 15610.70.
- (b) A person or entity shall be deemed to have taken, secreted, appropriated, obtained, or retained property for a wrongful use if, among other things, the person or entity takes, secretes, appropriates, obtains, or retains the property and the person or entity knew or should have known that this conduct is likely to be harmful to the elder or dependent adult.
- (c) For purposes of this section, a person or entity takes, secretes, appropriates, obtains, or retains real or personal property when an elder or dependent adult is deprived of any property right, including by means of an agreement, donative transfer, or testamentary bequest, regardless of whether the property is held directly or by a representative of an elder or dependent adult.
- (d) For purposes of this section, "representative" means a person or entity that is either of the following:
  1. A conservator, trustee, or other representative of the estate of an elder or dependent adult.
  2. An attorney-in-fact of an elder or dependent adult who acts within the authority of the power of attorney.

#### **Welfare and Institutions Code § 15610.43**

- (a) "Isolation" means any of the following:
  1. Acts intentionally committed for the purpose of preventing, and that do serve to prevent, an elder or dependent adult from receiving his or her mail or telephone calls.
  2. Telling a caller or prospective visitor that an elder or dependent adult is not present, or does not wish to talk with the caller, or does not wish to meet with the visitor where the statement is false, is contrary to the express wishes of the elder or the dependent adult, whether he or she is competent or not, and is made for the purpose of preventing the elder or dependent adult from having contact with family, friends, or concerned persons.
  3. False imprisonment, as defined in Section 236 of the Penal Code.
  4. Physical restraint of an elder or dependent adult, for the purpose of preventing the elder or dependent adult from meeting with visitors.
- (b) The acts set forth in subdivision (a) shall be subject to a rebuttable presumption that they do not constitute isolation if they are performed pursuant to the instructions of a physician and surgeon licensed to practice medicine in the state, who is caring for the elder or dependent adult at the time the instructions are given, and who gives the instructions as part of his or her medical care.
- (c) The acts set forth in subdivision (a) shall not constitute isolation if they are performed in response to a reasonably perceived threat of danger to property or physical safe.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

#### **Welfare and Institutions Code § 15610.57**

- (a) "Neglect" means either of the following:
  - 1. The negligent failure of any person having the care or custody of an elder or a dependent adult to exercise that degree of care that a reasonable person in a like position would exercise.
  - 2. The negligent failure of an elder or dependent adult to exercise that degree of self care that a reasonable person in a like position would exercise.
- (b) Neglect includes, but is not limited to, all of the following:
  - 1. Failure to assist in personal hygiene, or in the provision of food, clothing, or shelter.
  - 2. Failure to provide medical care for physical and mental health needs. A person shall not be deemed neglected or abused for the sole reason that the person voluntarily relies on treatment by spiritual means through prayer alone in lieu of medical treatment.
  - 3. Failure to protect from health and safety hazards.
  - 4. Failure to prevent malnutrition or dehydration.
  - 5. Substantial inability or failure of an elder or dependent adult to manage personal finances.
  - 6. Failure of an elder or dependent adult to satisfy any of the needs specified in paragraphs (1) to (5), inclusive, for themselves as a result of poor cognitive functioning, mental limitation, substance abuse, or chronic poor health.
- (c) Neglect includes being homeless if the elder or dependent adult is also unable to meet any of the needs specified in paragraphs (1) to (5), inclusive, of subdivision (b).

#### **Welfare and Institutions Code § 15610.63**

"Physical abuse" means any of the following:

- (a) Assault, as defined in Section 240 of the Penal Code.
- (b) Battery, as defined in Section 242 of the Penal Code.
- (c) Assault with a deadly weapon or force likely to produce great bodily injury, as defined in Section 245 of the Penal Code.
- (d) Unreasonable physical constraint, or prolonged or continual deprivation of food or water.
- (e) Sexual assault, that means any of the following:
  - 1. Sexual battery, as defined in Section 243.4 of the Penal Code.
  - 2. Rape, as defined in Section 261 of the Penal Code, or former Section 262 of the Penal Code.
  - 3. Rape in concert, as described in Section 264.1 of the Penal Code.
  - 4. Incest, as defined in Section 285 of the Penal Code.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

5. Sodomy, as defined in Section 286 of the Penal Code.
  6. Oral copulation, as defined in Section 287 or former Section 288a of the Penal Code.
  7. Sexual penetration, as defined in Section 289 of the Penal Code.
  8. Lewd or lascivious acts as defined in paragraph (2) of subdivision (b) of Section 288 of the Penal Code.
- (f) Use of a physical or chemical restraint or psychotropic medication under any of the following conditions:
1. For punishment.
  2. For a period beyond that for which the medication was ordered pursuant to the instructions of a physician and surgeon licensed in the State of California, who is providing medical care to the elder or dependent adult at the time the instructions are given.
  3. For any purpose not authorized by the physician and surgeon.

#### **426.14 CHIEF OF INVESTIGATIONS RESPONSIBILITIES**

The Chief of Investigations or the authorized designee responsibilities include but are not limited to (Penal Code § 368.6):

- (a) Taking leadership within the Bureau and in the community, including by speaking out publicly in major cases of senior and disability victimization, to assure the community of bureau support for the victims and their families and for others in the community who are terrorized and traumatized by the crimes, and to encourage victims and witnesses to the crimes or similar past or future crimes to report those crimes to help bring the perpetrators to justice and prevent further crimes.
- (b) Developing and including bureau protocols in this policy, including but not limited to the following:
  1. Protocols for seeking emergency protective orders by phone from a court at any time of day or night pursuant to Family Code § 6250(d).
  2. Protocols for arrest warrants and arrests for senior and disability victimization for matters other than domestic violence and consistent with the requirements of Penal Code § 368.6(c)(9)(B) that include the following:
    - (a) In the case of a senior and disability victimization committed in an investigator's presence, including but not limited to a violation of a relevant protective order, the investigator shall make a warrantless arrest based on probable cause when necessary or advisable to protect the safety of the victim or others.
    - (b) In the case of a felony not committed in an investigator's presence, the officer shall make a warrantless arrest based on probable cause when necessary or advisable to protect the safety of the victim or others.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Senior and Disability Victimization*

---

- (c) In the case of a misdemeanor not committed in the investigator's presence, including but not limited to misdemeanor unlawful interference with a mandated report or a misdemeanor violation of a relevant protective order, or when necessary or advisable to protect the safety of the victim or others, the agency shall seek an arrest warrant based on probable cause.
  - (d) Protocol for seeking arrest warrants based on probable cause for crimes for which no arrest has been made.
- 3. Procedures for first responding investigators to follow when interviewing persons with cognitive and communication disabilities until investigators, or staff of other responsible agencies with more advanced training, are available. The procedure shall include an instruction to avoid repeated interviews whenever possible.
- (c) For each bureau protocol, include either a specific title-by-title list of investigator responsibilities or a specific office or unit in the Bureau responsible for implementing the protocol.
- (d) Ensuring an appendix is created and attached to this policy that describes requirements for elder and dependent adult abuse investigations consistent with Penal Code § 368.6(c)(8)(B).
- (e) Ensuring a detailed checklist is created and attached to this policy regarding first responding responsibilities that includes but is not limited to the requirements of Penal Code § 368.6(c)(23).
- (f) Ensuring that all members carry out their responsibilities under this policy.
- (g) Verifying a process is in place for transmitting and periodically retransmitting this policy and related orders to investigators, including a simple and immediate way for investigators to access the policy in the field when needed.
- (h) Ensuring this policy is available to the Protection and Advocacy Agency upon request.

#### **426.15 ELDER AND DEPENDENT ADULT ABUSE LIAISON**

The Special Victims Unit (SVU) investigator will serve as the Elder and Dependent Adult Abuse Liaison. Responsibilities of the liaison include but are not limited to (Penal Code § 368.6):

- (a) Acting as a liaison to other responsible agencies (defined by Penal Code § 368.6(b)(15)) to increase cooperation and collaboration among them while retaining the law enforcement agency's exclusive responsibility for criminal investigations (Welfare and Institutions Code § 15650).
- (b) Reaching out to the senior and disability communities and to the public to encourage prevention and reporting of senior and disability victimization.

## Eyewitness Identification

### 427.1 PURPOSE AND SCOPE

This policy sets forth guidelines to be used when members of this bureau employ eyewitness identification techniques (Penal Code § 859.7).

#### 427.1.1 DEFINITIONS

Definitions related to the policy include:

**Eyewitness identification process** - Any field identification, live lineup or photographic identification.

**Field identification** - A live presentation of a single individual to a witness following the commission of a criminal offense for the purpose of identifying or eliminating the person as the suspect.

**Live lineup** - A live presentation of individuals to a witness for the purpose of identifying or eliminating an individual as the suspect.

**Photographic lineup** - Presentation of photographs to a witness for the purpose of identifying or eliminating an individual as the suspect.

### 427.2 POLICY

The Stanislaus County District Attorney's Office will strive to use eyewitness identification techniques, when appropriate, to enhance the investigative process and will emphasize identifying persons responsible for crime and exonerating the innocent.

### 427.3 INTERPRETIVE SERVICES

Members should make a reasonable effort to arrange for an interpreter before proceeding with eyewitness identification if communication with a witness is impeded due to language or hearing barriers.

Before the interpreter is permitted to discuss any matter with the witness, the investigating member should explain the identification process to the interpreter. Once it is determined that the interpreter comprehends the process and can explain it to the witness, the eyewitness identification may proceed as provided for within this policy.

### 427.4 EYEWITNESS IDENTIFICATION PROCESS AND FORM

The Investigative Bureau supervisors shall be responsible for the development and maintenance of an eyewitness identification process for use by members when they are conducting eyewitness identifications.

The process should include appropriate forms or reports that provide (Penal Code § 859.7):

- (a) The date, time and location of the eyewitness identification procedure.
- (b) The name and identifying information of the witness.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Eyewitness Identification*

---

- (c) The name of the person administering the identification procedure.
- (d) If applicable, the names of all of the individuals present during the identification procedure.
- (e) An instruction to the witness that it is as important to exclude innocent persons as it is to identify a perpetrator.
- (f) An instruction to the witness that the perpetrator may or may not be among those presented and that the witness is not obligated to make an identification.
- (g) If the identification process is a photographic or live lineup, an instruction to the witness that the perpetrator may not appear exactly as he/she did on the date of the incident.
- (h) An instruction to the witness that the investigation will continue regardless of whether an identification is made by the witness.
- (i) A signature line where the witness acknowledges that he/she understands the identification procedures and instructions.
- (j) A statement from the witness in the witness's own words describing how certain he/she is of the identification or non-identification. This statement should be taken at the time of the identification procedure.
- (k) Any other direction to meet the requirements of Penal Code § 859.7, including direction regarding blind or blinded administrations and filler selection.

The process and related forms should be reviewed at least annually and modified when necessary.

#### **427.5 EYEWITNESS IDENTIFICATION**

Members are cautioned not to, in any way, influence a witness as to whether any subject or photo presented in a lineup is in any way connected to the case.

Members should avoid mentioning that:

- The individual was apprehended near the crime scene.
- The evidence points to the individual as the suspect.
- Other witnesses have identified or failed to identify the individual as the suspect.

In order to avoid undue influence, witnesses should view suspects or a lineup individually and outside the presence of other witnesses. Witnesses should be instructed to avoid discussing details of the incident or of the identification process with other witnesses.

The eyewitness identification procedure should be audio and video recorded and the recording should be retained according to current evidence procedures. When it is not feasible to make a recording with both audio and visual representations, an audio recording should be made (Penal Code § 859.7).

#### **427.6 FIELD IDENTIFICATION CONSIDERATIONS**

Field identifications, also known as field elimination show-ups or one-on-one identifications, may be helpful in certain cases, where exigent circumstances make it impracticable to conduct a photo



### *Eyewitness Identification*

---

or live lineup identifications. A field elimination show-up or one-on-one identification should not be used when independent probable cause exists to arrest a suspect. In such cases a live or photo lineup is the preferred course of action if eyewitness identification is contemplated.

When initiating a field identification, the member should observe the following guidelines:

- (a) Obtain a complete description of the suspect from the witness.
- (b) Assess whether a witness should be included in a field identification process by considering:
  - 1. The length of time the witness observed the suspect.
  - 2. The distance between the witness and the suspect.
  - 3. Whether the witness could view the suspect's face.
  - 4. The quality of the lighting when the suspect was observed by the witness.
  - 5. Whether there were distracting noises or activity during the observation.
  - 6. Any other circumstances affecting the witness's opportunity to observe the suspect.
  - 7. The length of time that has elapsed since the witness observed the suspect.
- (c) If safe and practicable, the person who is the subject of the show-up should not be handcuffed or in a patrol vehicle.
- (d) When feasible, members should bring the witness to the location of the subject of the show-up, rather than bring the subject of the show-up to the witness.
- (e) The person who is the subject of the show-up should not be shown to the same witness more than once.
- (f) In cases involving multiple suspects, witnesses should only be permitted to view the subjects of the show-up one at a time.
- (g) The person who is the subject of the show-up should not be required to put on clothing worn by the suspect, to speak words uttered by the suspect or to perform other actions mimicking those of the suspect.
- (h) If a witness positively identifies a subject of the show-up as the suspect, members should not conduct any further field identifications with other witnesses for that suspect. In such instances members should document the contact information for any additional witnesses for follow up, if necessary.

#### **427.7 DOCUMENTATION**

A thorough description of the eyewitness process and the result of any eyewitness identification should be documented in the case report.

If a photographic lineup is utilized, a copy of the photographic lineup presented to the witness should be included in the case report. In addition, the order in which the photographs were presented to the witness should be documented in the case report.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Eyewitness Identification*

---

#### 427.7.1 DOCUMENTATION RELATED TO RECORDINGS

The handling member shall document the reason that a video recording or any other recording of an identification was not obtained (Penal Code § 859.7).

#### 427.7.2 DOCUMENTATION RELATED TO BLIND ADMINISTRATION

If a presentation of a lineup is not conducted using blind administration, the handling member shall document the reason (Penal Code § 859.7).

#### **427.8 PHOTOGRAPHIC LINEUP AND LIVE LINEUP CONSIDERATIONS**

When practicable, the member presenting the lineup should not be involved in the investigation of the case or know the identity of the suspect. In no case should the member presenting a lineup to a witness know which photograph or person in the lineup is being viewed by the witness (Penal Code § 859.7). Techniques to achieve this include randomly numbering photographs, shuffling folders, or using a computer program to order the persons in the lineup.

Individuals in the lineup should reasonably match the description of the perpetrator provided by the witness and should bear similar characteristics to avoid causing any person to unreasonably stand out. In cases involving multiple suspects, a separate lineup should be conducted for each suspect. The suspects should be placed in a different order within each lineup (Penal Code § 859.7).

The member presenting the lineup should do so sequentially (i.e., show the witness one person at a time) and not simultaneously. The witness should view all persons in the lineup.

A live lineup should only be used before criminal proceedings have been initiated against the suspect. If there is any question as to whether any criminal proceedings have begun, the investigating member should contact the appropriate prosecuting attorney before proceeding.

#### 427.8.1 OTHER SAFEGUARDS

Witnesses should be asked for suspect descriptions as close in time to the incident as possible and before conducting an eyewitness identification. No information concerning a suspect should be given prior to obtaining a statement from the witness describing how certain he/she is of the identification or non-identification. Members should not say anything to a witness that may validate or invalidate an eyewitness' identification. In photographic lineups, writings or information concerning any previous arrest of a suspect shall not be visible to the witness (Penal Code § 859.7).

#### **427.9 EYEWITNESS IDENTIFICATION FORMS**

[See attachment: Photo Lineup Advisement.pdf](#)

[See attachment: Live Line Up and In Field Show Up Advisement Form.pdf](#)

## Brady Material Disclosure

### 428.1 PURPOSE AND SCOPE

This policy establishes guidelines for the Stanislaus District Attorney's (SCDA) Bureau of Investigation (BI) when identifying and releasing potentially exculpatory or impeachment information (so-called "*Brady* information") to a prosecuting attorney.

#### 428.1.1 DEFINITIONS

Definitions related to this policy include:

***Brady* information** -Information known or possessed by the BI that is both favorable and material to the current prosecution or defense of a criminal defendant.

### 428.2 POLICY

The BI will conduct fair and impartial criminal investigations and will provide the prosecution with both incriminating and exculpatory evidence, as well as information that may adversely affect the credibility of a witness. In addition to reporting all evidence of guilt, the BI will assist the prosecution by complying with its obligation to disclose information that is both favorable and material to the defense. The BI will identify and disclose to the prosecution potentially exculpatory information, as provided in this policy.

### 428.3 DISCLOSURE OF INVESTIGATIVE INFORMATION

Investigators must include in their investigative reports adequate investigative information and reference to all material evidence and facts that are reasonably believed to be either incriminating or exculpatory to any individual in the case. If an investigator learns of potentially incriminating or exculpatory information any time after submission of a case, the investigator or the handling investigator must prepare and submit a supplemental report documenting such information as soon as practicable. Supplemental reports shall be promptly processed and transmitted to the prosecutor's office.

If information is believed to be privileged or confidential (e.g., confidential informant or attorney-client information, attorney work product), the investigator should discuss the matter with a supervisor and/or prosecutor to determine the appropriate manner in which to proceed.

Evidence or facts are considered material if there is a reasonable probability that they would affect the outcome of a criminal proceeding or trial. Determining whether evidence or facts are material often requires legal or even judicial review. If an investigator is unsure whether evidence or facts are material, the investigator should address the issue with a supervisor.

Supervisors who are uncertain about whether evidence or facts are material should address the issue in a written memo to an appropriate prosecutor. A copy of the memo should be retained in the Bureau case file.

### *Brady Material Disclosure*

---

#### **428.4 DISCLOSURE OF PERSONNEL INFORMATION**

Whenever it is determined that *Brady* information is located in the personnel file of a member of the BI who is a material witness in a criminal case, the following procedure shall apply:

- (a) In the event that a *Pitchess* motion has not already been filed by the criminal defendant or other party pursuant to Evidence Code § 1043, the prosecuting attorney shall be notified of the potential presence of *Brady* information in the investigator's personnel file.
- (b) The prosecuting attorney should then be requested to file a *Pitchess* motion in order to initiate an in-camera review by the court.
- (c) Any member who is the subject of such a motion shall be notified in writing that a motion has been filed.
- (d) The Custodian of Records shall accompany all relevant files during any in-camera inspection and address any issues or questions raised by the court in determining whether any information contained in the files is both material and favorable to the criminal defendant.
- (e) If the court determines that there is relevant *Brady* information contained in the files, only that information ordered released will be copied and released to the parties filing the motion.
  1. Prior to the release of any information pursuant to this process, the Custodian of Records should request a protective order from the court limiting the use of such information to the involved case and requiring the return of all copies upon completion of the case.

#### **428.5 INVESTIGATING BRADY ISSUES**

If the BI receives information from any source that a member may have issues of credibility, dishonesty or has been engaged in an act of moral turpitude or criminal conduct, the information shall be investigated and processed in accordance with the Personnel Complaints Policy.

#### **428.6 TRAINING**

BI members should receive periodic training on the requirements of this policy.

## Public Alerts

### 429.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for alerting the public to important information and soliciting public aid when appropriate.

### 429.2 POLICY

Public alerts may be employed using the Emergency Alert System (EAS), local radio, television and press organizations and other groups to notify the public of incidents, or enlist the aid of the public, when the exchange of information may enhance the safety of the community. Various types of alerts may be available based upon each situation and the alert system's individual criteria.

### 429.3 RESPONSIBILITIES

#### 429.3.1 MEMBER RESPONSIBILITIES

Members of the Stanislaus County District Attorney's Office should notify their supervisor, Lieutenant, or Investigative Bureau Supervisor as soon as practicable upon learning of a situation where public notification, a warning, or enlisting the help of the media and public could assist in locating a missing person, apprehending a dangerous person, or gathering information.

#### 429.3.2 SUPERVISOR RESPONSIBILITIES

A supervisor apprised of the need for a public alert is responsible to make the appropriate notifications based upon the circumstances of each situation. The supervisor shall promptly notify the Chief of Investigations, the appropriate Lieutenant and the Public Information Officer when any public alert is generated.

The supervisor in charge of the investigation to which the alert relates is responsible for the following:

- (a) Updating alerts
- (b) Canceling alerts
- (c) Ensuring all appropriate reports are completed
- (d) Preparing an after-action evaluation of the investigation to be forwarded to the Lieutenant

### 429.4 AMBER ALERTS

The AMBER Alert™ Program is a voluntary partnership between law enforcement agencies, broadcasters, transportation agencies and the wireless industry, to activate urgent bulletins in child abduction cases.

#### 429.4.1 CRITERIA FOR AMBER ALERT

The following conditions must be met before activating an AMBER Alert (Government Code § 8594(a)):

# Stanislaus County District Attorney's Office

## Policy Manual

### *Public Alerts*

---

- (a) A child has been abducted or taken by anyone, including but not limited to a custodial parent or guardian.
- (b) The victim is 17 years of age or younger, or has a proven mental or physical disability.
- (c) The victim is in imminent danger of serious injury or death.
- (d) There is information available that, if provided to the public, could assist in the child's safe recovery.

#### **429.4.2 PROCEDURE FOR AMBER ALERT**

The supervisor in charge will ensure the following:

- (a) An initial press release is prepared that includes all available information that might aid in locating the child:
  - 1. The child's identity, age and description
  - 2. Photograph if available
  - 3. The suspect's identity, age and description, if known
  - 4. Pertinent vehicle description
  - 5. Detail regarding location of incident, direction of travel, potential destinations, if known
  - 6. Name and telephone number of the Public Information Officer or other authorized individual to handle media liaison
  - 7. A telephone number for the public to call with leads or information
- (b) The local California Highway Patrol communications center should be contacted to initiate a multi-regional or statewide EAS broadcast, following any policies and procedures developed by CHP (Government Code § 8594).
- (c) The press release information is forwarded to the Sheriff's Department Emergency Communications Bureau so that general broadcasts can be made to local law enforcement agencies.
- (d) Information regarding the missing person should be entered into the California Law Enforcement Telecommunication System (CLETS).
- (e) Information regarding the missing person should be entered into the California Department of Justice Missing and Unidentified Persons System (MUPS)/National Crime Information Center (NCIC).
- (f) The following resources should be considered as circumstances dictate:
  - 1. The local FBI office
  - 2. National Center for Missing and Exploited Children (NCMEC)

#### **429.5 BLUE ALERTS**

Blue Alerts may be issued when an investigator is killed, injured or assaulted and the suspect may pose a threat to the public or other law enforcement personnel.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Public Alerts*

---

#### **429.5.1 CRITERIA FOR BLUE ALERTS**

All of the following conditions must be met before activating a Blue Alert (Government Code § 8594.5):

- (a) A law enforcement officer has been killed, suffered serious bodily injury or has been assaulted with a deadly weapon, and the suspect has fled the scene of the offense.
- (b) The investigating law enforcement agency has determined that the suspect poses an imminent threat to the public or other law enforcement personnel.
- (c) A detailed description of the suspect's vehicle or license plate is available for broadcast.
- (d) Public dissemination of available information may help avert further harm or accelerate apprehension of the suspect.

#### **429.5.2 PROCEDURE FOR BLUE ALERT**

The supervisor in charge should ensure the following:

- (a) An initial press release is prepared that includes all available information that might aid in locating the suspect:
  - 1. The license number and/or any other available description or photograph of the vehicle
  - 2. Photograph, description and/or identification of the suspect
  - 3. The suspect's identity, age and description, if known
  - 4. Detail regarding location of incident, direction of travel, potential destinations, if known
  - 5. Name and telephone number of the Public Information Officer or other authorized individual to handle media liaison
  - 6. A telephone number for the public to call with leads or information
- (b) The local California Highway Patrol communications center is contacted to initiate a multi-regional or statewide EAS broadcast.
- (c) The information in the press release is forwarded to the Sheriff's Department Emergency Communications Bureau so that general broadcasts can be made to local law enforcement agencies.
- (d) The following resources should be considered as circumstances dictate:
  - 1. Entry into the California Law Enforcement Telecommunication System (CLETS)
  - 2. The FBI local office

#### **429.6 SILVER ALERTS**

Silver Alerts® is an emergency notification system for people who are 65 years of age or older, developmentally disabled or cognitively impaired and have been reported missing (Government Code § 8594.10).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Public Alerts*

---

#### 429.6.1 CRITERIA FOR SILVER ALERTS

All of the following conditions must be met before activating a Silver Alert (Government Code § 8594.10):

- (a) The missing person is 65 years of age or older, developmentally disabled or cognitively impaired.
- (b) The bureau has utilized all available local resources.
- (c) The investigating investigator or supervisor has determined that the person is missing under unexplained or suspicious circumstances.
- (d) The investigating investigator or supervisor believes that the person is in danger because of age, health, mental or physical disability, environment or weather conditions, that the person is in the company of a potentially dangerous person, or that there are other factors indicating that the person may be in peril.
- (e) There is information available that, if disseminated to the public, could assist in the safe recovery of the missing person.

#### 429.6.2 PROCEDURE FOR SILVER ALERT

Requests for a Silver Alert shall be made through the California Highway Patrol (Government Code § 8594.10).

### **429.7 ADDITIONAL ALERTS FOR PUBLIC SAFETY EMERGENCIES**

Additional public safety emergency alerts may be authorized that utilize wireless emergency alert system (WEA) and emergency alert system (EAS) equipment for alerting and warning the public to protect lives and save property (Government Code § 8593.7).

#### 429.7.1 CRITERIA

Public safety emergency alerts may be issued to alert or warn the public about events including but not limited to:

- (a) Evacuation orders (including evacuation routes, shelter information, key information).
- (b) Shelter-in-place guidance due to severe weather.
- (c) Terrorist threats.
- (d) HazMat incidents.

#### 429.7.2 PROCEDURE

Public safety emergency alerts should be activated by following the guidelines issued by the Office of Emergency Services (Government Code § 8593.7).

### **429.8 YELLOW ALERT**

A Yellow Alert may be issued when a person is killed due to a hit-and-run incident and the bureau has specified information concerning the suspect or the suspect's vehicle (Government Code § 8594.15).



# Stanislaus County District Attorney's Office

## Policy Manual

### *Public Alerts*

---

#### 429.8.1 CRITERIA FOR YELLOW ALERT

All of the following conditions must be met before activating a Yellow Alert (Government Code § 8594.15):

- (a) A person has been killed due to a hit-and-run incident.
- (b) There is an indication that a suspect has fled the scene utilizing the state highway system or is likely to be observed by the public on the state highway system.
- (c) The bureau has additional information concerning the suspect or the suspect's vehicle including but not limited to the following:
  - 1. The complete license plate number of the suspect's vehicle.
  - 2. A partial license plate number and additional unique identifying characteristics, such as the make, model, and color of the suspect's vehicle, which could reasonably lead to the apprehension of a suspect.
  - 3. The identity of a suspect.
  - 4. Public dissemination of available information could either help avert further harm or accelerate apprehension of a suspect based on any factor, including but not limited to the time elapsed between a hit-and-run incident and the request or the likelihood that an activation would reasonably lead to the apprehension of a suspect.

#### 429.8.2 PROCEDURE FOR YELLOW ALERT

Requests for a Yellow Alert shall be made through the California Highway Patrol (Government Code § 8594.15).

#### **429.9 FEATHER ALERT**

A Feather Alert may be issued when an Indigenous person is reported missing. The determination that criteria has been met for the alert shall be made within 24 hours following the initial report being made to the Bureau (Government Code § 8594.13).

#### 429.9.1 CRITERIA FOR FEATHER ALERT

The Bureau may request that a Feather Alert be activated if it is determined that the alert would be an effective tool in the investigation of missing and murdered Indigenous persons, including young women or girls. The following factors shall be considered to make that determination (Government Code § 8594.13):

- (a) The missing person is an Indigenous person.
- (b) The Bureau has utilized local and tribal resources.
- (c) The investigating investigator has determined the person is missing.
- (d) The investigating investigator or supervisor believes that the person is in danger and missing under circumstances that indicate any of the following:
  - 1. The missing person's physical safety may be endangered.
  - 2. The missing person may be subject to trafficking.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Public Alerts*

---

3. The missing person suffers from a mental or physical disability, or substance use disorder.
- (e) There is information available that, if disseminated to the public, could assist in the safe recovery of the missing person.

#### 429.9.2 PROCEDURE FOR FEATHER ALERT

Requests for a Feather Alert shall be made through the California Highway Patrol (Government Code § 8594.13).

#### **429.10 ENDANGERED MISSING ADVISORY**

An Endangered Missing Advisory may be requested when a person is reported missing who is developmentally disabled, or cognitively impaired, or has been abducted, or is unable to otherwise care for themselves, placing their physical safety at risk (Government Code § 8594.11).

##### 429.10.1 CRITERIA FOR ENDANGERED MISSING ADVISORY

All of the following conditions must be met before activating an Endangered Missing Advisory (Government Code § 8594.11):

- (a) The missing person is developmentally disabled, cognitively impaired, has been abducted or is otherwise unable to care for themselves, placing their physical safety at risk.
- (b) The Bureau has utilized all available local resources.
- (c) The investigating investigator has determined the person has gone missing under unexplained or suspicious circumstances.
- (d) The investigating investigator or supervisor believes that the person is in danger because of age, health, mental or physical disability, environment or weather conditions, that the person is in the company of a potentially dangerous person, or that there are other factors indicating that the person may be in peril.
- (e) There is information available that, if disseminated to the public, could assist in the safe recovery of the missing person.

##### 429.10.2 PROCEDURE FOR ENDANGERED MISSING ADVISORIES

Requests for an endangered missing advisory shall be made through the California Highway Patrol (Government Code § 8594.11).

#### **429.11 EBONY ALERT**

An Ebony Alert may be requested when it is determined the alert would be an effective tool in the investigation of missing Black youth, including a young woman or girl (Government Code § 8594.14).

##### 429.11.1 CRITERIA FOR EBONY ALERT

The investigating investigator may consider the following factors to make the determination that an Ebony Alert would be an effective tool (Government Code § 8594.14):

# Stanislaus County District Attorney's Office

## Policy Manual

### *Public Alerts*

---

- (a) The missing person is between the ages of 12 and 25 years old, inclusive.
- (b) The missing person is missing under circumstances that indicate their physical safety is endangered or they have been subject to trafficking.
- (c) The missing person suffers from a mental or physical disability.
- (d) Determination that the person has gone missing under unexplained or suspicious circumstances.
- (e) Belief that the person is in danger because of age, health, mental or physical disability, environment or weather conditions, that the person is in the company of a potentially dangerous person, or that there are other factors indicating that the person may be in peril.
- (f) The Bureau has utilized all available local resources.
- (g) There is information available that, if disseminated to the public, could assist in the safe recovery of the missing person.

#### **429.11.2 PROCEDURE FOR EBONY ALERT**

Requests for an Ebony Alert shall be made through the California Highway Patrol (Government Code § 8594.14).

#### **429.12 LANGUAGE REQUIREMENTS FOR PUBLIC EMERGENCIES**

In the event of an emergency, as defined in Government Code § 7299.7, the Stanislaus County District Attorney's Office shall provide information to the public relating to the emergency in all languages jointly spoken by the local population as provided in Government Code § 7299.7.

# Unmanned Aerial System

## 430.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of an unmanned aerial system (UAS) and for the storage, retrieval and dissemination of images and data captured by the UAS.

### 430.1.1 DEFINITIONS

Definitions related to this policy include:

**Unmanned aerial system (UAS)** - An unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV)), and all of the supporting or attached systems designed for gathering information through imaging, recording or any other means.

## 430.2 POLICY

Unmanned aerial systems may be utilized to enhance the bureau's mission of protecting lives and property when other means and resources are not available or are less effective. In addition, UAS systems are an advanced technique for capturing, recording, and documenting crime scenes that can later be used for evidentiary purposes. Any use of a UAS will be in strict accordance with constitutional and privacy rights and Federal Aviation Administration (FAA) regulations.

## 430.3 PRIVACY

The use of the UAS potentially involves privacy considerations. Absent a warrant or exigent circumstances, operators and observers shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure). Operators and observers shall take reasonable precautions to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy. Reasonable precautions can include, for example, deactivating or turning imaging devices away from such areas or persons during UAS operations.

## 430.4 PROGRAM COORDINATOR

The Chief of Investigations will appoint a program coordinator who will be responsible for the management of the UAS program. The program coordinator will ensure that policies and procedures conform to current laws, regulations, and best practices and will have the following additional responsibilities:

- Coordinating the FAA Certificate of Waiver or Authorization (COA) application process and ensuring that the COA is current, and/or coordinating compliance with FAA Part 107 Remote Pilot Certificate, as appropriate for bureau operations.
- Ensuring that all authorized operators and required observers have completed all required FAA and bureau-approved training in the operation, applicable laws, policies, and procedures regarding use of the UAS.
- Developing uniform protocol for submission and evaluation of requests to deploy a UAS, including urgent requests made during ongoing or emerging incidents.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Unmanned Aerial System*

---

Deployment of a UAS shall require written authorization of the Chief of Investigations or the authorized designee, depending on the type of mission.

- Coordinating the completion of the FAA Emergency Operation Request Form in emergency situations, as applicable (e.g., natural disasters, search and rescue, emergency situations to safeguard human life).
- Developing protocol for conducting criminal investigations involving a UAS, including documentation of time spent monitoring a subject.
- Implementing a system for public notification of UAS deployment.
- Developing an operational protocol governing the deployment and operation of a UAS including but not limited to safety oversight, use of visual observers, establishment of lost link procedures, and secure communication with air traffic control facilities.
- Developing a protocol for fully documenting all missions.
- Developing a UAS inspection, maintenance, and record-keeping protocol to ensure continuing airworthiness of a UAS, up to and including its overhaul or life limits.
- Developing protocols to ensure that all data intended to be used as evidence are accessed, maintained, stored, and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, authenticity certificates, and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.
- Developing protocols that ensure retention and purge periods are maintained in accordance with established records retention schedules.
- Facilitating law enforcement access to images and data captured by the UAS.
- Recommending program enhancements, particularly regarding safety and information security.
- Ensuring that established protocols are followed by monitoring and providing periodic reports on the program to the Chief of Investigations.
- Maintaining familiarity with FAA regulatory standards, state laws and regulations, and local ordinances regarding the operations of a UAS.

#### **430.5 USE OF UAS**

Only authorized operators who have completed the required training shall be permitted to operate the UAS.

Use of vision enhancement technology (e.g., thermal and other imaging equipment not generally available to the public) is permissible in viewing areas only where there is no protectable privacy interest or when in compliance with a search warrant or court order. In all other instances, legal counsel should be consulted.

UAS operations should only be conducted consistent with FAA regulations.

*Unmanned Aerial System*

---

**430.6 PROHIBITED USE**

The UAS video surveillance equipment shall not be used:

- To conduct random surveillance activities.
- To target a person based solely on actual or perceived characteristics, such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, economic status, age, cultural group, or disability.
- To harass, intimidate, or discriminate against any individual or group.
- To conduct personal business of any type.

The UAS shall not be weaponized.

**430.7 RETENTION OF UAS DATA**

Data collected by the UAS shall be retained in Evidence.com as provided in the established records retention schedule.

# California Witness Relocation and Assistance Program (Cal-WRAP)

## 431.1 PURPOSE AND SCOPE

CAL-WRAP is a program to provide protection for witnesses in criminal proceedings where CREDIBLE EVIDENCE exists of a SUBSTANTIAL DANGER that a witness (or their family) may suffer intimidation or retaliatory violence for cooperating with the Stanislaus District Attorney's Office. The authorizing department (in Stanislaus County this is the District Attorney's Office) funds these expenditures and requests reimbursement from the California Department of Justice (DOJ).

## 431.2 POLICY

It is the policy of the Bureau of Investigation to assist local law enforcement agencies who are inquiring about or needing to place a witness into Cal-WRAP. A District Attorney Criminal Investigator (DAI) will work with the originating law enforcement officer (LEO) lead investigator to evaluate the necessity as well as determine whether the witness meets the criteria for the program.

## 431.3 CAL-WRAP SERVICES

A number of assistance services are available through this program, but Stanislaus County DA's Office generally only provides the following:

- (a) Temporary lodgings (such as hotel costs)
- (b) Semi-permanent lodgings (such as apartment/house rental and utilities)
- (c) Permanent relocation (one-time costs)
- (d) Food and incidentals (may be ongoing or one-time)
- (e) Relocation costs (such as mileage/gas, public transportation costs, etc.)
- (f) Moving costs (for semi-permanent or permanent relocation)

Other types of services may be provided on a case by case basis and must be approved by the District Attorney in advance of any offers made to witnesses.

Please see the official manual from DOJ for details on types of services possible as well as maximum costs, etc. Please do NOT inform the witness of what services are possible other than the above, and do not inform them of maximum allowable amounts.

At this time DOJ is only approving these requests on a six-month basis.

## 431.4 ROLES AND RESPONSIBILITIES

The lead LEO will work together with a DAI and they will be responsible for all communications with the witness with regards to this program. The Deputy District Attorney (DDA) prosecuting the case may also be involved. The LEO may need to assist the witness in locating temporary or semi-permanent lodgings. The LEO and DAI are responsible for communicating the conditions of the agreement to enter the program.

# Stanislaus County District Attorney's Office

## Policy Manual

### *California Witness Relocation and Assistance Program (Cal-WRAP)*

---

LEO/DAI may also have the responsibility for obtaining necessary receipts and other documents from the witness, landlord, etc., as requested/required by the local Program Coordinator (currently the District Attorney Office's Fiscal Services Manager) and/or the Program.

The LEO/DAI and DDA may have other responsibilities depending upon the case. The District Attorney (or in her absence, the Assistant District Attorney) must approve all requests, either verbally or in writing. Normally the DDA prosecuting the case will discuss the merits of the case with the DA, with or without LE present.

The Program Coordinator will provide checks for expenditures and forward all documents, reimbursement requests, etc., to DOJ. Please note that the Program Coordinator has no communications with the witness and generally none with landlords but may work with hotels/motels for payment via third party authorizations.

#### 431.4.1 STEPS TO FOLLOW FOR SETTING UP A WITNESS

- (a) LEO/DAI determine that there is a credible threat and be able to state specifics.
- (b) Get approval from the District Attorney.
- (c) LEO meets with DAI, DAI Lieutenant overseeing Cal-WRAP, DDA, and Program Coordinator to discuss the case.
- (d) Determine what services can be/should be offered.
- (e) LEO/DAI prepare the "Program Application" (CAL-WRAP-1); the "Expenses Requested" portion should be completed with the assistance of the Program Coordinator. The "Witness Agreement" (CAL-WRAP-2 or a Spanish language version CAL-WRAP-3) must have all the clauses in the agreement initialed by the witness. The completed form must be signed by the witness and whoever is communicating these conditions must also sign. Anyone relocating with the witness over the age of 12 should be made aware of the terms of the "Witness Agreement".
- (f) Program Coordinator sends the application to DOJ for approval.
- (g) If approved by DOJ, LEO and/or DAI will meet with the Program Coordinator to complete any documentation, provide copies of leases...etc., and obtain checks as appropriate.
- (h) DOJ requires a match of 25% for the DA's Office to receive full reimbursement of all expenses. LEO/DAI/DDA must keep track of their time spent relocating/assisting the witness as well as any administrative time spent on the program. These hours must be reported to the Program Coordinator. **This is very important.** Hours/time spent may be communicated via memo, email or other written communication. Once a witness is set up and stable, a set monthly amount of time spent may be determined for the match requirement and reporting may no longer be required unless conditions change. For non-DA personnel, the hourly weighted labor rate must be communicated to the Program Coordinator to calculate the match amount.



# Stanislaus County District Attorney's Office

## Policy Manual

### *California Witness Relocation and Assistance Program (Cal-WRAP)*

---

#### **431.5 SERVICES FUNDED**

If approved by the District Attorney, witnesses and family members will be enrolled into Cal-WRAP with services funded by the California Department of Justice.

##### **431.5.1 ONE-TIME RELOCATION**

Receipts are required for all moving expenses, rent, deposits, etc. In the case of hardship, funds may be provided initially without documentation, but it is the responsibility of the LEO/DAI who initially set up the witness to obtain receipts. Moving expenses (U-Haul, gas, etc.) may also be reimbursed but unless there is significant hardship, this is done as a reimbursement to the witness rather than up-front funding.

##### **431.5.2 TEMPORARY LODGINGS**

The witness may be housed in a hotel/motel for a limited amount of time, usually when there is an imminent threat and prior to finding semi-permanent lodgings (house/apt rental) or a permanent relocation. Most hotels/motels will take a "third party authorization" so that the DA's Office will pay the costs directly. This is done on a county procurement (credit) card; if LEO involved is not DA staff, these costs may be charged to the procurement card assigned to the DDA prosecuting the case, a DAI, or the Program Coordinator. Most hotels will fax a copy of their third-party authorization form which can be completed and returned. ONLY room rate and applicable fees/taxes will be authorized. The LEO/DAI handling the witness is responsible for obtaining the hotel "folio" (detailed invoice); having the hotel email it directly to the Program Coordinator is acceptable, but it is the LEO/DAI's responsibility to see that this is done.

##### **431.5.3 SEMI-PERMANENT LODGINGS**

Rent may be paid on an ongoing basis, or as a one-time payment, for witnesses who are financially unable to do so. Witnesses should be encouraged to obtain employment, so they can take over responsibility for payment. The witness must be able to be approved for a rental/lease agreement on their own merits (or on the merits of a spouse, partner, family member, etc.). First month's rent and deposit will be paid directly to the landlord by the Program Coordinator. Payment directly to the witness may be approved on a case by case basis. Receipt of payment must be obtained and sent to the Program Coordinator. LEO/DAI is responsible for obtaining these receipts. Any refund of deposit must be paid to the DA's Office and not to the witness directly. The DA's Office may send a letter to the landlord notifying of the direct payment from our office and that a 30-day notice will be given when no longer responsible for payment. Moving expenses may be funded as described under "One-time Relocation."

##### **431.5.4 FOOD AND INCIDENTALS**

Funds for food and incidentals may be provided for the witness and approved family members residing with the witness on a one-time or ongoing basis; maximum amounts are listed in the official DOJ manual but wherever possible less than the maximum (especially while in temporary lodgings) should be requested. If the witness is in temporary lodgings which include a kitchen or cooking facilities (as many motels do), the semi-permanent rates are the maximum. Witnesses should be encouraged to obtain employment once their living situation is stabilized so that they

# Stanislaus County District Attorney's Office

## Policy Manual

### *California Witness Relocation and Assistance Program (Cal-WRAP)*

---

may be migrated off dependence on the program. What will be provided, on an on-going basis, for how long, etc. varies from case to case, and should be discussed with the Program Coordinator. Witnesses must understand that these funds are provided for food and incidentals ONLY—no alcohol, cigarettes, illegal drugs, or other uses, are allowed (incidentals include such things as shampoo, diapers, personal hygiene items, etc.). A letter stating funds must be used for food only will be provided with the witness check to be signed by the witness and returned to the Program Coordinator.

#### **431.5.5 UTILITIES**

Reimbursement may be provided for electric, gas, sewer, water and waste pickup only. No cable, telephone, satellite, internet connections, etc., costs will be reimbursed. Reimbursement is after the fact only and receipt of payment by witness is required. Initial deposits for allowed services may also be reimbursed, but the witness must be informed that any refund of deposits must be returned to the DA's Office.

#### **431.6 DOCUMENTATION**

The official DOJ manual should be reviewed for appropriate actions and costs. However, whenever possible, one-time relocations and assistance are preferable to on-going support and will be determined on a case by case basis.

Form CAL-WRAP-9 Questionnaire must be completed when the witness is terminated from the program. Forms in the official DOJ manual, other than the ones already noted, are generally used by the DA's Office.

Whenever possible, all documentation and necessary program forms should be completed prior to the first expenditures. However, this is sometimes impractical and there may be an immediate and serious threat; under these circumstances, a verbal approval to move the witness into temporary lodgings immediately may be appropriate and allowable.

Several of the Criminal Investigators in the District Attorney's office have experience with the program, and it is suggested that other LE consult with them and utilize their experiences handling protected witnesses and dealing with the CAL-WRAP program.

The following are the typical forms used by the LEO/DAI/Program Coordinator:

- (a) CALWRAP-1 Application
- (b) CALWRAP-2 Witness Agreement
- (c) CALWRAP-3 Witness Agreement Spanish
- (d) CALWRAP-4 List of Expenditures
- (e) CALWRAP-5 25% Match Requirement
- (f) CALWRAP-6 Amendment Request
- (g) CALWRAP-8 Opt Out Form
- (h) CALWRAP-9 Questionnaire

# Stanislaus County District Attorney's Office

## Policy Manual

### *California Witness Relocation and Assistance Program (Cal-WRAP)*

---

#### **431.7 PROGRAM COORDINATOR - DAI LIEUTENANT**

Lori Denego, Fiscal Services Manager

Office (209) 525-5505 Cell (209) 996-0610

Froilan Mariscal, Lieutenant

Office (209) 525-6941 Cell (209) 652-1277

# Restoration of Rights and Application for Pardon Investigations

## 432.1 PURPOSE AND SCOPE

In 2018, Governor Edmund "Jerry" Brown signed into law Assembly Bill 2845 which is known as the Pardon and Commutation Reform Act of 2018. The bill allowed for persons convicted of a felony who were committed to a state prison or other institution or agency, including a commitment to a county jail, to file a petition for certificate of rehabilitation and pardon pursuant to the provisions of Penal Code §§ 4852.01 - 4852.22.

Penal Code § 4852.12 states:

(a) In a proceeding for the ascertainment and declaration of the fact of rehabilitation under this chapter, the court, upon the filing of the application for petition of rehabilitation, may request from the district attorney an investigation of the residence of the petitioner, the criminal record of the petitioner as shown by the records of the Department of Justice, any representation made to the court by the applicant, the conduct of the petitioner during the period of rehabilitation, including all matters mentioned in Section 4852.11, and any other information the court deems necessary in making its determination. The district attorney shall, upon request of the court, provide the court with a full and complete report of the investigations.

(b) In any proceeding for the ascertainment and declaration of the fact of rehabilitation under this chapter of a person convicted of a crime the accusatory pleading of which has been dismissed pursuant to Section 1203.4, the district attorney, upon request of the court, shall deliver to the court the criminal record of petitioner as shown by the records of the Department of Justice. The district attorney may investigate any representation made to the court by petitioner and may file with the court a report of the investigation including all matters known to the district attorney relating to the conduct of the petitioner, the place and duration of residence of the petitioner during the period of rehabilitation, and all known violations of law committed by the petitioner.

## 432.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office, that either upon request of the court or at the District Attorney's discretion (or by one of her designees) that after the filing of the application for petition of rehabilitation, the Bureau of Investigation (BI) will conduct an investigation into the petitioners conduct and prepare a written report outlining the investigation pursuant to Penal Code §§ 4852.11 and 4852.12.

It is the intent of the People of the State of California that the person shall live an honest and upright life, shall conduct himself or herself with sobriety and industry, shall exhibit a good moral character, and shall conform to and obey the laws of the land. Penal Code § 4852.05

## 432.3 INITIAL INVESTIGATION

Upon notification of an application for petition for rehabilitation and pardon, a BI Lieutenant will assign an Investigator to conduct a thorough review of the petitioner's conduct that resulted

# Stanislaus County District Attorney's Office

## Policy Manual

### *Restoration of Rights and Application for Pardon Investigations*

---

in a felony conviction as well as their conduct after release from custody to parole and/or probation and thereafter. The HUB will prepare the file and send a questionnaire to the petitioner or if represented to the petitioners attorney. [See attachment: Questionnaire from LA Cty Certificate Rehab and Pardon Packet.pdf](#)

#### **432.3.1 INVESTIGATOR RESPONSIBILITIES**

Investigators responsible for investigating petitions for rehabilitation and pardon shall examine the following: Penal Code §§ 4852.11 and 4852.12

- (a) All known violations of law committed by the petitioner after release from custody.
- (b) The petitioners established place of residence or residences.
- (c) The complete criminal record of the petitioner.
- (d) Any representation made to the court by the petitioner
- (e) The conduct of the petitioner during period of rehabilitation.
- (f) Any other information the court deems necessary in making its determination.

#### **432.3.2 FULL AND COMPLETE REPORT OF INVESTIGATION**

Investigators will complete an investigative report outlining the findings of their investigation to include interviews of persons known to the petitioner, information obtained from official documents and information obtained from social media accounts.

#### **432.4 SUPERVISOR REVIEW AND APPROVAL**

At the conclusion of the investigation, a BI supervisor will conduct a review of the investigation and upon final approval will provide the investigative report to the Deputy District Attorney assigned.

## **Chapter 5 - Equipment**

## Bureau Owned and Personal Property

### 500.1 PURPOSE AND SCOPE

Bureau employees are expected to properly care for bureau property assigned or entrusted to them. Employees may also suffer occasional loss or damage to personal or bureau property while performing their assigned duty. Certain procedures are required depending on the loss and ownership of the item.

### 500.2 CARE OF BUREAU PROPERTY

Employees shall be responsible for the safekeeping, serviceable condition, proper care, use and replacement of bureau property assigned or entrusted to them. An employee's intentional or negligent abuse or misuse of bureau property may lead to discipline including, but not limited to the cost of repair or replacement.

- (a) Employees shall promptly report through their chain of command, any loss, damage to, or unserviceable condition of any bureau issued property or equipment assigned for their use.
- (b) The use of damaged or unserviceable bureau property should be discontinued as soon as practical and replaced with comparable Bureau property as soon as available and following notice to a supervisor.
- (c) Except when otherwise directed by competent authority or required by exigent circumstances, bureau property shall only be used by those to whom it was assigned. Use should be limited to official purposes and in the capacity for which it was designed.
- (d) Bureau property shall not be thrown away, sold, traded, donated, destroyed, or otherwise disposed of without proper authority.
- (e) In the event that any Bureau property becomes damaged or unserviceable, no employee shall attempt to repair the property without prior approval of a supervisor.

### 500.3 FILING CLAIMS FOR PERSONAL PROPERTY

Claims for reimbursement for damage or loss of personal property must be made on the proper form. Bureau employees who damage or lose issued equipment shall outline the circumstances in a memorandum. This memorandum is submitted to the employee's immediate supervisor. The supervisor, depending on the circumstances, may require a separate written report of the loss or damage.

The supervisor shall direct the memorandum to the Chief Investigator, which shall include the results of his/her investigation and whether the employee followed proper procedures. The supervisor's report shall address whether reasonable care was taken to prevent the loss or damage.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Bureau Owned and Personal Property*

---

Upon review by staff and a finding that no misconduct or negligence was involved, repair or replacement may be recommended by the Chief of Investigations who will then forward the claim to the Finance Department for replacement.

The Bureau will not replace or repair luxurious or overly expensive items (jewelry, exotic equipment, etc.) that are not reasonably required as a part of work.

#### **500.4 LOSS OR DAMAGE OF PROPERTY OF ANOTHER**

Investigators and other employees intentionally or unintentionally may cause damage to the real or personal property of another while performing their duties. Any employee who damages or causes to be damaged any real or personal property of another while performing any law enforcement functions, regardless of jurisdiction, shall report it as provided below.

- (a) A verbal report shall be made to the employee's immediate supervisor as soon as circumstances permit.
- (b) A written report shall be submitted before the employee goes off duty or within the time frame directed by the supervisor to whom the verbal report is made.

##### **500.4.1 DAMAGE BY PERSON OF ANOTHER AGENCY**

If employees of another jurisdiction cause damage to real or personal property belonging to the County, it shall be the responsibility of the employee present or the employee responsible for the property to make a verbal report to his/her immediate supervisor as soon as circumstances permit. The employee shall submit a written report before going off duty or as otherwise directed by the supervisor.

These written reports, accompanied by the supervisor's written report, shall promptly be forwarded to the Chief Investigator.



## Personal Communication Devices

### 501.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of mobile telephones and communication devices, whether issued or funded by the Office or personally owned, while on-duty or when used for authorized work-related purposes.

This policy generically refers to all such devices as Personal Electronic Devices (PEDs) but is intended to include all mobile telephones, personal digital assistants (PDAs), wireless capable tablets, computers and similar wireless two-way communications and/or portable Internet access devices. PCD use includes, but is not limited to, placing and receiving calls, text messaging, blogging and microblogging, emailing, using video or camera features, playing games and accessing sites or services on the Internet.

### 501.2 POLICY

The Stanislaus District Attorney's Office allows members to utilize Office-issued or funded PCDs and to possess personally owned PCDs in the workplace, subject to certain limitations. Any PCD used in any manner reasonably related to the business of the Office, will be subject to inspection and monitoring by the Office IT Unit consistent with the standards set forth in this policy.

Additionally, members are advised and cautioned that the use of a personally owned PCD either on-duty or after duty hours for business-related purposes may subject the member and the member's PCD records to civil or criminal discovery or disclosure under applicable public records laws.

Members who have questions regarding the application of this policy or the guidelines contained herein are encouraged to seek clarification from their immediate supervisor.

### 501.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to any communication accessed, transmitted, received or reviewed on any PCD issued or funded by the Office and shall have no expectation of privacy in their location should the device be equipped with location detection capabilities.

#### 501.3.1 CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT (CALECPA)

No member is authorized to be the sole possessor of a Office-issued PCD. Office-issued PCDs can be retrieved, reassigned, accessed or used by any member as directed by a supervisor without notice. Member use of a Office-issued PCD and use of a personal PCD at work or for work-related business constitutes specific consent for access for Office purposes. Prior to conducting an administrative search of a PCD, supervisors should consult legal counsel to ensure access is consistent with CalECPA (Penal Code § 1546; Penal Code § 1546.1).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personal Communication Devices*

---

#### **501.4 BUREAU-ISSUED PCD**

Depending on a member's assignment and the needs of the position, the Office may, at its discretion, issue or fund a PCD. Office-issued or funded PCDs are provided as a convenience to facilitate work performance only. Such devices and the associated telephone number shall remain the sole property of the Office and shall be subject to inspection or monitoring (including all related records and content) at any time without notice and without cause.

#### **501.5 PERSONALLY OWNED PCD**

Members may carry a personally owned PCD while on-duty, subject to the following conditions and limitations:

- (a) Permission to carry a personally owned PCD on-duty may be revoked if it is used contrary to provisions of this policy.
- (b) The Office accepts no responsibility for loss of or damage to a personally owned PCD.
- (c) The PCD and any associated services shall be purchased, used and maintained solely at the member's expense.
- (d) Unless approved by your supervisor/manager, personally owned PCD's shall not be used for work-related purposes except in circumstances where issued PCD's are not functioning (e.g., no service, dead battery) and there is a necessity to communicate with another member of this office. Members will have a reduced expectation of privacy when using a personally owned PCD in the workplace and have no expectation of privacy with regard to any Office business-related communication.
- (e) Work related software shall not be loaded onto a personally owned PCD.
- (f) Unless approved by your supervisor/manager, the device shall not be utilized to record or disclose any business-related information, including photographs, video or the recording or transmittal of any information or material obtained or made accessible as a result of employment with the Office.
- (g) Use of a personally owned PCD for work-related business constitutes consent for the Office to access the PCD to inspect and copy data to meet the needs of the Office, which may include litigation, public records retention and release obligations and internal investigations.
- (h) If the use of a personally owned PCD for work-related business is approved by your supervisor/manager, all work-related documents, emails, photographs, recordings or other public records created or received on a member's personally owned PCD shall be transferred to the Stanislaus County District Attorney's Office network and deleted from the member's PCD as soon as reasonably practicable.

#### **501.6 SUPERVISOR RESPONSIBILITIES**

The responsibilities of supervisors include, but are not limited to:

- (a) Ensuring that members under their command are provided appropriate training on the use of PCDs consistent with this policy.
- (b) Monitoring, to the extent practicable, PCD use in the workplace and taking prompt corrective action if a member is observed or reported to be improperly using a PCD.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personal Communication Devices*

---

- (a) An investigation into improper conduct should be promptly initiated when circumstances warrant.
- (b) Before conducting any administrative search of a member's personally owned device, supervisors should consult with the District Attorney and the HR Manager.

#### **501.7 OFFICIAL USE**

Members are reminded that PCDs are not secure devices and conversations may be intercepted or overheard. Caution should be exercised while utilizing PCDs to ensure that sensitive information is not inadvertently transmitted. Members are not permitted to access personal email accounts through the use of an Office-issued PCD.

#### **501.8 USE WHILE DRIVING**

The use of a PCD while driving can adversely affect safety, cause unnecessary distractions and present a negative image to the public. Criminal Investigators operating emergency vehicles should minimize the use of these devices to matters of importance and should, where practicable, stop the vehicle at an appropriate location to use the PCD, unless the emergency vehicle is configured to allow hands-free use.

Members who are operating Office vehicles that are not authorized emergency vehicles shall not use a PCD while driving unless the device is specifically designed and configured to allow hands-free use. In an emergency, a wireless phone may be used to place an emergency call to the Office or other emergency services agency (Vehicle Code § 23123; Vehicle Code § 23123.5). Hands-free use should be restricted to business-related calls or calls of an urgent nature.

## Vehicle Use

### 502.1 PURPOSE AND SCOPE

The purpose of this policy is to establish a system of accountability to ensure Stanislaus County District Attorney vehicles are used appropriately. This policy provides guidelines for on/off duty use of vehicles and shall not be construed to create or imply any contractual obligation by the County of Stanislaus to provide assigned take-home vehicles.

### 502.2 POLICY

The Stanislaus County District Attorney's Office provides vehicles for work related business and may assign vehicles based on a determination of operational efficiency, economic impact, specific work related needs, and other considerations.

#### 502.2.1 RESPONSIBILITIES

Employee will be responsible to:

- Obtain authorization to drive from the Department Head or designee by completing an Application for Authorization to Drive on Official County Business form.
- Complete County approved defensive driver training as outlined in the Driver Authorization and Performance Policy Employee Training Standards form. Maintain a valid California driver's license for the type of vehicle(s) driven.
- Complete the Annual Employee Driver Acknowledgement.
- Maintain current automobile insurance with limits no less than those required by State Law. All vehicles driven within the scope of employment must be insured in accordance with State Law at all times. Employees are not required to purchase additional "business use" coverage on their existing insurance policies.
- Fully comply with the State of California Vehicle Code and standards for safe vehicle operation while driving on County or personal business.
- If operating a personal vehicle, drivers will maintain their vehicle in a manner to ensure safe operation on public streets. Driving personal vehicles within the scope of employment is one option that may be available to employees based on the needs of the individual department and the availability and/or cost of alternative options (fleet vehicles or rental cars). Employees will not be required to drive their personal vehicle within the scope of employment unless they are currently receiving an auto allowance. Departments may require the use of fleet or rental vehicles based on the individual needs of the department.  
Additional information on the use of vehicles is located in the County Travel Policy.
- In the event your license has been suspended or if your personal auto insurance has been canceled, report it immediately to your supervisor.
- Wear seatbelts or restraints in the vehicle if so equipped. When transporting children – child restraints shall be used.
- Drive carefully and defensively.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Use*

---

- County drivers may not operate cellular phones while driving except as otherwise provided by State Law (hands-free devices, law enforcement exceptions, etc.). Any hands-free cell phone use will be limited and must not compromise driving ability and driving safety at any time. It is expected that should the use of cell phones compromise safety, the driver will pull over and stop the vehicle to complete the phone call.
- Fully comply with this policy.

Supervisor/Manager will be responsible to:

- Ensure that all supervised employees are aware of their responsibilities under this Policy and have received training in compliance with Driver Authorization and Performance Policy Employee Training Standards.
- Ensure that supervised employees who drive on official County business have a current completed Application for Authorization to Drive on Official County Business form on file with Risk Management.

[See attachment: Application for Authorization to Drive on Official County Business Form.pdf](#)

[See attachment: Driver Authorization and Performance Policy Employee Training Standards.pdf](#)

### **502.3 USE OF VEHICLES**

Stanislaus County District Attorney members who need to use an office vehicle for official business travel can sign out a pool vehicle for that purpose. Available pool vehicles can be obtained from the Bureau of Investigation (BI). You are required to email (DA\_Cars) to prearrange the use of an office pool car and fill out the sign-in sheet when you take possession of the pool car.

#### **502.3.1 INSPECTIONS**

Members shall be responsible for inspecting the interior and exterior of any assigned vehicle before taking the vehicle into service and at the conclusion of their shifts. Any previously unreported damage, mechanical problems, unauthorized contents, or other problems with the vehicle shall be promptly reported to a supervisor and documented as appropriate.

The interior of any vehicle that has been used to transport any person other than a member of this bureau should be inspected prior to placing another person in the vehicle and again after the person is removed. This is to ensure that unauthorized or personal items have not been left in the vehicle.

All bureau vehicles are subject to inspection and/or search at any time by a supervisor without notice and without cause. No member assigned to or operating such vehicle shall be entitled to any expectation of privacy with respect to the vehicle or its contents.

#### **502.3.2 SECURITY AND UNATTENDED VEHICLES**

Unattended vehicles should be locked and secured at all times. No key should be left in the vehicle except when it is necessary that the vehicle be left running (e.g., continued activation of emergency lights, equipment charging). Investigators who exit a vehicle rapidly in an emergency situation or to engage in a foot pursuit must carefully balance the need to exit the vehicle quickly with the need to secure the vehicle.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Use*

---

Investigators shall ensure all weapons are secured with a vehicle locking device or inside the vehicles attached locked safe while the vehicle is unattended.

#### 502.3.3 AUTHORIZED PASSENGERS

Transportation in a County-owned vehicle of any non-County person while not engaged in official County business is prohibited, unless otherwise expressly permitted by applicable law or department policy, or unless prior specific authorization is given by the Chief Executive Officer.

#### 502.3.4 ALCOHOL

Members may not violate state law regarding vehicle operation while intoxicated. Members are strongly encouraged to review and understand the County's policy on alcohol and drugs in the workplace.

[See attachment: Personnel Manual TAB 8 Drug Free Workplace Policy.pdf](#)

#### 502.3.5 ACCESSORIES AND/OR MODIFICATIONS

There shall be no modifications, additions or removal of any equipment or accessories without written permission from the assigned vehicle program manager within the Bureau of Investigation.

#### 502.3.6 MAINTENANCE

Members are responsible for the cleanliness (exterior and interior) and overall maintenance of County vehicles. Cleaning and maintenance supplies will be provided by the Bureau. Failure to adhere to these requirements may result in discipline and/or loss of vehicle use. The following should be performed as outlined below:

- (a) Members shall make inspections of their vehicles for service/maintenance requirements and damage.
- (b) It is the member's responsibility to ensure that his/her assigned vehicle is maintained according to the established service and maintenance schedule. Unassigned pool vehicles will be scheduled for maintenance by a member of the Bureau of Investigation.
- (c) All scheduled vehicle maintenance and car washes shall be performed as necessary at a facility approved by the bureau supervisor in charge of vehicle maintenance.
- (d) The Bureau shall be notified of problems with the vehicle and approve any major repairs before they are performed.
- (e) When leaving the vehicle at the maintenance facility, the member will complete a vehicle repair card explaining the service or repair, and leave it on the seat or dash.
- (f) All weapons shall be removed from any vehicle left for maintenance.
- (g) The Bureau supervisors should make, at a minimum, monthly inspections of vehicles assigned to members under their command to ensure the vehicles are being maintained in accordance with this policy.
- (h) If less than or at 1/2 a tank of fuel, members should refill the fuel tank to full before returning the pool car.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Use*

---

#### 502.3.7 DAMAGE, ABUSE AND MISUSE

When any County vehicle is involved in a traffic collision or otherwise incurs damage, the involved member shall promptly notify their immediate supervisor and a BI Lieutenant. Any traffic collision report shall be filed with the agency having jurisdiction where the collision occurred. Employees and supervisors are responsible for completing the County vehicle accident report for and submit the form to Human Resources and Risk Management.

Damage to any County vehicle that was not caused by a traffic collision shall be immediately reported during the shift in which the damage was discovered, documented in memorandum format, photographed, and forwarded to a Lieutenant. An administrative investigation should be initiated to determine if there has been any vehicle abuse or misuse.

[See attachment: Stanislaus County Motor Vehicle Accident Report.pdf](#)

#### 502.3.8 TOLL ROAD USAGE

Law enforcement vehicles are not routinely exempted from incurring toll road charges.

To avoid unnecessary toll road charges, all members operating County vehicles on a toll road shall adhere to the following:

- (a) Members operating County vehicles for any reason other than in response to an emergency shall pay the appropriate toll charge or utilize the appropriate toll way transponder. Members may submit a request for reimbursement from the County for any toll fees incurred in the course of official business.
- (b) Members operating a County vehicle passing through an automated toll plaza or booth shall, upon return, notify their immediate supervisor of the incurred toll costs and vehicle used so these costs can be tracked by finance and appropriately paid.
- (c) Members passing through a toll plaza or booth during a response to an emergency shall notify, in writing, the appropriate Lieutenant within five working days explaining the circumstances.

#### 502.3.9 DRIVER PERFORMANCE

Employees who are required to drive in the performance of their duties shall abide by all applicable vehicle codes. Failure of an employee to drive safely may result in disciplinary action. Departments and/or safety committees shall review all employee motor vehicle accidents, including, but not limited to:

- (a) Repeated Non-Serious Accidents: (2) or more on-the-job, non-serious, accidents within (24) months. A non-serious accident is limited to property damage of less than \$1,500 without bodily injury.
- (b) Serious Vehicle Accidents: Vehicle accident that results in injury or death, or involves a history of (2) or more vehicle accidents, within a (36) month period resulting in property damage of more than \$1,500 each.
- (c) Willful Misconduct or Recklessness: Any occasion where a safety committee (established under County Ordinance 2. 36.00 and 2. 60.00) finds the employee has demonstrated driving behavior more serious than a failure to exercise due care. \

# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Use*

---

Criminal Investigators have authorized emergency vehicle exemptions as outlined in Vehicle Code 21055 however, this section does not relieve the driver of a vehicle from the duty to drive with due regard for the safety of all persons using the highway, nor protect him from the consequences of an arbitrary exercise of the privileges granted (VC 21056). For additional guidance on emergency vehicle operations, refer to Policy 308.

#### **502.4 CRIMINAL INVESTIGATOR VEHICLE ASSIGNMENTS**

Stanislaus County District Attorney vehicles may be assigned to sworn peace officers within the Bureau of Investigation at the discretion of the Chief of Investigations. Vehicles may be assigned for on-duty and/or take-home use. Assigned vehicles may be changed at any time. Permission to take home a vehicle may be withdrawn at any time.

The assignment of vehicles may be suspended when the member is unable to perform his/her regular assignment.

##### **502.4.1 ASSIGNED VEHICLES**

Members who have been assigned a take-home vehicle may use the vehicle to commute to the workplace and for office-related business. The member must be approved for an assigned vehicle by the Chief Investigator and shall adhere to the following criteria:

- (a) The member must live within a 25 miles of the Stanislaus County line. A longer response time may be permitted subject to approval from the Chief Investigator. Members who reside outside the permissible radius may be required to secure or garage the vehicle at a designated location at the direction of the Chief Investigator.
- (b) Except as may be provided by a memorandum of understanding, time spent during normal commuting is not compensable.
- (c) The vehicle may be used to drive from home to an assigned duty location and from there to home. The vehicle may be stopped en route to or from the duty assignment for minor personal necessities.
- (d) The member may be responsible for the care and maintenance of the vehicle.
- (e) When at the member's residence, the vehicle should be parked inside of a garage, behind a fenced area, in the driveway, or legally parked in the street in front of the member's residence.
- (f) Vehicles shall be locked when not attended.
- (g) If the vehicle is not secured inside a locked garage, all firearms and other Bureau safety equipment shall be removed from the interior of the vehicle and properly secured inside the residence. The only exception to this is if the vehicle is equipped with a secure locking vehicle safe installed by the County's Fleet Department.
- (h) When the member will be away (e.g., on vacation) for periods exceeding one week, the vehicle shall be stored in a secure garage at the member's residence or at the office.
- (i) All office identification, portable radios and equipment should be secured and out of view from the public.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Vehicle Use*

---

Members are cautioned that under federal and local tax rules, personal use of a County owned vehicle may create an income tax liability to the member. Members should address questions regarding tax consequences to their tax adviser.

The assignment of vehicles is at the discretion of the Chief Investigator. Assigned vehicles may be changed at any time and/or permissions to take home a vehicle may be withdrawn at any time.

#### 502.4.2 ENFORCEMENT ACTIONS

When driving a take-home vehicle to and from work outside of the jurisdiction of the Stanislaus County District Attorney's Office or while off-duty, an investigator shall not initiate enforcement actions except in those circumstances where a potential threat to life or serious property damage exists (see the Off-Duty Law Enforcement Actions and Law Enforcement Authority policies).

Investigators may render public assistance when it is deemed prudent (e.g., to a stranded motorist).

Investigators driving take-home vehicles shall be armed, appropriately attired and carry their bureau-issued identification. Investigators should also ensure that bureau radio communication capabilities are maintained to the extent feasible.

# Military Equipment

## 503.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the approval, acquisition, and reporting requirements of military equipment (Government Code § 7070; Government Code § 7071; Government Code § 7072).

### 503.1.1 DEFINITIONS

Definitions related to this policy include (Government Code § 7070):

**Governing body** – The elected or appointed body that oversees the Bureau.

**Military equipment** – Includes but is not limited to the following:

- Unmanned, remotely piloted, powered aerial or ground vehicles.
- Mine-resistant ambush-protected (MRAP) vehicles or armored personnel carriers.
- High mobility multipurpose wheeled vehicles (HMMWV), two-and-one-half-ton trucks, five-ton trucks, or wheeled vehicles that have a breaching or entry apparatus attached.
- Tracked armored vehicles that provide ballistic protection to their occupants.
- Command and control vehicles that are either built or modified to facilitate the operational control and direction of public safety units.
- Weaponized aircraft, vessels, or vehicles of any kind.
- Battering rams, slugs, and breaching apparatuses that are explosive in nature. This does not include a handheld, one-person ram.
- Firearms and ammunition of .50 caliber or greater, excluding standard-issue shotguns and standard-issue shotgun ammunition.
- Specialized firearms and ammunition of less than .50 caliber, including firearms and accessories identified as assault weapons in Penal Code § 30510 and Penal Code § 30515, with the exception of standard-issue firearms.
- Any firearm or firearm accessory that is designed to launch explosive projectiles.
- Noise-flash diversionary devices and explosive breaching tools.
- Munitions containing tear gas or OC, excluding standard, service-issued handheld pepper spray.
- Area denial electroshock devices, microwave weapons, water cannons, long-range acoustic devices (LRADs), acoustic hailing devices, and sound cannons.
- Kinetic energy weapons and munitions.
- Any other equipment as determined by a governing body or a state agency to require additional oversight.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Military Equipment*

---

#### **503.2 POLICY**

It is the policy of the Stanislaus County District Attorney's Office that members of this bureau comply with the provisions of Government Code § 7071 with respect to military equipment.

#### **503.3 MILITARY EQUIPMENT COORDINATOR**

The Chief of Investigations should designate a member of this bureau to act as the military equipment coordinator. The responsibilities of the military equipment coordinator include but are not limited to:

- (a) Acting as liaison to the governing body for matters related to the requirements of this policy.
- (b) Identifying bureau equipment that qualifies as military equipment in the current possession of the Bureau, or the equipment the Bureau intends to acquire that requires approval by the governing body.
- (c) Conducting an inventory of all military equipment at least annually.
- (d) Collaborating with any allied agency that may use military equipment within the jurisdiction of Stanislaus County District Attorney's Office (Government Code § 7071).
- (e) Preparing for, scheduling, and coordinating the annual community engagement meeting to include:
  - 1. Publicizing the details of the meeting.
  - 2. Preparing for public questions regarding the bureau's funding, acquisition, and use of equipment.
- (f) Preparing the annual military equipment report for submission to the Chief of Investigations and ensuring that the report is made available on the bureau website (Government Code § 7072).
- (g) Establishing the procedure for a person to register a complaint or concern, or how that person may submit a question about the use of a type of military equipment, and how the Bureau will respond in a timely manner.

#### **503.4 MILITARY EQUIPMENT INVENTORY**

The following constitutes a list of qualifying equipment for the Bureau:

[See attachment: 2022-10-03 Military Equipment Attachment.pdf](#)

#### **503.5 APPROVAL**

The Chief of Investigations or the authorized designee shall obtain approval from the governing body by way of an ordinance adopting the military equipment policy. As part of the approval process, the Chief of Investigations or the authorized designee shall ensure the proposed military equipment policy is submitted to the governing body and is available on the bureau website at least 30 days prior to any public hearing concerning the military equipment at issue (Government Code § 7071). The military equipment policy must be approved by the governing body prior to engaging in any of the following (Government Code § 7071):

- (a) Requesting military equipment made available pursuant to 10 USC § 2576a.

### *Military Equipment*

---

- (b) Seeking funds for military equipment, including but not limited to applying for a grant, soliciting or accepting private, local, state, or federal funds, in-kind donations, or other donations or transfers.
- (c) Acquiring military equipment either permanently or temporarily, including by borrowing or leasing.
- (d) Collaborating with another law enforcement agency in the deployment or other use of military equipment within the jurisdiction of this bureau.
- (e) Using any new or existing military equipment for a purpose, in a manner, or by a person not previously approved by the governing body.
- (f) Soliciting or responding to a proposal for, or entering into an agreement with, any other person or entity to seek funds for, apply to receive, acquire, use, or collaborate in the use of military equipment.
- (g) Acquiring military equipment through any means not provided above.

#### **503.6 COORDINATION WITH OTHER JURISDICTIONS**

Military equipment should not be used by any other law enforcement agency or member in this jurisdiction unless the military equipment is approved for use in accordance with this policy.

#### **503.7 ANNUAL REPORT**

Upon approval of a military equipment policy, the Chief of Investigations or the authorized designee should submit a military equipment report to the governing body for each type of military equipment approved within one year of approval, and annually thereafter for as long as the military equipment is available for use (Government Code § 7072).

The Chief of Investigations or the authorized designee should also make each annual military equipment report publicly available on the bureau website for as long as the military equipment is available for use. The report shall include all information required by Government Code § 7072 for the preceding calendar year for each type of military equipment in bureau inventory.

#### **503.8 COMMUNITY ENGAGEMENT**

Within 30 days of submitting and publicly releasing the annual report, the Bureau shall hold at least one well-publicized and conveniently located community engagement meeting, at which the Bureau should discuss the report and respond to public questions regarding the funding, acquisition, or use of military equipment.

## **Chapter 6 - Support Services**

# Property and Evidence

## 600.1 PURPOSE AND SCOPE

This policy provides for the proper collection, storage, and security of evidence and other property. Additionally, this policy provides for the protection of the chain of evidence and identifies those persons authorized to remove and/or destroy property.

### 600.1.1 DEFINITIONS

Definitions related to this policy include:

**Property** - All articles placed in secure storage within the Evidence Room, including the following:

- Evidence - Items taken or recovered in the course of an investigation that may be used in the prosecution of a case, including photographs and latent fingerprints.
- Found property - Items found by members of the Bureau or the public that have no apparent evidentiary value and where the owner cannot be readily identified or contacted.
- Safekeeping - Items received by the Bureau for safekeeping, such as a firearm, the personal property of an arrestee that has been not taken as evidence, and items taken for safekeeping under authority of law.

## 600.2 PROPERTY HANDLING

Any member who first comes into possession of any property shall retain such property in their possession until it is properly tagged and placed in the designated property locker or storage room along with the property form. Care shall be taken to maintain the chain of custody for all evidence.

Whenever property is taken or received (e.g., relinquished firearms) from an individual, a property receipt form will be completed. The receipt shall describe the property and contain a notice on how to retrieve the property, as applicable, from the Bureau. A copy of the property receipt form shall be given to the individual from whom the property was taken or received.

Where ownership can be established as to found property with no apparent evidentiary value, such property may be released to the owner without the need for booking. The property form must be completed to document the release of property not booked and the owner shall sign the form acknowledging receipt of the items.

### 600.2.1 PROPERTY BOOKING PROCEDURE

All property must be booked prior to the employee going off-duty unless otherwise approved by a supervisor. Employees booking property shall observe the following guidelines:

- (a) Complete the property form describing each item of property separately, listing all serial numbers, owner's name, finder's name, and other identifying information or markings.
- (b) Mark each item of evidence with the booking employee's initials and the date booked using the appropriate method so as not to deface or damage the value of the property.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Property and Evidence*

---

- (c) Place the date, item number, case number, description, investigator, and suspect on the evidence package and/or on the evidence sticker affixed to the package. The item number shall include the investigator's initials such as FM-1.
- (d) Seal the evidence package with tape and place your initials and date along the tape..
- (e) The original property receipt form shall be submitted with the case report. A copy of the property receipt form shall be submitted to the evidence clerk.
- (f) An investigator who has previously booked evidence under a case number will number any new evidence starting from the last evidence item number he/she used. For example: If an investigator books evidence in a case on 1/1/20 and had ten evidence items, those items would be labeled (investigator initials) 1-10. If the same investigator wishes to book evidence in the same case at a later date they will start with the evidence item number where they left off. In this case it would be evidence item 11.
- (g) If a new investigator obtains evidence for a case in which evidence was already booked by a different investigator, the new investigator will start with evidence item #1.

#### 600.2.2 NARCOTICS AND DANGEROUS DRUGS

All narcotics and dangerous drugs shall be booked separately, listing the items on the property receipt form.. Paraphernalia as defined by Health and Safety Code § 11364 shall also be booked separately.

Needles and syringes shall not be booked into the Evidence and Property facility. They shall be digitally photographed and the photographs will be downloaded onto a CD and stored. They syringe shall be placed in a SHARPS container for destruction.

Glass drug pipes shall not be booked in the Evidence and Property facility unless needed for specific evidentiary purposes not related to the charge of possessing the item. Any evidence (e.g. residue) shall be removed from the pipe if needed for future court presentation. The pipe shall be digitally photographed and the photographs will be downloaded onto a CD and stored. The glass drug pipe shall be placed in a SHARPS container or clearly marked for destruction.

#### 600.2.3 EXPLOSIVES

Investigators who encounter a suspected explosive device shall promptly notify their immediate supervisor. The bomb squad will be called to handle explosive-related incidents and will be responsible for the handling, storage, sampling and disposal of all suspected explosives. Explosives shall not be booked into the Evidence and Property Facility.

Fireworks will be photographed. Photographs of the fireworks are to be placed into evidence. The actual fireworks will be collected and disposed of by an Arson investigator.

#### 600.2.4 EXCEPTIONAL HANDLING

Certain property items require a separate process. The following items shall be processed in the described manner:

A. Bodily fluids such as blood or semen stains shall be air dried prior to booking.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Property and Evidence*

---

B. All cash shall be packaged separately. Two SCDA employees shall individually count all money, and both employees will sign the sealed package verifying the total cash amount. Currency will then be delivered to the Stanislaus County Auditor's office to store.

C. Do not book any electronic evidence (Hard Drives, Flash Drives, Memory Cards, etc.) into our evidence room without having IT scan them first. Follow the process outlined below regarding electronic evidence:

1. Take the device to the IT unit to scan prior to booking into evidence.

2. The IT unit will scan the device and:

**(a) If the device is clean (No Malware found), IT:**

Will attach a report to the device to confirm the device is clean.

You can upload the data from the scanned device to a folder on the DA's network for future reference and you can book the device into evidence.

If the device has **CELLEBRITE DATA**, **Do Not Upload the Data to the DA network storage or Evidence.com**

**(b) If the device contains viruses or malware:**

The Original device will be marked "Contaminated."

The IT unit will duplicate the contaminated device.

Any infected files with malware will be deleted from the **duplicate device**. A report will be attached to the duplicate device to show the duplicate device is "clean" and which files were deleted from which directories on the duplicate device.

You can then upload the data from the duplicate device to a folder on the DA's network for future reference and you can book the device into evidence.

**NO ONE IS PERMITTED TO ATTACH THE ORIGINAL CONTAMINATED EVIDENCE DEVICE TO ANY DA OFFICE DEVICES (PCS, LAPTOPS AND MOBILE PHONES).**

**The original contaminated device can be booked into evidence once it is clearly marked as contaminated.**

**Do Not Upload **CELLEBRITE DATA** to our network storage or Evidence.com.**

**Document in your report that the evidence that will be discovered will be missing some data due to it containing malware.**

D. County property, unless connected to a known criminal case, should be released directly to the appropriate County department. No formal booking is required. In cases where no responsible person can be located, the property should be booked for safekeeping in the normal manner.

### **600.3 PACKAGING OF PROPERTY**

Certain items require special consideration and shall be booked separately as follows:



# Stanislaus County District Attorney's Office

## Policy Manual

### *Property and Evidence*

---

- (a) Narcotics and dangerous drugs
- (b) Firearms (ensure they are unloaded and booked separately from ammunition)
- (c) Property with more than one known owner
- (d) Paraphernalia as described in Health and Safety Code § 11364
- (e) Fireworks
- (f) Contraband

#### **600.3.1 PACKAGING CONTAINER**

Members shall package all property, except narcotics and dangerous drugs, in a suitable container available for its size. Knife boxes should be used to package knives, and syringe tubes should be used to package syringes and needles.

A property tag shall be securely attached to the outside of all items or group of items packaged together.

#### **600.3.2 PACKAGING NARCOTICS**

The investigator seizing narcotics and dangerous drugs shall retain such property in his/her possession until it is properly weighed, packaged, labeled, and placed in evidence. Prior to packaging and if the quantity allows, a presumptive test should be made on all suspected narcotics. If conducted, the results of this test shall be included in the investigator's report.

Narcotics and dangerous drugs shall be packaged in a DOJ drug envelope of appropriate size.. The booking investigator shall initial the sealed envelope and the initials covered with cellophane tape. Narcotics and dangerous drugs shall not be packaged with other property.

#### **600.4 RECORDING OF PROPERTY**

The Evidence and Property clerk receiving custody of evidence or property shall record his/her name, the date and time the property was booked by the booking officer and where the property will be stored within ICJIS.

Any changes in the location of property held by the Stanislaus County District Attorney's Office shall be noted in ICJIS and on the chain of custody form..

#### **600.5 PROPERTY CONTROL**

Each time the Evidence and Property clerk receives property she/he shall enter this information in ICJIS. When the Evidence and Property clerk releases property to another person, he/she shall document the release on the Evidence and Property Chain of Custody form. Investigators desiring property for court shall contact the Evidence and Property clerk at least one day prior to the court day.

#### **600.5.1 RESPONSIBILITY OF OTHER PERSONNEL**

Every time property is released or received, an appropriate entry on the Evidence and Property Chain of Custody form shall be completed to maintain the chain of evidence.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Property and Evidence*

---

#### 600.5.2 TRANSFER OF EVIDENCE TO CRIME LABORATORY

The transporting employee will check the evidence out of property, indicating the date and time on the Evidence and Property Chain of Custody form and the request for laboratory analysis.

The Evidence and Property clerk releasing the evidence must complete the required information on the Evidence and Property Chain of Custody form and in ICJIS. The lab forms will be transported with the property to the examining laboratory.

#### 600.5.3 STATUS OF PROPERTY

Each person receiving property will make the appropriate entry to document the chain of evidence. Temporary release of property to investigators for investigative purposes, or for court, shall be noted on the Evidence and Property Chain of Custody form, stating the date, time and to whom released. If an investigator received property for investigative purposes, the investigator will document in a report what was done with the property while under their control.

The Evidence and Property clerk shall obtain the signature of the person to whom property is released, and the reason for release. Any employee receiving property shall be responsible for such property until it is properly returned to property or properly released to another authorized person or entity.

The return of the property shall be recorded on the Evidence and Property Chain of Custody form.

#### 600.5.4 AUTHORITY TO RELEASE PROPERTY

The Investigative Bureau shall authorize the disposition or release of all evidence and property coming into the care and custody of the Bureau.

#### 600.5.5 RELEASE OF PROPERTY

All reasonable attempts shall be made to identify the rightful owner of found property or evidence not needed for an investigation.

Release of property shall be made upon receipt of an authorized release form, listing the name and address of the person to whom the property is to be released. The release authorization shall be signed by the authorizing supervisor or detective and must conform to the items listed on the property form or must specify the specific item(s) to be released. Release of all property shall be documented on the property form.

With the exception of firearms and other property specifically regulated by statute, found property and property held for safekeeping shall be held for a minimum of 90 days. During such period, property personnel shall attempt to contact the rightful owner by telephone and/or mail when sufficient identifying information is available. Property not held for any other purpose and not claimed within 90 days after notification (or receipt, if notification is not feasible) may be auctioned to the highest bidder at a properly published public auction. If such property is not sold at auction or otherwise lawfully claimed, it may thereafter be destroyed (Civil Code § 2080.6). The final disposition of all such property shall be fully documented in related reports.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Property and Evidence*

---

A Lieutenant shall release the property upon proper identification being presented by the owner for which an authorized release has been received. A signature of the person receiving the property shall be recorded on the original property form. After release of all property entered on the property control card, the card shall be forwarded to the Records Bureau for filing with the case. If some items of property have not been released, the property card will remain with the Evidence Room. Upon release, the proper entry shall be documented in the Property Log.

Under no circumstances shall any firearm, magazine, or ammunition be returned to any individual unless and until such person presents valid identification and written notification from the California Department of Justice that conforms to the provisions of Penal Code § 33865.

The Evidence Room Supervisor should also make reasonable efforts to determine whether the person is the subject of any court order preventing the person from possessing a firearm and, if so, the firearm should not be released to the person while the order is in effect.

The Bureau is not required to retain any firearm, magazine, or ammunition longer than 180 days after notice has been provided to the owner that such items are available for return. At the expiration of such period, the firearm, magazine, or ammunition may be processed for disposal in accordance with applicable law (Penal Code § 33875).

#### 600.5.6 DISPUTED CLAIMS TO PROPERTY

Occasionally more than one party may claim an interest in property being held by the Bureau, and the legal rights of the parties cannot be clearly established. Such property shall not be released until one party has obtained a valid court order or other undisputed right to the involved property.

All parties should be advised that their claims are civil and in extreme situations, legal counsel for the Bureau may wish to file an interpleader to resolve the disputed claim (Code of Civil Procedure § 386(b)).

#### 600.5.7 CONTROL OF NARCOTICS AND DANGEROUS DRUGS

The Evidence and Property Unit will be responsible for the storage, control and destruction of all narcotics and dangerous drugs coming into the custody of this bureau, including paraphernalia as described in Health and Safety Code § 11364.

#### 600.5.8 RELEASE OF FIREARMS IN DOMESTIC VIOLENCE MATTERS

Within five days of the expiration of a restraining order issued in a domestic violence matter that required the relinquishment of a firearm or ammunition, the Lieutenant shall return the weapon or ammunition to the owner if the requirements of Penal Code § 33850 and Penal Code § 33855 are met, unless the firearm or ammunition is determined to be stolen, evidence in a criminal investigation, another successive order has been issued against the individual, or the individual is otherwise prohibited from possessing a firearm (Family Code § 6389(g); Penal Code § 29825.5; Penal Code § 33855).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Property and Evidence*

---

#### 600.5.9 RELEASE OF FIREARMS, MAGAZINES, AND AMMUNITION

The Bureau shall not return any firearm, magazine, or ammunition taken into custody to any individual unless all requirements of Penal Code § 33855 are met.

#### **600.6 DISPOSITION OF PROPERTY**

All property not held for evidence in a pending criminal investigation or proceeding, and held for six months or longer where the owner has not been located or fails to claim the property, may be disposed of in compliance with existing laws upon receipt of proper authorization for disposal. The Lieutenant shall request a disposition or status on all property which has been held in excess of 120 days, and for which no disposition has been received from a supervisor or detective.

##### 600.6.1 EXCEPTIONAL DISPOSITIONS

The following types of property shall be destroyed or disposed of in the manner, and at the time prescribed by law, unless a different disposition is ordered by a court of competent jurisdiction:

- Weapons declared by law to be nuisances (Penal Code § 25700; Penal Code § 26110; Penal Code § 26395; Penal Code § 29300; Penal Code § 18010; Penal Code § 32750)
- Animals, birds, and related equipment that have been ordered forfeited by the court (Penal Code § 599a)
- Counterfeiting equipment (Penal Code § 480)
- Gaming devices (Penal Code § 335a)
- Obscene matter ordered to be destroyed by the court (Penal Code § 312)
- Altered vehicles or component parts (Vehicle Code § 10751)
- Narcotics (Health and Safety Code § 11474 et seq.)
- Unclaimed, stolen, or embezzled property (Penal Code § 1411)
- Destructive devices (Penal Code § 19000)
- Sexual assault evidence (Penal Code § 680)

##### 600.6.2 RETENTION OF BIOLOGICAL EVIDENCE

The Evidence and Property Unit Supervisor shall ensure that no biological evidence held by the Bureau is destroyed without adequate notification to the following persons, when applicable:

- (a) The defendant
- (b) The defendant's attorney
- (c) The appropriate prosecutor and Attorney General
- (d) Any sexual assault victim
- (e) The General Crimes Bureau supervisor

Biological evidence shall be retained for either a minimum period that has been established by law (Penal Code § 1417.9) or that has been established by the Evidence and Property Unit Supervisor, or until the expiration of any imposed sentence that is related to the evidence, whichever time

# Stanislaus County District Attorney's Office

## Policy Manual

### *Property and Evidence*

---

period is greater. Following the retention period, notifications should be made by certified mail and should inform the recipient that the evidence will be destroyed after a date specified in the notice unless a motion seeking an order to retain the sample is filed and served on the Bureau within 180 days of the date of the notification. A record of all certified mail receipts shall be retained in the appropriate file. Any objection to, or motion regarding, the destruction of the biological evidence should be retained in the appropriate file and a copy forwarded to the Evidence and Property supervisor.

Biological evidence related to a homicide shall be retained indefinitely and may only be destroyed with the written approval of the Chief of Investigations and the head of the applicable prosecutor's office.

Biological evidence or other crime scene evidence from an unsolved sexual assault should not be disposed of prior to expiration of the statute of limitations and shall be retained as required in Penal Code § 680. Even after expiration of an applicable statute of limitations, the Evidence and Property supervisor should be consulted and the sexual assault victim shall be notified at least 60 days prior to the disposal (Penal Code § 680). Reasons for not analyzing biological evidence shall be documented in writing (Penal Code § 680.3).

#### **600.6.3 DESTRUCTION OF FIREARMS AND OTHER WEAPONS**

The Evidence Room supervisor or the authorized designee shall develop and maintain guidelines and procedures relating to the destruction of firearms and other weapons that includes but is not limited to the following (Penal Code § 18005):

- (a) Identification of firearms and other weapons that need to be destroyed
- (b) Maintenance of records of firearms and other weapons that need to be destroyed, including entry into the Automated Firearms System, as applicable, and records of the destruction and disposal of those firearms and other weapons
- (c) Identification of any law enforcement agency that the Bureau contracts with or has an agreement with related to the storage or destruction of firearms or other weapons that outlines the responsibilities of this bureau and the other agency
  - 1. If the Bureau contracts with a third-party for destruction of firearms or other weapons, the contract must explicitly prohibit the sale of any firearm or weapon or any part or attachment to the firearm or weapon.

The Evidence Room supervisor or the authorized designee should ensure guidelines and procedures relating to the destruction of firearms and other weapons are posted on the Stanislaus County District Attorney's Office website (Penal Code § 18005).

#### **600.7 INSPECTIONS OF THE EVIDENCE ROOM**

- (a) Every six months,, the supervisor of the Evidence and Property Unit shall make an inspection of the evidence storage facilities and practices to ensure adherence to appropriate policies and procedures.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Property and Evidence*

---

- (b) An annual audit of evidence held by the Bureau shall be conducted by the Property and Evidence Lieutenant
- (c) Whenever a change is made in personnel who have access to the evidence room, an inventory of all evidence/property shall be made by the newly designated property and evidence clerk and the property and evidence supervisor ensure that records are correct and all evidence property is accounted for.

#### **600.8 POLICY**

It is the policy of the Stanislaus County District Attorney's Office to process and store all property in a manner that will protect it from loss, damage, or contamination, while maintaining documentation that tracks the chain of custody, the location of property, and its disposition.

## Protected Information

### 601.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the Stanislaus County District Attorney's Office. This policy addresses the protected information that is used in the day-to-day operation of the Bureau and not the public records information covered in the Records Maintenance and Release Policy.

#### 601.1.1 DEFINITIONS

Definitions related to this policy include:

**Protected information** - Any information or data that is collected, stored or accessed by members of the Stanislaus County District Attorney's Office and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

### 601.2 POLICY

Members of the Stanislaus County District Attorney's Office will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

### 601.3 RESPONSIBILITIES

The Chief of Investigations shall select a member of the Bureau to coordinate the use of protected information.

The responsibilities of this position include but are not limited to:

- (a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Department of Motor Vehicles (DMV) records, and California Law Enforcement Telecommunications System (CLETS).
- (b) Developing, disseminating, and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) Security Policy. See the Stanislaus County District Attorney's Office CJIS Access, Maintenance, and Security Policy for additional guidance.
- (c) Developing, disseminating, and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release, and security of protected information.
- (d) Developing procedures to ensure training and certification requirements are met.
- (e) Resolving specific questions that arise regarding authorized recipients of protected information.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Protected Information*

---

- (f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

#### **601.4 ACCESS TO PROTECTED INFORMATION**

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Stanislaus County District Attorney's Office policy, or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution. See the CJIS Access, Maintenance, and Security Policy for additional guidance.

##### **601.4.1 PENALTIES FOR MISUSE OF RECORDS**

It is a misdemeanor to furnish, buy, receive or possess Department of Justice criminal history information without authorization by law (Penal Code § 11143).

Authorized persons or agencies violating state regulations regarding the security of Criminal Offender Record Information (CORI) maintained by the California Department of Justice may lose direct access to CORI (11 CCR 702).

#### **601.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION**

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Records Manager for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Bureau may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Bureau to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

##### **601.5.1 REVIEW OF CRIMINAL OFFENDER RECORD**

Individuals requesting to review their own California criminal history information shall be referred to the Department of Justice (Penal Code § 11121).

Individuals shall be allowed to review their arrest or conviction record on file with the Bureau after complying with all legal requirements regarding authority and procedures in Penal Code § 11120 through Penal Code § 11127 (Penal Code § 13321).



# Stanislaus County District Attorney's Office

## Policy Manual

### *Protected Information*

---

#### **601.5.2 TRANSMISSION GUIDELINES**

Protected information, such as restricted Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should not be transmitted via unencrypted radio. When circumstances reasonably indicate that the immediate safety of investigators, other bureau members, or the public is at risk, only summary information may be transmitted.

In cases where the transmission of protected information, such as Personally Identifiable Information, is necessary to accomplish a legitimate law enforcement purpose, and utilization of an encrypted radio channel is infeasible, a MDC or bureau-issued cellular telephone should be utilized when practicable. If neither are available, unencrypted radio transmissions shall be subject to the following:

- Elements of protected information should be broken up into multiple transmissions, to minimally separate an individual's combined last name and any identifying number associated with the individual, from either first name or first initial.
- Additional information regarding the individual, including date of birth, home address, or physical descriptors, should be relayed in separate transmissions.

Nothing in this policy is intended to prohibit broadcasting warrant information.

#### **601.6 CALIFORNIA RELIGIOUS FREEDOM ACT**

Members shall not release personal information from any agency database for the purpose of investigation or enforcement of any program compiling data on individuals based on religious belief, practice, affiliation, national origin or ethnicity (Government Code § 8310.3).

#### **601.7 SECURITY OF PROTECTED INFORMATION**

The Chief of Investigations will select a member of the Bureau to oversee the security of protected information.

The responsibilities of this position include but are not limited to (see the CJIS Access, Maintenance, and Security Policy for additional guidance):

- (a) Developing and maintaining security practices, procedures, and training.
- (b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.
- (c) Establishing procedures to provide for the preparation, prevention, detection, analysis, and containment of security incidents, including computer attacks.
- (d) Tracking, documenting, and reporting all breach of security incidents to the Chief of Investigations and appropriate authorities.

#### **601.7.1 MEMBER RESPONSIBILITIES**

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended

# Stanislaus County District Attorney's Office

## Policy Manual

### *Protected Information*

---

table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

#### **601.8 TRAINING**

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination.

## **Chapter 7 - Custody**

# Temporary Custody of Adults

## 700.1 PURPOSE AND SCOPE

This policy provides guidelines to address the health and safety of adults taken into temporary custody by members of the Stanislaus County District Attorney's Office for processing prior to being released or transferred to a housing or other type of facility.

Temporary custody of juveniles is addressed in the Temporary Custody of Juveniles Policy. Juveniles will not be permitted where adults in custody are being held.

Custodial searches are addressed in the Custodial Searches Policy.

Additional guidance for transferring persons in custody to another facility or court is provided in the Transporting Persons in Custody Policy.

### 700.1.1 DEFINITIONS

Definitions related to this policy include:

**Holding cell/cell** - Any locked enclosure for the custody of an adult or any other enclosure that prevents the occupants from being directly visually monitored at all times by a member of the Bureau.

**Safety checks** - Direct, visual observation by a member of this bureau performed at random intervals, within time frames prescribed in this policy, to provide for the health and welfare of adults in temporary custody.

**Temporary custody** - The time period an adult is in custody at the Stanislaus County District Attorney's Office prior to being released or transported to a housing or other type of facility.

## 700.2 POLICY

The Stanislaus County District Attorney's Office is committed to releasing adults from temporary custody as soon as reasonably practicable, and to keeping adults safe while in temporary custody at the Bureau. Adults should be in temporary custody only for as long as reasonably necessary for investigation, processing, transfer or release.

## 700.3 GENERAL CRITERIA AND SUPERVISION

No adult should be in temporary custody for longer than six hours.

### 700.3.1 INDIVIDUALS WHO SHOULD NOT BE IN TEMPORARY CUSTODY

Individuals who exhibit certain behaviors or conditions should not be in temporary custody at the Stanislaus County District Attorney's Office, but should be transported to a jail facility, a medical facility, or another type of facility as appropriate. These include:

- (a) Any individual who is unconscious or has been unconscious while being taken into custody or while being transported.
- (b) Any individual who has a medical condition, including pregnancy, that may require medical attention, supervision, or medication while in temporary custody.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

- (c) Any individual who is seriously injured.
- (d) Individuals who are a suspected suicide risk (see the Mental Illness Commitments Policy).
  - 1. If the investigator taking custody of an individual believes that the individual may be a suicide risk, the investigator shall ensure continuous direct supervision until evaluation, release, or a transfer to an appropriate facility is completed (15 CCR 1030).
- (e) Individuals who are obviously in crisis, as defined in the Crisis Intervention Incidents Policy.
- (f) Individuals who are under the influence of alcohol, a controlled substance, or any substance to the degree that may require medical attention, or who have ingested any substance that poses a significant risk to their health, whether or not they appear intoxicated.
- (g) Any individual who has exhibited extremely violent or continuously violent behavior including behavior that results in the destruction of property or demonstrates an intent to cause physical harm to themselves or others (15 CCR 1053; 15 CCR 1055).
- (h) Any individual who claims to have, is known to be afflicted with, or displays symptoms of any communicable disease that poses an unreasonable exposure risk (15 CCR 1051).
- (i) Any individual with a prosthetic or orthopedic device where removal of the device would be injurious to the individual's health or safety.
- (j) Any individual with an obvious developmental disability (15 CCR 1057).
- (k) Any individual who appears to be a danger to themselves or others due to a behavioral crisis, or who appears gravely disabled (15 CCR 1052).
- (l) Any individual who needs restraint beyond the use of handcuffs or shackles for security reasons (15 CCR 1058).
- (m) Any individual obviously suffering from drug or alcohol withdrawal (15 CCR 1213).

Investigators taking custody of a person who exhibits any of the above conditions should notify a supervisor of the situation. These individuals should not be in temporary custody at the Bureau unless they have been evaluated by a qualified medical or mental health professional, as appropriate for the circumstances.

#### 700.3.2 SUPERVISION IN TEMPORARY CUSTODY

An authorized bureau member capable of supervising shall be present at all times when an individual is held in temporary custody. The member responsible for supervising should not have other duties that could unreasonably conflict with the member's supervision. Any individual in custody must be able to summon the supervising member if needed. If the person in custody has a hearing or speech impairment, accommodations shall be made to provide this ability.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

At least one female bureau member should be present when a female adult is in temporary custody. In the event that none is readily available, the female in custody should be transported to another facility or released pursuant to another lawful process (15 CCR 1027).

Absent exigent circumstances, such as a medical emergency or a violent subject, members should not enter the cell of a person of the opposite sex unless a member of the same sex as the person in custody is present (Penal Code § 4021).

No individual in custody shall be permitted to supervise, control, or exert any authority over other individuals in custody.

#### **700.3.3 STAFFING PLAN**

The Chief of Investigations or the authorized designee shall ensure a staffing plan is prepared and maintained, indicating assigned personnel and their duties. The plan should ensure that at least one member who meets the training standards established by the Board of State and Community Corrections (BSCC) for general fire- and life-safety and is trained in fire- and life-safety procedures relating specifically to the facility is on-duty at all times (15 CCR 1028).

The staffing plan shall be available for biennial review by BSCC staff. The review and recommendations of the BSCC biennial review shall be forwarded to the County, as required by 15 CCR 1027.

#### **700.3.4 ENTRY RESTRICTIONS**

Entry into any location where a person is held in custody should be restricted to:

- (a) Authorized members entering for official business purposes.
- (b) Emergency medical personnel when necessary.
- (c) Any other person authorized by the Lieutenant.

When practicable, more than one authorized member should be present for entry into a location where a person is held in custody for security purposes and to witness interactions.

#### **700.4 INITIATING TEMPORARY CUSTODY**

The investigator responsible for an individual in temporary custody should evaluate the person for any apparent chronic illness, disability, vermin infestation, possible communicable disease, or any other potential risk to the health or safety of the individual or others. The investigator should specifically ask if the individual is contemplating suicide and evaluate the individual for obvious signs or indications of suicidal intent.

The receiving investigator should ask the arresting investigator if there is any statement, indication, or evidence surrounding the individual's arrest and transportation that would reasonably indicate the individual is at risk for suicide or critical medical care. If there is any suspicion that the individual may be suicidal, the individual shall be transported to the County jail or the appropriate mental health facility.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

The investigator should promptly notify the Lieutenant of any conditions that may warrant immediate medical attention or other appropriate action. The Lieutenant shall determine whether the individual will be placed in a cell, immediately released, or transported to jail or other facility.

#### 700.4.1 SCREENING AND PLACEMENT

The investigator responsible for an individual in custody shall (15 CCR 1050):

- (a) Advise the Lieutenant of any significant risks presented by the individual (e.g., suicide risk, health risk, violence).
- (b) Evaluate the following issues against the stated risks in (a) to determine the need for placing the individual in a single cell:
  - 1. Consider whether the individual may be at a high risk of being sexually abused based on all available known information (28 CFR 115.141), or whether the person is facing any other identified risk.
  - 2. Provide any individual identified as being at a high risk for sexual or other victimization with heightened protection. This may include (28 CFR 115.113; 28 CFR 115.141):
    - (a) Continuous, direct sight and sound supervision.
    - (b) Single-cell placement in a cell that is actively monitored on video by a member who is available to immediately intervene.
  - 3. Ensure individuals are separated according to severity of the crime (e.g., felony or misdemeanor).
  - 4. Ensure males and females are separated by sight and sound when in cells.
  - 5. Ensure restrained individuals are not placed in cells with unrestrained individuals.
- (c) Ensure that those confined under civil process or for civil causes are kept separate from those who are in temporary custody pending criminal charges.
- (d) Ensure separation, as appropriate, based on other factors, such as age, criminal sophistication, assaultive/non-assaultive behavior, mental state, disabilities and sexual orientation.

#### 700.4.2 CONSULAR NOTIFICATION

Consular notification may be mandatory when certain foreign nationals are arrested. The XXX Lieutenant will ensure that the U.S. Department of State's list of countries and jurisdictions that require mandatory notification is readily available to bureau members. There should also be a published list of foreign embassy and consulate telephone and fax numbers, as well as standardized notification forms that can be transmitted and then retained for documentation. Prominently displayed signs informing foreign nationals of their rights related to consular notification should also be posted in areas used for the temporary custody of adults.

Bureau members assigned to process a foreign national shall:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

- (a) Inform the individual, without delay, that the individual may have the individual's consular officers notified of the arrest or detention and may communicate with them.
  - 1. This notification should be documented.
- (b) Determine whether the foreign national's country is on the U.S. Department of State's mandatory notification list.
  - 1. If the country is on the mandatory notification list, then:
    - (a) Notify the country's nearest embassy or consulate of the arrest or detention by fax or telephone.
    - (b) Tell the individual that this notification has been made and inform the individual without delay that the individual may communicate with consular officers.
    - (c) Forward any communication from the individual to the individual's consular officers without delay.
    - (d) Document all notifications to the embassy or consulate and retain the faxed notification and any fax confirmation for the individual's file.
  - 2. If the country is not on the mandatory notification list and the individual requests that the individual's consular officers be notified, then:
    - (a) Notify the country's nearest embassy or consulate of the arrest or detention by fax or telephone.
    - (b) Forward any communication from the individual to the individual's consular officers without delay.

## **700.5 SAFETY, HEALTH AND OTHER PROVISIONS**

### **700.5.1 TEMPORARY CUSTODY LOGS**

Any time an individual is in temporary custody at the Stanislaus County District Attorney's Office, the custody shall be promptly and properly documented in a custody log, including:

- (a) Identifying information about the individual, including the individual's name.
- (b) Date and time of arrival at the Bureau.
- (c) Any charges for which the individual is in temporary custody and any case number.
- (d) Time of all safety checks (15 CCR 1027; 15 CCR 1027.5).
- (e) Any medical and other screening requested and completed.
- (f) Any emergency situations or unusual incidents.
- (g) Any other information that may be required by other authorities, such as compliance inspectors.
- (h) Date and time of release from the Stanislaus County District Attorney's Office.

The Lieutenant should initial the log to approve the temporary custody and should also initial the log when the individual is released from custody or transferred to another facility.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

The Lieutenant should make periodic checks to ensure all log entries and safety and security checks are made on time.

#### 700.5.2 TEMPORARY CUSTODY REQUIREMENTS

Members monitoring or processing anyone in temporary custody shall ensure:

- (a) Safety checks and significant incidents/activities are noted on the log.
- (b) Individuals in custody are informed that they will be monitored at all times, except when using the toilet.
  - 1. There shall be no viewing devices, such as peep holes or mirrors, of which the individual is not aware.
  - 2. This does not apply to surreptitious and legally obtained recorded interrogations.
- (c) There is reasonable access to toilets and wash basins.
- (d) There is reasonable access to a drinking fountain or water.
- (e) There are reasonable opportunities to stand and stretch, particularly if handcuffed or otherwise restrained.
- (f) There is privacy during attorney visits.
- (g) Those in temporary custody are generally permitted to remain in their personal clothing unless it is taken as evidence or is otherwise unsuitable or inadequate for continued wear while in custody.
- (h) Clean blankets are provided as reasonably necessary to ensure the comfort of an individual.
  - 1. The supervisor should ensure that there is an adequate supply of clean blankets.
- (i) Adequate shelter, heat, light and ventilation are provided without compromising security or enabling escape.
- (j) Adequate furnishings are available, including suitable chairs or benches.

#### 700.5.3 MEDICAL CARE

First-aid equipment and basic medical supplies should be available to bureau members (15 CCR 1220). At least one member who has current certification in basic first aid and CPR should be on-duty at all times.

Should a person in custody be injured or become ill, appropriate medical assistance should be sought. A supervisor should meet with those providing medical aid at the facility to allow access to the person. Members shall comply with the opinion of medical personnel as to whether an individual in temporary custody should be transported to the hospital. If the person is transported while still in custody, the person will be accompanied by an investigator.

Those who require medication while in temporary custody should not be at the Stanislaus County District Attorney's Office. They should be released or transferred to another facility as appropriate.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

#### 700.5.4 ORTHOPEDIC OR PROSTHETIC APPLIANCE

Subject to safety and security concerns, individuals shall be permitted to retain an orthopedic or prosthetic appliance. However, if the member supervising the individual has probable cause to believe the possession of the appliance presents a risk of bodily harm to any person or is a risk to the security of the facility, the appliance may be removed from the individual unless its removal would be injurious to the individual's health or safety.

Whenever a prosthetic or orthopedic appliance is removed, the Lieutenant shall be promptly apprised of the reason. It shall be promptly returned when it reasonably appears that any risk no longer exists (Penal Code § 2656; 15 CCR 1207).

#### 700.5.5 TELEPHONE CALLS

Immediately upon being booked and, except where physically impossible, no later than three hours after arrest, an individual in custody has the right to make at least three completed calls to an attorney, bail bondsman, and a relative or other person (Penal Code § 851.5). Additional calls may be made as reasonable and necessary (15 CCR 1067). In providing further access to a telephone beyond that required by Penal Code § 851.5, legitimate law enforcement interests such as officer safety, effect on ongoing criminal investigations, and logistics should be balanced against the individual's desire for further telephone access.

- (a) Telephone calls may be limited to local calls, except that long-distance calls may be made by the individual at the individual's own expense.
  - 1. The Bureau should pay the cost of any long-distance calls related to arranging for the care of a child or dependent adult (see the Child and Dependent Adult Safety Policy).
  - 2. The provisions of Penal Code § 851.5 concerning this issue shall be posted in bold, block type in a conspicuous place within the facility.
- (b) The individual should be given sufficient time to contact whomever the individual desires and to make any necessary arrangements, including child or dependent adult care, or transportation upon release.
  - 1. Telephone calls are not intended to be lengthy conversations. The member assigned to monitor or process the individual may use the member's judgment in determining the duration of the calls.
  - 2. Within three hours of the arrest, the member supervising the individual should inquire whether the individual is a custodial parent with responsibility for a minor child, and notify the individual that the individual may make two additional telephone calls to a relative or other person for the purpose of arranging for the care of minor children (Penal Code § 851.5).
- (c) Calls between an individual in temporary custody and the individual's attorney shall be deemed confidential and shall not be monitored, eavesdropped upon, or recorded (Penal Code § 851.5(b)(1); 15 CCR 1068).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

- (d) Individuals who are known to have, or are perceived by others as having, hearing or speech impairments shall be provided access to a telecommunication device which will facilitate communication (15 CCR 1067).

#### 700.5.6 RELIGIOUS ACCOMMODATION

Subject to available resources, safety and security, the religious beliefs and needs of all individuals in custody should be reasonably accommodated (15 CCR 1072). Requests for religious accommodation should generally be granted unless there is a compelling security or safety reason and denying the request is the least restrictive means available to ensure security or safety. The responsible supervisor should be advised any time a request for religious accommodation is denied.

Those who request to wear headscarves or simple head coverings for religious reasons should generally be accommodated absent unusual circumstances. Head coverings shall be searched before being worn.

Individuals wearing headscarves or other approved coverings shall not be required to remove them while in the presence of or while visible to the opposite sex if they so desire. Religious garments that substantially cover the individual's head and face may be temporarily removed during the taking of any photographs.

#### 700.5.7 FIREARMS AND OTHER SECURITY MEASURES

Firearms and other weapons and control devices shall not be permitted in secure areas where individuals are in custody or are processed. They should be properly secured outside of the secure area. An exception may occur only during emergencies, upon approval of a supervisor.

All perimeter doors to secure areas shall be kept locked at all times, except during routine cleaning, when no individuals in custody are present or in the event of an emergency, such as an evacuation.

#### 700.5.8 REPORTING PHYSICAL HARM OR SERIOUS THREAT OF PHYSICAL HARM

In addition to a custody log entry, any incident that results in physical harm or serious threat of physical harm to a member, person in custody, or any other person shall be documented as stated in the Use of Force or Occupational Disease and Work-Related Injury Reporting policies, or other applicable reporting process. A copy of all reports generated regarding the above circumstances shall be submitted as soon as reasonably practicable. The Lieutenant will retain a record of these reports for inspection purposes (15 CCR 1044).

#### 700.5.9 ATTORNEYS AND BAIL BONDSMEN

- (a) An attorney may visit at the request of the individual in custody or a relative (Penal Code § 825).
- (b) Attorneys and bail bondsmen who need to interview an individual in custody should do so inside a secure interview room.
- (c) The individual in custody as well as the attorney or bail bondsman should be searched for weapons prior to being admitted to the interview room and at the conclusion of the interview.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

- (d) Attorneys must produce a current California Bar card as well as other matching appropriate identification.
- (e) Interviews between attorneys and their clients shall not be monitored or recorded (15 CCR 1068).

#### 700.5.10 DISCIPLINE

Discipline will not be administered to any individual in custody at this facility. Any individual in custody who repeatedly fails to follow directions or facility rules should be transported to the appropriate jail, mental health facility or hospital as soon as practicable. Such conduct should be documented and reported to the receiving facility (15 CCR 1081).

#### **700.6 USE OF RESTRAINT DEVICES**

Individuals in custody may be handcuffed in accordance with the Handcuffing and Restraints Policy. Unless an individual presents a heightened risk, handcuffs should generally be removed when the person is in a cell.

The use of restraints, other than handcuffs or leg irons, generally should not be used for individuals in temporary custody at the Stanislaus County District Attorney's Office unless the person presents a heightened risk, and only in compliance with the Handcuffing and Restraints Policy.

Individuals in restraints shall be kept away from other unrestrained individuals in custody and monitored to protect them from abuse.

##### 700.6.1 PREGNANT ADULTS

Adults who are known to be pregnant should be restrained in accordance with the Handcuffing and Restraints Policy.

#### **700.7 PERSONAL PROPERTY**

The personal property of an individual in temporary custody should be removed, inventoried, and processed as provided in the Custodial Searches Policy, unless the individual requests a different disposition. For example, an individual may request property (i.e., cash, car or house keys, medications) be released to another person. A request for the release of property to another person must be made in writing. Release of the property requires the recipient's signature on the appropriate form.

Upon release of an individual from temporary custody, the individual's items of personal property shall be compared with the inventory, and the individual shall sign a receipt for the property's return. If the individual is transferred to another facility or court, the member transporting the individual is required to obtain the receiving person's signature as notice of receipt. The Bureau shall maintain a copy of the property receipt.

The Lieutenant shall be notified whenever an individual alleges that there is a shortage or discrepancy regarding the individual's property. The Lieutenant shall attempt to prove or disprove the claim.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

#### **700.8 HOLDING CELLS**

A thorough inspection of a cell shall be conducted before placing an individual into the cell to ensure there are no weapons or contraband and that the cell is clean and sanitary. An inspection also should be conducted when the individual is released. Any damage noted to the cell should be photographed and documented.

The following requirements shall apply:

- (a) The individual shall be searched (see the Custodial Searches Policy), and anything that could create a security or suicide risk, such as contraband, hazardous items, belts, shoes or shoelaces, and jackets, shall be removed.
- (b) The individual shall constantly be monitored by an audio/video system during the entire custody.
- (c) The individual shall have constant auditory access to bureau members.
- (d) The individual's initial placement into and removal from a locked enclosure shall be logged.
- (e) Safety checks by bureau members shall occur no less than every 15 minutes (15 CCR 1027.5).
  - 1. Safety checks should be at varying times.
  - 2. All safety checks shall be logged.
  - 3. The safety check should involve questioning the individual as to the individual's well-being.
  - 4. Individuals who are sleeping or apparently sleeping should be awakened.
  - 5. Requests or concerns of the individual should be logged.

#### **700.8.1 USE OF SOBERING CELL**

Individuals who are to be held in the temporary holding facility and who present a threat to their own safety or the safety of others due to their state of intoxication should be placed in a sobering cell until their condition allows for continued processing.

The following guidelines apply when placing any individual in a sobering cell (15 CCR 1056):

- (a) Placement of an individual into the cell requires approval of the Lieutenant.
- (b) A cell log shall be initiated every time an individual is placed in the cell. The log shall be maintained for the entire time the individual is housed in the cell.
- (c) A safety check consisting of direct visual observation sufficient to assess the individual's well-being and behavior shall occur at least once every 30 minutes with no more than a 15-minute lapse between safety checks. Each safety check shall be documented in the cell log. Supervisors shall check the logs for completeness every two hours and document this action on the cell log.
- (d) Under no circumstances shall an individual be held in a sobering cell for more than six hours without being evaluated by qualified medical personnel to ensure that the individual does not have an urgent medical issue.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

- (e) Individuals will be removed from the cell when they no longer pose a threat to their own safety and the safety of others, and are able to continue processing.

#### **700.9 SUICIDE ATTEMPT, DEATH, OR SERIOUS INJURY**

Bureau management will ensure procedures are in place to address any suicide attempt, death, or serious injury of any individual in temporary custody at the Stanislaus County District Attorney's Office. The procedures should include the following:

- (a) Immediate request for emergency medical assistance if appropriate
- (b) Immediate notification of the Chief of the Investigation Bureau and the District Attorney
- (c) Notification of the spouse, next of kin, or other appropriate person
- (d) Notification of the appropriate prosecutor
- (e) Notification of the County Counsel
- (f) Notification of the Coroner
- (g) Evidence preservation
- (h) In-custody death review reports in compliance with 15 CCR 1046
  - 1. A copy of the initial review report of an in-custody death shall be provided to the BSCC within 60 days of the death.
- (i) Preparation of a written report to the Attorney General within 10 days of any death in custody including any reasonably known facts concerning the death (Government Code § 12525)
  - 1. A copy of the report submitted to the Attorney General shall also be submitted to the BSCC within 10 days of the death (15 CCR 1046).
  - 2. Any change or new information that becomes available after the initial reporting to the Attorney General shall be updated in the report and provided to the Attorney General within 10 days of the date of the change or the date the new information becomes available.

##### **700.9.1 IN-CUSTODY DEATH PUBLICATION**

The Chief of Investigations or the authorized designee should ensure that all specified information relating to an in-custody death is posted on the bureau website as prescribed and within the time frames provided in Penal Code § 10008.

#### **700.10 RELEASE AND/OR TRANSFER**

When an individual is released or transferred from custody, the member releasing the individual should ensure the following:

- (a) All proper reports, forms, and logs have been completed prior to release.
- (b) A check has been made to ensure that the individual is not reported as missing and does not have outstanding warrants.
- (c) It has been confirmed that the correct individual is being released or transported.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

- (d) All property, except evidence, contraband, or dangerous weapons, has been returned to, or sent with, the individual.
- (e) All pertinent documentation accompanies the individual being transported to another facility (e.g., copies of booking forms, medical records, an itemized list of the individual's property, warrant copies).
- (f) The individual is not permitted in any nonpublic areas of the Stanislaus County District Attorney's Office unless escorted by a member of the Bureau.
- (g) Any known threat or danger the individual may pose (e.g., escape risk, suicide potential, medical condition) is documented, and the documentation transported with the individual if the individual is being sent to another facility.
- (h) Transfers between facilities or other entities, such as a hospital, should be accomplished with a custodial escort of the same sex as the person being transferred to assist with the person's personal needs as reasonable.

#### **700.10.1 FORM REQUEST FOR PETITION TO SEAL RECORDS**

Upon request, a detained arrestee released from custody shall be provided with the appropriate Judicial Council forms to petition the court to have the arrest and related records sealed (Penal Code § 851.91).

The Bureau shall display the required signage that complies with Penal Code § 851.91 advising an arrestee of the right to obtain the Judicial Council forms.

#### **700.11 ASSIGNED ADMINISTRATOR**

The XXX Lieutenant will ensure any reasonably necessary supplemental procedures are in place to address the following issues (15 CCR 1029):

- (a) General security
- (b) Key control
- (c) Sanitation and maintenance
- (d) Emergency medical treatment (15 CCR 1200)
- (e) Escapes
- (f) Evacuation plans
- (g) Fire- and life-safety, including a fire suppression pre-plan as required by 15 CCR 1032
- (h) Disaster plans (e.g., natural disasters)
- (i) Building and safety code compliance
- (j) Civil and other disturbances including hostage situations
- (k) Periodic testing of emergency equipment
- (l) Emergency suspension of Title 15 regulations and notice to the BSCC as required in 15 CCR 1012
- (m) Inspections and operations reviews

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Custody of Adults*

---

- (n) Any other applicable requirements under 15 CCR 1029

Annual review and evaluation of security measures including internal and external security measures, sanitation, safety, and maintenance (15 CCR 1280).

These supplemental procedures shall be reviewed and updated no less than every two years and shall be available to all members (15 CCR 1029).

#### **700.12 TRAINING**

Bureau members should be trained and familiar with this policy and any supplemental procedures.

Bureau members responsible for supervising adults in temporary custody shall complete the Corrections Officer Core Course or eight hours of specialized training within six months of assignment. Such training shall include but not be limited to the following (15 CCR 1024):

- (a) Applicable minimum jail standards
- (b) Jail operations liability
- (c) Separation of incarcerated persons
- (d) Emergency procedures and planning, fire safety, and life safety
- (e) Suicide prevention
- (f) De-escalation
- (g) Juvenile procedures
- (h) Racial bias
- (i) Mental illness

Eight hours of refresher training shall be completed every two years (15 CCR 1024).

The Lieutenant shall maintain records of all such training in the member's training file.



# Transporting Persons in Custody

## 701.1 PURPOSE AND SCOPE

This policy provides guidelines for transporting persons who are in the custody of the Stanislaus County District Attorney's Office.

See the Handcuffing and Restraints Policy for additional guidance.

## 701.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to provide safe, secure, and humane transportation for all persons in custody.

## 701.3 TRAINING MANAGER RESPONSIBILITIES

The [Bureau Training manager should coordinate and](#) establish related procedures for:

- Safely transporting persons who have their legs restrained.
- Seating placement of persons being transported in vehicles with and without safety barriers.

## 701.4 INVESTIGATOR RESPONSIBILITIES

Persons in custody should be transported in a vehicle properly equipped to transport passengers. They should be appropriately restrained and positioned during transport.

Investigators transporting a person in custody should:

- (a) Search all areas of the vehicle accessible to a person in custody before and after each transport.
- (b) Immediately search persons in custody after arrest, when receiving the person from the custody of another investigator, and before transferring the person. Refer to the Custodial Searches Policy before conducting any search other than a field search.
  1. Whenever practicable, a search should be conducted by an investigator of the same gender as the person being searched. If an investigator of the same gender is not reasonably available, a witnessing investigator should be present during the search.
- (c) Provide SR 911 with any required notifications (e.g., start time, mileage, end time).
- (d) Properly secure all property.
- (e) Use audio/video equipment (when properly equipped) to observe and record any person in custody during transport (see the Mobile Audio/Video and Body-Worn Camera policies for additional guidance).
- (f) Make a reasonable effort to prevent inappropriate conversations between persons being transported (e.g., demeaning or insulting language) or conversations between a person being transported and someone outside the vehicle.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Transporting Persons in Custody*

---

- (g) Plan travel times and routes to avoid situations that might impede transportation (e.g., heavy traffic, unfavorable road conditions, extreme weather) when reasonably practicable.
- (h) Make a verbal welfare check with a person in custody at least every 10 minutes. Provide sufficient visual observation and audio communication during the transport of:
  - 1. Individuals in auxiliary restraints.
  - 2. Individuals in leg restraints.
  - 3. Individuals wearing a spit hood.
  - 4. Individuals who are a suspected suicide risk.
- (i) Verify that the vehicle's security devices (e.g., window and rear-door child-safety locks) are activated.
- (j) Assess uncooperative persons who cannot or will not sit upright for a medical condition (see the Medical Aid and Response Policy for additional guidance):
  - 1. If no medical condition exists, alternative transportation should be arranged (e.g., a special transport van).

#### **701.5 TRANSPORT RESTRICTIONS**

When transporting multiple persons, investigators:

- (a) Should not transport persons in custody together. Persons in custody should be transported individually when practicable, or within their own compartment of a multiple-compartment vehicle, unless supervisor approval is received based on unusual circumstances.
  - 1. Juveniles and adults shall not be transported together.
  - 2. Persons with known hostilities toward each other, such as mutual combatants or rival gang members, shall not be transported together.
  - 3. Persons of different genders should not be transported together.
- (b) If segregating individuals is not possible, transporting investigators should be alert to inappropriate physical or verbal contact and take appropriate action.

#### **701.6 TRANSPORTING PERSONS IN CUSTODY WHO HAVE A DISABILITY**

When transporting a person in custody who has a disability, a transporting investigator should request assistance as necessary to transport the person in a reasonable and safe manner. The transporting investigator should ensure that any special equipment (e.g., canes, wheelchairs, prosthetics) is transported to the person's destination in a way that does not threaten the safety or security of the person in custody or the investigator.

Investigators transporting a person who has a disability should consult with the person in custody and use good judgment in determining what, if any, restraining devices may be appropriate based on the person's disability to ensure the security, safety, and dignity of all persons.

### *Transporting Persons in Custody*

---

#### **701.7 TRANSPORTING ILL OR INJURED PERSONS IN CUSTODY**

Except in exceptional cases where alternatives are not reasonably available, investigators should not transport persons in custody who are unconscious, have serious injuries, or who may be seriously ill. EMS personnel should be called to handle such transportation.

Investigators shall notify a supervisor as soon as practicable when transporting a person in custody to a hospital.

An investigator should accompany any person in custody during transport in an ambulance when requested by EMS personnel, when it reasonably appears necessary to provide security, when it is necessary for investigative purposes, or when so directed by a Lieutenant.

Any person in custody suspected of having a communicable disease should be transported in compliance with the exposure control plan in the Communicable Diseases Policy.

See the Medical Aid and Response Policy for additional guidance on ill or injured persons in custody.

#### **701.8 TRANSPORTING PREGNANT PERSONS IN CUSTODY**

Persons in custody who are known to be pregnant should be restrained during transport in the least restrictive manner that is effective for officer safety. Leg restraints, waist chains, or handcuffs behind the body should not be used unless the investigator has a reasonable suspicion that the person may resist, attempt escape, injure themselves or others, or damage property.

Absent exceptional circumstances, persons in labor or delivery should not be transported by investigators. EMS personnel should be called to handle transportation.

#### **701.9 MENTAL ILLNESS COMMITMENT TRANSPORTS**

When transporting any individual for a mental illness commitment, the transporting investigator should request that SR 911 notify the receiving facility of the estimated time of arrival, the level of cooperation of the individual, and whether any special medical care is needed.

Should the person require transport in a medical transport vehicle, and the safety of any person, including the person in custody, requires the presence of an investigator during the transport, Lieutenant approval is required before transport commences.

See the Mental Illness Commitments Policy for additional guidance.

#### **701.10 INTERRUPTION OF TRANSPORT**

Absent extraordinary circumstances, investigators should not interrupt a transport to provide emergency assistance without supervisory approval. Investigators encountering an emergency should notify SR 911 and request an appropriate response.

#### **701.11 EXTENDED TRANSPORTS**

During transports for extended durations, transporting investigators may be required to make necessary stops. With supervisory approval and due consideration for security risks and the in-

# Stanislaus County District Attorney's Office

## Policy Manual

### *Transporting Persons in Custody*

---

custody person's health and well-being, these stops should be limited to fuel, meals, bathroom breaks, and other purposes reasonably necessary for the continuation of the transport.

#### **701.12 PROHIBITIONS**

When transporting a person in custody, investigators should not:

- (a) Use transport as a form of punishment or retaliation (e.g., intentionally rough rides, excessive heat or cold, obnoxiously loud music).
- (b) Handcuff a person to any part of a vehicle.
- (c) Leave the vehicle unattended with the person in custody in the vehicle.
- (d) Allow any person who is not in custody (e.g., friend, family member) to have contact with or be in close proximity to the person in custody.
- (e) Allow any food, drink, or other consumables to be given to the person in custody by anyone other than bureau personnel or receiving agency personnel.
- (f) Stop to conduct any personal activities.
- (g) Engage in a pursuit.

#### **701.13 ESCAPES**

In the event that a person in custody escapes while being transported, the transporting investigator should immediately advise SR 911 and other units of the escape, provide a description of the escapee, notify the Lieutenant, and submit a written report as soon as practicable describing the circumstances of the escape and any recapture.

The Lieutenant should notify the Chief of Investigations or the authorized designee upon learning of an escape.

If the escape occurs outside the jurisdiction of the Stanislaus County District Attorney's Office, the Lieutenant should notify the appropriate agency or agencies within the jurisdiction where the escape occurred.

#### **701.14 DOCUMENTATION**

If a person is injured during transportation, investigators should document the injury in the appropriate report. Documentation should include the condition of the person prior to transportation and the known or suspected causes of the injury during transportation (e.g., hitting head, struggling with restraints, fighting with other persons in custody). Any visible or reported injuries should be photographed and included with the report.

#### **701.15 NOTIFICATIONS**

Investigators should notify a supervisor and any receiving facility of information regarding any circumstances the investigator reasonably believes would be potential safety concerns or medical risks to the person (e.g., uncooperative or violent, prolonged struggle, extreme agitation, medical conditions) that may have occurred prior to, or during, transportation.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Transporting Persons in Custody*

---

#### **701.16 TRAINING**

The Lieutenant should provide periodic training on this policy and procedures related to transporting persons in custody, restraint systems, and restraint devices.

## **Chapter 8 - Personnel**

# Standards of Conduct

## 800.1 PURPOSE AND SCOPE

This policy establishes standards of conduct that are consistent with the values and mission of the Stanislaus County District Attorney's Office (SCDA) Bureau of Investigation (BI) and are expected of all BI members. The standards contained in this policy are not intended to be an exhaustive list of requirements and prohibitions but they do identify many of the important matters concerning conduct. In addition to the provisions of this policy, BI members are subject to all other provisions contained in this manual, as well as any additional guidance on conduct that may be disseminated by the SCDA or a member's supervisors.

## 800.2 POLICY

The continued employment or appointment of every member of the BI shall be based on conduct that reasonably conforms to the guidelines set forth herein. Failure to meet the guidelines set forth in this policy, whether on- or off-duty, may be cause for disciplinary action.

## 800.3 DIRECTIVES AND ORDERS

Members shall comply with lawful directives and orders from any BI supervisor or person in a position of authority, absent a reasonable and bona fide justification.

### 800.3.1 UNLAWFUL OR CONFLICTING ORDERS

Supervisors shall not knowingly issue orders or directives that, if carried out, would result in a violation of any law or office policy. Supervisors should not issue orders that conflict with any previous order without making reasonable clarification that the new order is intended to countermand the earlier order.

No member is required to obey any order that appears to be in direct conflict with any federal law, state law or local ordinance. Following a known unlawful order is not a defense and does not relieve the member from criminal or civil prosecution or administrative discipline. If the legality of an order is in doubt, the affected member shall ask the issuing supervisor to clarify the order or shall confer with a higher authority. The responsibility for refusal to obey rests with the member, who shall subsequently be required to justify the refusal.

Unless it would jeopardize the safety of any individual, members who are presented with a lawful order that is in conflict with a previous lawful order, SCDA policy or BI policy shall respectfully inform the issuing supervisor of the conflict. The issuing supervisor is responsible for either resolving the conflict or clarifying that the lawful order is intended to countermand the previous lawful order or directive, in which case the member is obliged to comply. Members who are compelled to follow a conflicting lawful order after having given the issuing supervisor the opportunity to correct the conflict, will not be held accountable for disobedience of the lawful order or directive that was initially issued.

The supervisor countermanding the original order shall notify, in writing, the person issuing the original order, indicating the action taken and the reason.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Standards of Conduct*

---

#### 800.3.2 SUPERVISOR RESPONSIBILITIES

Supervisors and managers are required to follow all policies and procedures and may be subject to discipline for:

- (a) Failure to be reasonably aware of the performance of their subordinates or to provide appropriate guidance and control.
- (b) Failure to promptly and fully report any known misconduct of a member to his/her immediate supervisor or to document such misconduct appropriately or as required by policy.
- (c) Directing a subordinate to violate a policy or directive, acquiesce to such a violation, or are indifferent to any such violation by a subordinate.
- (d) The unequal or disparate exercise of authority on the part of a supervisor toward any member for malicious or other improper purpose.

#### 800.4 GENERAL STANDARDS

Members shall conduct themselves, whether on- or off-duty, in accordance with the United States and California constitutions and all applicable laws, ordinances, and rules enacted or established pursuant to legal authority.

Members shall familiarize themselves with policies and procedures and are responsible for compliance with each. Members should seek clarification and guidance from supervisors in the event of any perceived ambiguity or uncertainty.

Discipline may be initiated for any good cause. It is not mandatory that a specific policy or rule violation be cited to sustain discipline. This policy is not intended to cover every possible type of misconduct.

#### 800.5 CAUSES FOR DISCIPLINE

The following are illustrative of causes for disciplinary action. This list is not intended to cover every possible type of misconduct and does not preclude the recommendation of disciplinary action for violation of other rules, standards, ethics and specific action or inaction that is detrimental to efficient SCDA service:

##### 800.5.1 LAWS, RULES AND ORDERS

- (a) Violation of, or ordering or instructing a subordinate to violate any policy, procedure, rule, order, directive, requirement or failure to follow instructions contained in SCDA, BI or Stanislaus County manuals.
- (b) Disobedience of any legal directive or order issued by any SCDA member of a higher rank.
- (c) Violation of federal, state, local or administrative laws, rules or regulations.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Standards of Conduct*

---

#### 800.5.2 ETHICS

- (a) Using or disclosing one's status as a member of the SCDA in any way that could reasonably be perceived as an attempt to gain influence or authority for non SCDA business or activity.
- (b) The wrongful or unlawful exercise of authority on the part of any member for malicious purpose, personal gain, willful deceit or any other improper purpose.
- (c) The receipt or acceptance of a reward, fee or gift from any person for service incident to the performance of the member's duties (lawful subpoena fees and authorized work permits excepted).
- (d) Acceptance of fees, gifts or money contrary to the rules of the SCDA and/or laws of the state.
- (e) Offer or acceptance of a bribe or gratuity.
- (f) Misappropriation or misuse of public funds, property, personnel or services.
- (g) Any other failure to abide by the standards of ethical conduct.

#### 800.5.3 DISCRIMINATION, OPPRESSION, OR FAVORITISM

Unless required by law or policy, discriminating against, oppressing, or providing favoritism to any person because of actual or perceived characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, economic status, cultural group, veteran status, marital status, and any other classification or status protected by law, or intentionally denying or impeding another in the exercise or enjoyment of any right, privilege, power, or immunity, knowing the conduct is unlawful.

#### 800.5.4 RELATIONSHIPS

- (a) Unwelcome solicitation of a personal or sexual relationship while on duty or through the use of one's official capacity.
- (b) Engaging in on-duty sexual activity, including but not limited to sexual intercourse, excessive displays of public affection, or other sexual contact.
- (c) Establishing or maintaining an inappropriate personal or financial relationship, as a result of an investigation, with a known victim, witness, suspect, or defendant while a case is being investigated or prosecuted, or as a direct result of any official contact.
- (d) Associating with or joining a criminal gang, organized crime, and/or criminal syndicate when the member knows or reasonably should know of the criminal nature of the organization. This includes any organization involved in a definable criminal activity or enterprise, except as specifically directed and authorized by this bureau.
- (e) Associating on a personal, rather than official basis with persons who demonstrate recurring involvement in serious violations of state or federal laws after the member knows, or reasonably should know of such criminal activities, except as specifically directed and authorized by this bureau.
- (f) Participation in a law enforcement gang as defined by Penal Code § 13670. Participation is grounds for termination (Penal Code § 13670).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Standards of Conduct*

---

#### 800.5.5 ATTENDANCE

- (a) Leaving the job to which the member is assigned during duty hours without reasonable excuse and proper permission and approval.
- (b) Unexcused or unauthorized absence or tardiness.
- (c) Excessive absenteeism or abuse of leave privileges.
- (d) Failure to report to work or to the place of assignment at the time specified and fully prepared to perform duties without reasonable excuse.

#### 800.5.6 UNAUTHORIZED ACCESS, DISCLOSURE, OR USE

- (a) Unauthorized and inappropriate intentional release of confidential or protected information, materials, data, forms, or reports obtained as a result of the member's position with this bureau.
  - (a) Members of this bureau shall not disclose the name, address, or image of any victim of human trafficking except as authorized by law (Penal Code § 293).
- (b) Disclosing to any unauthorized person any active investigation information.
- (c) The use of any information, photograph, video, or other recording obtained or accessed as a result of employment or appointment to this bureau for personal or financial gain or without the express authorization of the Chief of Investigations or the authorized designee.
- (d) Loaning, selling, allowing unauthorized use, giving away, or appropriating any bureau property for personal use, personal gain, or any other improper or unauthorized use or purpose.
- (e) Using bureau resources in association with any portion of an independent civil action. These resources include but are not limited to personnel, vehicles, equipment, and nonsubpoenaed records.

#### 800.5.7 EFFICIENCY

- (a) Neglect of duty.
- (b) Unsatisfactory work performance including but not limited to failure, incompetence, inefficiency, or delay in performing and/or carrying out proper orders, work assignments, or the instructions of supervisors without a reasonable and bona fide excuse.
- (c) Concealing, attempting to conceal, removing, or destroying defective or incompetent work.
- (d) Unauthorized sleeping during on-duty time or assignments.
- (e) Failure to notify the Bureau within 24 hours of any change in residence address or contact numbers.
- (f) Failure to notify the Human Resources of changes in relevant personal information (e.g., information associated with benefits determination) in a timely fashion.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Standards of Conduct*

---

#### 800.5.8 PERFORMANCE

- (a) Failure to disclose or misrepresenting material facts, or making any false or misleading statement on any application, examination form, or other official document, report or form, or during the course of any workrelated investigation.
- (b) The falsification of any work-related records, making misleading entries or statements with the intent to deceive or the willful and unauthorized removal, alteration, destruction and/or mutilation of any SCDA record, public record, paper or document.
- (c) Failure to participate in, or giving false or misleading statements, or misrepresenting or omitting material information to a supervisor or other person in a position of authority, in connection with any investigation or in the reporting of any SCDA related business.
- (d) Being untruthful or knowingly making false, misleading or malicious statements that are reasonably calculated to harm the reputation, authority or official standing of the SCDA or its members.
- (e) Disparaging remarks or conduct concerning duly constituted authority to the extent that such conduct disrupts the efficiency of the SCDA or subverts the good order, efficiency and discipline of the SCDA or that would tend to discredit any of its members.
- (f) Unlawful gambling or unlawful betting at any time or any place. Legal gambling or betting under any of the following conditions:
  - (a) While on SCDA premises.
  - (b) At any work site, while onduty or while in uniform, or while using any SCDA equipment or system.
  - (c) Gambling activity undertaken as part of BI official duties and with the express knowledge and permission of a direct supervisor is exempt from this prohibition.
- (g) Improper political activity including:
  - (a) Unauthorized attendance while onduty at official legislative or political sessions.
  - (b) Solicitations, speeches or distribution of campaign literature for or against any political candidate or position while onduty or, on SCDA property except as expressly authorized by Stanislaus County policy, the memorandum of understanding, or the District Attorney.
- (h) Engaging in political activities during assigned working hours except as expressly authorized by Stanislaus County policy, the memorandum of understanding, or the District Attorney.
- (i) Any act on or offduty that brings discredit to the SCDA.

#### 800.5.9 CONDUCT

- (a) Failure of any member to promptly and fully report activities on his/her part or the part of any other member where such activities resulted in contact with any other law enforcement agency or that may result in criminal prosecution or discipline under this policy.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Standards of Conduct*

---

- (b) Unreasonable and unwarranted force to a person encountered or a person under arrest.
- (c) Exceeding lawful peace officer powers by unreasonable, unlawful or excessive conduct.
- (d) Unauthorized or unlawful fighting, threatening or attempting to inflict unlawful bodily harm on another.
- (e) Engaging in horseplay that reasonably could result in injury or property damage.
- (f) Discourteous, disrespectful or discriminatory treatment of any member of the public or any member of the SCDA.
- (g) Use of obscene, indecent, profane or derogatory language while on duty.
- (h) Criminal, dishonest, or disgraceful conduct, whether on- or off-duty, that adversely affects the member's relationship with the SCDA.
- (i) Unauthorized possession of, loss of, or damage to SCDA property or the property of others, or endangering it through carelessness or maliciousness.
- (j) Attempted or actual theft of SCDA property; misappropriation or misuse of public funds, property, personnel or the services or property of others; unauthorized removal or possession of SCDA property or the property of another person.
- (k) Activity that is incompatible with a member's conditions of employment or appointment as established by law or that violates a provision of any memorandum of understanding or contract to include fraud in securing the appointment or hire.
- (l) Initiating any civil action for recovery of any damages or injuries incurred in the course and scope of employment or appointment without first notifying the Chief Investigator of such action.
- (m) Any other on or off duty conduct which any member knows or reasonably should know is unbecoming a member of the SCDA, is contrary to good order, efficiency or morale, or tends to reflect unfavorably upon the SCDA or its members.

#### 800.5.10 SAFETY

- (a) Failure to observe or violating SCDA safety standards or safe working practices.
- (b) Failure to maintain current licenses or certifications required for the assignment or position (e.g., driver license, first aid).
- (c) Unsafe firearm or other dangerous weapon handling to include loading or unloading firearms in an unsafe manner, either on- or off- duty.
- (d) Carrying, while on the premises of the work place, any firearm or other lethal weapon that is not authorized by the member's appointing authority.
- (e) Unsafe or improper driving habits or actions in the course of employment or appointment.
- (f) Any personal action contributing to a preventable traffic collision.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Standards of Conduct*

---

- (g) Concealing or knowingly failing to report any on-the-job or work-related accident or injury as soon as practicable but within 24 hours.

#### 800.5.11 INTOXICANTS

- (a) Reporting for work or being at work while intoxicated or when the member's ability to perform assigned duties is impaired due to the use of alcohol, medication or drugs, whether legal, prescribed or illegal.
- (b) Possession or use of alcohol at any work site or while on-duty, except as authorized in the performance of an official assignment. A member who is authorized to consume alcohol is not permitted to do so to such a degree that it may impair on-duty performance.
- (c) Unauthorized possession, use of, or attempting to bring a controlled substance, illegal drug or non-prescribed medication to any work site.

# Evaluation of Employees

## 801.1 PURPOSE AND SCOPE

The Bureau's employee performance evaluation system is designed to record work performance for both the Bureau and the employee, providing recognition for good work and developing a guide for improvement.

## 801.2 POLICY

The Stanislaus County District Attorney's Office utilizes a performance evaluation report to measure performance and to use as a factor in making personnel decisions that relate to merit increases, promotion, reassignment, discipline, demotion, and termination. The evaluation report is intended to serve as a guide for work planning and review by the supervisor and employee. It gives supervisors a way to create an objective history of work performance based on job standards.

The Bureau evaluates employees in a non-discriminatory manner based upon job-related factors specific to the employee's position, without regard to actual or perceived race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, pregnancy, genetic information, veteran status, marital status, and any other classification or status protected by law.

## 801.3 EVALUATION PROCESS

Annual evaluation reports will cover a specific period of time and should be based on documented performance during that period. Evaluation reports will be completed by each employee's immediate supervisor or manager. Other supervisors and managers directly familiar with the employee's performance during the rating period should be consulted for their input.

Each supervisor or manager should discuss the tasks of the position, standards of performance expected and the evaluation criteria with each employee at the beginning of the rating period. Supervisors should document this discussion in the prescribed manner.

Assessment of an employee's job performance is an ongoing process. Continued coaching and feedback provides supervisors and employees with opportunities to correct performance issues as they arise.

Non-probationary employees demonstrating unsatisfactory performance shall be notified as soon as possible in order to have an opportunity to remediate the issues. Such notification should occur at the earliest opportunity when identified, with the goal being a minimum of 90 days prior to the end of the evaluation period. The supervisor or manager shall document the notification and monitor the the employee progress before completion of the annual performance evaluation.

Employees who disagree with their evaluation and who desire to provide a formal response or a rebuttal may do so in writing within 30 days of receiving their evaluation. A formal response or rebuttal shall be signed by the employee and submitted to their direct supervisor or manager. The Chief Investigator will review all Bureau employee performance evaluations as well as any rebuttal

# Stanislaus County District Attorney's Office

## Policy Manual

### *Evaluation of Employees*

---

and make a final determination regarding any necessary changes to the employee performance evaluation. Rebuttals, regardless of any changes to the employee performance evaluation, shall be attached to and accompany the employee performance evaluation and will be a permanent employee record with Human Resources.

#### 801.3.1 PART-TIME AND CONTRACT EMPLOYEES

**Part-Time Employees** - Bureau members who work 2,080 hours or more in a calendar year are entitled to a pay increase review by their supervisor and manager. The review will be conducted by utilizing an employee performance evaluation and shall be submitted through the chain of command to Human Resources.

**Contract Employees** - Contract employees are not entitled to a documented employee performance evaluation.

#### 801.4 FULL TIME PROBATIONARY PERSONNEL

Non-Sworn and Sworn personnel are on probation for 12 months before being eligible for certification as permanent employees. Probationary employees receive an end of probation employee performance evaluation and are evaluated daily throughout their probationary period.

If the employee work performance has shown progress but has not meet satisfactory performance standards, the Chief Investigator may extend the employee's probationary period six months. At the completion of this extension, the supervisor or manager will complete an additional end of probation evaluation that will cover the work performance performed during the extension.

#### 801.5 FULL-TIME PERMANENT STATUS PERSONNEL

Permanent employees are subject to two types of performance evaluations:

**Regular** - An Employee Performance Evaluation shall be completed once each year by the employee's immediate supervisor or manager on the anniversary of the employee's date of hire except for employees who have been promoted in which case an Employee Performance Evaluation shall be completed on the anniversary of the employee's date of last promotion.

**Performance Improvement Plan (PIP)** - A PIP is a systematic documented approach to correct and improve unacceptable or unsatisfactory performance or behavior. Supervisors or managers will work with an employee ensuring performance standards are understood as well as provide a vision and a path to success. Supervisors or managers will meet with the employee regularly to discuss their work performance as well as provide an opportunity for positive reinforcement and additional training. At the completion of the PIP, the supervisor or manager will provide documented recommendations to the Chief Investigator.

##### 801.5.1 RATINGS

When completing the Employee Performance Evaluation, the rater will place a check mark in the column that best describes the employee's performance. The definition of each rating category is as follows:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Evaluation of Employees*

---

**Outstanding** -The employee consistently performs at a level above others and far exceeds expectations.

**Excellent** - The employee is looked up to by his / her peers and other in the community. The employee consistently performs at a level above the performance work elements.

**Satisfactory** - The employee is doing all that is expected and required. His / her value to the organization is what makes the organization what it should be. The employee consistently performs at a level that meets all the department's work elements for the assignment.

**Needs Improvement** -The employee needs to improve certain areas to meet the expected and required standards.

**Unsatisfactory** - The employee is not meeting expected and required standards.

Space for written comments is provided throughout the evaluation. This allows the rater to document the employee's strengths, weaknesses, and suggestions for improvement. Any rating under any job dimension marked unsatisfactory or outstanding shall be substantiated in the rater comments section.

#### **801.6 EVALUATION INTERVIEW**

The supervisor or manager shall forward the completed the preliminary evaluation to the Chief Investigator for review and signage. After the Chief Investigator has reviewed and signed the employee evaluation, the supervisor or manager will make arrangements for a private discussion about the evaluation with the employee. The supervisor should discuss the results of the completed rating period and clarify any questions the employee may have. If the employee has valid and reasonable protests of any of the ratings, the supervisor may make appropriate changes to the evaluation. Areas needing improvement and goals for reaching the expected level of performance should be identified and discussed. The supervisor should also provide relevant counseling regarding advancement, specialty positions and training opportunities. The supervisor and employee will sign and date the evaluation. Permanent employees may also write comments in the Employee Comments section of the performance evaluation report.

#### **801.7 EVALUATION DISTRIBUTION**

The original performance evaluation shall be maintained by Human Resources in the employee's personnel file in the office for the tenure of the employee's employment. The supervisor or manager may maintain a copy of the performance evaluation and a copy will be provided to the employee.



## Recruitment and Selection

### 803.1 PURPOSE AND SCOPE

This policy provides a framework for peace officer recruiting efforts and identifying job-related standards for the selection process. This policy supplements the rules that govern employment practices for the Stanislaus County District Attorney's Office and that are promulgated and maintained by the Human Resources.

### 803.2 POLICY

In accordance with applicable federal, state, and local law, the Stanislaus County District Attorney's Office provides equal opportunities for applicants and employees regardless of actual or perceived race, ethnicity, national origin, religion, sex, sexual orientation, gender identity or expression, age, disability, pregnancy, genetic information, veteran status, marital status, and any other classification or status protected by law. The Bureau does not show partiality or grant any special status to any applicant, employee, or group of employees unless otherwise required by law.

The Bureau will recruit and hire only those individuals who demonstrate a commitment to service and who possess the traits and characteristics that reflect personal integrity and high ethical standards.

### 803.3 SELECTION PROCESS

The Bureau shall actively strive to identify a diverse group of candidates who have in some manner distinguished themselves as being outstanding prospects. Minimally, the Bureau shall employ a comprehensive screening, background investigation, and selection process that assesses cognitive and physical abilities and includes review and verification of the following:

- (a) A comprehensive application for employment (including previous employment, references, current and prior addresses, education, military record)
  - 1. The personnel records of any applicant with prior peace officer experience in this state shall be requested from the appropriate law enforcement agency and reviewed prior to extending an offer of employment (Penal Code § 832.12).
  - 2. This includes review of prior law enforcement employment information maintained by POST (Penal Code § 13510.9).
- (b) Driving record
- (c) Personal and professional reference checks
- (d) Employment eligibility, including U.S. Citizenship and Immigration Services (USCIS) Employment Eligibility Verification Form I-9 and acceptable identity and employment authorization documents consistent with Labor Code § 1019.1. This required documentation should not be requested until a candidate is hired. This does not prohibit obtaining documents required for other purposes.
- (e) Information obtained from public internet sites

# Stanislaus County District Attorney's Office

## Policy Manual

### *Recruitment and Selection*

---

1. This review should include the identification of any activity that promotes or supports unlawful violence or unlawful bias against persons based on protected characteristics (e.g., race, ethnicity, national origin, religion, gender, gender identity, sexual orientation, disability).
- (f) Financial history consistent with the Fair Credit Reporting Act (FCRA) (15 USC § 1681 et seq.)
- (g) Local, state, and federal criminal history record checks
- (h) Lie detector test (when legally permissible) (Labor Code § 432.2)
- (i) Medical and psychological examination (may only be given after a conditional offer of employment)
  1. The Medical Suitability Declaration (POST form 2-363) provided by the evaluating physician shall be maintained in the candidate's background investigation file (11 CCR 1954).
  2. The Psychological Suitability Declaration (POST form 2-364) provided by the evaluator shall be maintained in the candidate's background investigation file (11 CCR 1955).
- (j) Review board or selection committee assessment
- (k) Relevant national and state decertification records, if available, including the National Decertification Index

#### **803.4 BACKGROUND INVESTIGATION**

Every candidate shall undergo a thorough background investigation to verify his/her personal integrity and high ethical standards, and to identify any past behavior that may be indicative of the candidate's unsuitability to perform duties relevant to the operation of the Stanislaus County District Attorney's Office (11 CCR 1953).

The narrative report and any other relevant background information shall be shared with the psychological evaluator. Information shall also be shared with others involved in the hiring process if it is relevant to their respective evaluations (11 CCR 1953).

##### **803.4.1 BACKGROUND INVESTIGATION UPDATE**

A background investigation update may, at the discretion of the Chief of Investigations, be conducted in lieu of a complete new background investigation on a peace officer candidate who is reappointed within 180 days of voluntary separation from the Stanislaus County District Attorney's Office, or who is an interim police chief meeting the requirements contained in 11 CCR 1953(f).

##### **803.4.2 NOTICES**

Background investigators shall ensure that investigations are conducted and notices provided in accordance with the requirements of the FCRA and the California Investigative Consumer Reporting Agencies Act (15 USC § 1681d; Civil Code § 1786.16).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Recruitment and Selection*

---

#### 803.4.3 STATE NOTICES

If information disclosed in a candidate's criminal offender record information (CORI) is the basis for an adverse employment decision, a copy of the CORI shall be provided to the applicant (Penal Code § 11105).

#### 803.4.4 REVIEW OF SOCIAL MEDIA SITES

All peace officer candidates shall be subject to a social media search for statements, postings, and/or endorsements made by the candidate that are relevant to suitability for peace officer employment, including bias-relevant information consistent with the requirements of 11 CCR 1955(d)(3) and any public expression of hate made in an online forum, as defined in Penal Code § 13680(g) (11 CCR 1953(e)(12)).

Due to the potential for accessing unsubstantiated, private, or protected information, the Office of the District Attorney Lieutenant shall not require candidates to provide passwords, account information, or access to password-protected social media accounts (Labor Code § 980).

The Office of the District Attorney Lieutenant should consider utilizing the services of an appropriately trained and experienced third party to conduct open source, internet-based searches, and/or review information from social media sites to ensure that:

- (a) The legal rights of candidates are protected.
- (b) Material and information to be considered are verified, accurate, and validated.
- (c) The Bureau fully complies with applicable privacy protections and local, state, and federal law.

Regardless of whether a third party is used, the Office of the District Attorney Lieutenant should ensure that potentially impermissible information is not available to any person involved in the candidate selection process.

#### 803.4.5 DOCUMENTING AND REPORTING

The background investigator shall summarize the results of the background investigation in a narrative report that includes sufficient information to allow the reviewing authority to decide whether to extend a conditional offer of employment. The report shall include sections that summarize relevant Background Investigation Dimensions and include any findings of behaviors, traits, and/or attributes relevant to bias per the Bias Assessment Framework as described in the POST Background Investigation Manual. The report shall identify the data sources reviewed for the findings, regardless of weight given. The report shall include narrative information in the format described in 11 CCR 1953(g)(1). The report shall also include whether the candidate has engaged or is engaging in membership in a hate group, participation in hate group activity, or advocacy or public expressions of hate, pursuant to Penal Code § 13680 et seq. (11 CCR 1953).

The report shall not include any information that is prohibited from use, including that from social media sites, in making employment decisions. The report and all supporting documentation including relevant documentation of bias-related findings and documentation obtained through the

# Stanislaus County District Attorney's Office

## Policy Manual

### *Recruitment and Selection*

---

social media search shall be included in the candidate's background investigation file (11 CCR 1953).

The Lieutenant overseeing background investigations, or their designee, shall document proof of verification of qualification for peace officer appointment on the Verification of Qualification for Peace Officer Appointment form and will submit it to POST (11 CCR 1953).

The background investigation file shall be made available during POST compliance inspections (11 CCR 1953).

#### **803.4.6 RECORDS RETENTION**

The background report and all supporting documentation shall be maintained according to the established records retention schedule and at a minimum as follows (Government Code § 12946; 11 CCR 1953):

- (a) Reports and documentation for candidates hired by the Bureau shall be retained for the entire term of employment and a for a minimum of four years after separation from the Bureau.
- (b) Reports and documentation for candidates not hired by the Bureau for a minimum of four years.

#### **803.4.7 INVESTIGATOR TRAINING**

Bureau investigators assigned to complete peace officer background investigations shall complete POST-certified background investigation training prior to conducting investigations (11 CCR 1953; 11 CCR 1959).

#### **803.4.8 CONFIDENTIAL POST RECORDS**

Records released to the Bureau from POST that were previously withheld from the candidate by POST shall be kept confidential as provided in Penal Code § 13510.9.

### **803.5 DISQUALIFICATION GUIDELINES**

As a general rule, performance indicators and candidate information and records shall be evaluated by considering the candidate as a whole, and taking into consideration the following:

- Age at the time the behavior occurred
- Passage of time
- Patterns of past behavior
- Severity of behavior
- Probable consequences if past behavior is repeated or made public
- Likelihood of recurrence
- Relevance of past behavior to public safety employment
- Aggravating and mitigating factors
- Other relevant considerations

# Stanislaus County District Attorney's Office

## Policy Manual

### *Recruitment and Selection*

---

A candidate's qualifications will be assessed on a case-by-case basis, using a totality-of-the-circumstances framework.

#### **803.6 EMPLOYMENT STANDARDS**

All candidates shall meet the minimum standards required by state law (Government Code § 1029; Government Code § 1031; Penal Code § 13510.1; 11 CCR 1950 et seq.). Candidates will be evaluated based on merit, ability, competence, and experience, in accordance with the high standards of integrity and ethics valued by the Bureau and the community. The California Commission on Peace Officer Standards and Training (POST) developed a Job Dimensions list, which is used as a professional standard in background investigations.

Validated, job-related, and nondiscriminatory employment standards shall be established for each job classification and shall minimally identify the training, abilities, knowledge, and skills required to perform the position's essential duties in a satisfactory manner. Each standard should include performance indicators for candidate evaluation. The Human Resources should maintain validated standards for all positions.

##### **803.6.1 STANDARDS FOR CRIMINAL INVESTIGATORS**

Candidates shall meet the minimum standards established by POST or required by state law (Government Code § 1029; Government Code § 1031; 11 CCR 1950 et seq.):

- (a) Free of any felony convictions
- (b) Be legally authorized to work in the United States under federal law
- (c) At least 21 years of age except as provided by Government Code § 1031.4
- (d) Fingerprinted for local, state, and national fingerprint check
- (e) Good moral character as determined by a thorough background investigation (11 CCR 1953)
- (f) High school graduate, passed the GED or other high school equivalency test, or obtained a two-year, four-year, or advanced degree from an accredited or approved institution
- (g) Free from any physical, emotional, or mental condition, including bias against race or ethnicity, gender, nationality, religion, disability, or sexual orientation which might adversely affect the exercise of police powers (11 CCR 1954; 11 CCR 1955)
- (h) Free of hate group memberships, participation in hate group activities, or advocacy of public expressions of hate within the previous seven years, and since 18 years of age, as determined by a background investigation (Penal Code § 13681)
- (i) Candidates must also satisfy the POST selection requirements, including (11 CCR 1950 et seq.):
  - 1. Reading and writing ability assessment (11 CCR 1951)
  - 2. Oral interview to determine suitability for law enforcement service (11 CCR 1952)

# Stanislaus County District Attorney's Office

## Policy Manual

### *Recruitment and Selection*

---

- (j) POST certification that has not been revoked, denied, or voluntarily surrendered pursuant to Penal Code § 13510.8(f)
- (k) Not identified in the National Decertification Index of the International Association of Directors of Law Enforcement Standards and Training or similar federal government database that reflects revoked certification for misconduct or reflects misconduct that would result in a revoked certification in California.

In addition to the above minimum POST required standards, candidates may be subjected to additional standards established by the Bureau (Penal Code § 13510(d)).

#### **803.7 PROBATIONARY PERIODS**

The Office of the District Attorney Chief Investigator or designee should coordinate with the Stanislaus Human Resources to identify positions subject to probationary periods and procedures for:

- (a) Appraising performance during probation.
- (b) Assessing the level of performance required to complete probation.
- (c) Extending probation.
- (d) Documenting successful or unsuccessful completion of probation.

## Pre-employment Background Investigation

### 804.1 PURPOSE AND SCOPE

It is the policy of the District Attorney's Office to only employ people who are of high moral character and have proven to be truthful, reliable, and responsible. The object of the pre-employment background investigation is to ensure that only the highest quality applicants are offered positions within the District Attorney's Office.

This manual shall be used as a guide for conducting pre-employment background investigations for employees of the Stanislaus County District Attorney. Backgrounds on applicants for peace officer positions shall be conducted in accordance with the standards contained in the Commission on Peace Officer Standards and Training (POST) Background Manual. This manual will be a supplement to the POST manual on peace officer applicants. If there is a conflict between the two manuals for peace officer applicants, the POST manual will prevail.

### 804.2 PERSONAL HISTORY STATEMENT

After the job interview the candidates who have been selected to proceed further with the employment process will be provided with a copy of the Personal History Statement by the Human Resources Manager or designee. All Personal History Statements will be provided to the applicant by the Human Resources Manager via eSOPH which is the department's background investigation software. The applicant will be given a link/password to fill out all of the questionnaires and upload all required documents.

#### 804.2.1 PROVIDING THE PHS TO THE APPLICANT

The applicant shall be admonished that every statement listed on the Personal History Statement will be verified and the applicant should be sure to fill out the document completely. The applicant should be advised that failure to follow these directions will result in delays in the hiring process and could disqualify them from further consideration for employment.

#### 804.2.2 RECEIVING THE PHS FROM THE APPLICANT

The applicant shall be instructed to submit the completed Personal History Statement to eSOPH when it's completed and all required documents have been uploaded.

The Investigations Administration Lieutenant will check the Personal History Statement for completeness, and ensure that copies of all requested supporting documents have been provided and that all of the waiver forms have been properly signed/notarized by the applicant. If the Investigations Lieutenant finds problems with the Personal History Statement they can contact the applicant directly to correct the problems. If the applicant does not respond to these requests, the Investigations Lieutenant will work with the Human Resources Manager to make contact with the applicant or disqualify them from the process.

#### 804.2.3 PROVIDING PHS TO MORE APPLICANTS THAN YOU HAVE POSITIONS

In some cases, the Human Resources Manager may hand out Personal History Statements to more people than they have positions to fill. In the event the Human Resources Manager does

# Stanislaus County District Attorney's Office

## Policy Manual

### *Pre-employment Background Investigation*

---

this, the Human Resources Manager must coordinate with the Investigations Division to ensure that background investigations will only be conducted on the person that is intended to be hired first. If that person fails the background process the background investigation on the next person on the list can be conducted.

We should avoid conducting simultaneous background investigations on more applicants than we have open positions for. In the event a supervisor feels it is necessary to conduct more than one background investigation for a position, that supervisor will notify a supervisor in the Investigations Division of this request.

#### **804.3 LIVESCAN FINGERPRING CHECKS AND DRUG SCREENING**

California Code of Regulations Title 11, Division 1, Chapter 7, Article 1, Sections 700 through 707 requires that DOJ and FBI fingerprint checks be done on any employee who has access to any Criminal Offender Record Information (CORI) which comes off of a CLETS terminal. This does not mean that a person must have a password and access to the terminal itself, only information from the terminal. Files throughout the DA's Office can and do contain CORI information. Because of this, all full time, part time or contract employees working within the DA's office must at the very least have had a DOJ and FBI fingerprint check completed.

We currently contract with the Stanislaus County Sheriff's Office for conducting "LiveScan" fingerprint checks on prospective employees of the District Attorney's Office. All employees shall have completed the LiveScan fingerprint check and the results returned to the District Attorney's Office prior to beginning employment with this office.

The LiveScan fingerprint forms and instructions to the applicant shall be maintained by the Human Resources Manager. Drug screening will be coordinated by the Human Resources Manager after the livescan of the applicant has been completed or at the completion of the entire background investigation.

#### **804.4 BACKGROUND INVESTIGATION PROCEDURES**

Background investigations are complex and detail oriented investigations. Each position classification that must be investigated falls into a category known as a "Level". Each level may require more detail/investigation than another level. For example, a high school volunteer is considered a Level I background and is the lowest level of investigation. A criminal Investigator on the other hand is a Level IV background and requires the highest level of investigation and adherence to POST standards. Below is a hyperlink for investigators handling background investigations to refer to for each level of background investigation and the nuances that individual cases may uncover. [See attachment:](#)

[Background Procedures 2025 nrt.pdf](#)



## Special Assignments and Promotions

### 805.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for promotions and for making special assignments within the Stanislaus County District Attorney's Office, Bureau of Investigation.

### 805.2 POLICY

There are a variety of assignments within the Bureau of Investigation. Assignments and promotions are determined in a non-discriminatory manner based upon job-related factors, candidate skills, and qualifications. Assignments and promotions are made by the Chief of Investigations and the District Attorney.

### 805.3 SPECIAL ASSIGNMENT POSITIONS

The following positions are considered special assignments and not promotions:

- (a) Federal Bureau of Investigation (FBI) Task Force Officer
  - 1. Central Valley Gang Impact Task Force (CVGIT)
  - 2. Real Estate Fraud (REF) and Public Corruption (PC)
- (b) Bureau of Alcohol, Tobacco, Firearms, and Explosives (BATFE)
- (c) Fire Investigations Unit (FIU)
- (d) Special Investigations Unit (SIU)
- (e) Stanislaus County Auto Theft Task Force (STANCATT)
- (f) Cold Case Investigation
- (g) Special Victims, Domestic Violence, and Child Abduction Unit
- (h) Witness Location Unit
- (i) Bail Forfeitures

#### 805.3.1 GENERAL REQUIREMENTS

Historically, the Stanislaus County District Attorney's Office does not hire new peace officer recruits from the basic police academy. Bureau Criminal Investigators often have a tremendous amount of law enforcement experience gained from working at other law enforcement agencies in a variety of assignments. These assignments range from basic detective work, homicide, internal affairs, special victims investigations, officer involved shooting investigations, and large scale drug and firearms investigations. The following requirements should be considered when selecting a candidate for a special assignment:

- (a) Level and length of relevant experience
- (b) Past two year performance evaluation review
- (c) Possession of or ability to obtain any certification required by POST or law
- (d) Exceptional skills, experience, or abilities related to the special assignment

# Stanislaus County District Attorney's Office

## Policy Manual

### *Special Assignments and Promotions*

---

- (e) Adaptability to meet the needs of the assignment and scheduling.

#### **805.3.2 SELECTION PROCESS**

The selection process for special assignments will include:

- (a) When a vacancy exists or is expected, the Lieutenant overseeing that assignment will advertise the vacancy and request a memorandum of interest from anyone interested in the assignment.
- (b) The Lieutenant overseeing the assignment may schedule interviews with each Criminal Investigator interested. Outside agency supervisors assigned to the unit should be afforded an opportunity to participate with the interview and make recommendations as necessary.
  - 1. Based on the a review of the general requirements outlined above, the Lieutenant will provide his/her recommendations to the Chief of Investigations.
- (c) Assignment by the Chief of Investigations.

The selection process for all special assignment positions may be waived for the following:

- (a) Temporary assignments
- (b) Emergency situations
- (c) Training needs
- (d) Discretion of the Chief of Investigations.

#### **805.4 PROMOTIONAL REQUIREMENTS**

Requirements and information regarding any promotional process are available at the Stanislaus County Human Resources and the through the Stanislaus County District Attorney's HR/Business Manager.

# Grievance Procedure

## 806.1 PURPOSE AND SCOPE

The following is the County procedure for settling grievances. Exceptions to this procedure, which provided for Binding Arbitration, exist in a number of Memoranda of Understanding (MOU). Please refer to applicable MOU or check with the Personnel Department if there are questions.

It is the policy of this bureau that all grievances be handled quickly and fairly without discrimination against employees who file a grievance whether or not there is a basis for the grievance. Our Bureau's philosophy is to promote a free verbal communication between employees and supervisors. It is the intent of this policy to provide orderly and equitable procedures for the presentation and resolution of misunderstandings and disputes between the County and its employees. It is further intended that the exercises of these rights in good faith be available to all County employees, (except as herein provided) without fear of reprisal or coercion.

[See attachment: Complaint and Grievance Procedure.pdf](#)

## Anti-Retaliation

### 807.1 PURPOSE AND SCOPE

This policy prohibits retaliation against members who identify workplace issues, such as fraud, waste, abuse of authority, gross mismanagement or any inappropriate conduct or practices, including violations that may pose a threat to the health, safety or well-being of members.

This policy does not prohibit actions taken for nondiscriminatory or non-retaliatory reasons, such as discipline for cause.

These guidelines are intended to supplement and not limit members' access to other applicable remedies. Nothing in this policy shall diminish the rights or remedies of a member pursuant to any applicable federal law, provision of the U.S. Constitution, law, ordinance or memorandum of understanding.

### 807.2 POLICY

The Stanislaus County District Attorney's Office has a zero tolerance for retaliation and is committed to taking reasonable steps to protect from retaliation members who, in good faith, engage in permitted behavior or who report or participate in the reporting or investigation of workplace issues. All complaints of retaliation will be taken seriously and will be promptly and appropriately investigated.

### 807.3 RETALIATION PROHIBITED

No member may retaliate against any person for engaging in lawful or otherwise permitted behavior; for opposing a practice believed to be unlawful, unethical, discriminatory or retaliatory; for reporting or making a complaint under this policy; or for participating in any investigation related to a complaint under this or any other policy.

Retaliation includes any adverse action or conduct, including but not limited to:

- Refusing to hire or denying a promotion.
- Extending the probationary period.
- Unjustified reassignment of duties or change of work schedule.
- Real or implied threats or other forms of intimidation to dissuade the reporting of wrongdoing or filing of a complaint, or as a consequence of having reported or participated in protected activity.
- Taking unwarranted disciplinary action.
- Spreading rumors about the person filing the complaint or about the alleged wrongdoing.
- Shunning or unreasonably avoiding a person because he/she has engaged in protected activity.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Anti-Retaliation*

---

#### 807.3.1 RETALIATION PROHIBITED FOR REPORTING VIOLATIONS

An investigator shall not be retaliated against for reporting a suspected violation of a law or regulation of another investigator to a supervisor or other person in the Bureau who has the authority to investigate the violation (Government Code § 7286(b)).

#### 807.4 COMPLAINTS OF RETALIATION

Any member who feels he/she has been retaliated against in violation of this policy should promptly report the matter to any supervisor, command staff member, Chief of Investigations or the County Personnel Manager.

Members shall act in good faith, not engage in unwarranted reporting of trivial or minor deviations or transgressions, and make reasonable efforts to verify facts before making any complaint in order to avoid baseless allegations. Members shall not report or state an intention to report information or an allegation knowing it to be false, with willful or reckless disregard for the truth or falsity of the information or otherwise act in bad faith.

Investigations are generally more effective when the identity of the reporting member is known, thereby allowing investigators to obtain additional information from the reporting member. However, complaints may be made anonymously. All reasonable efforts shall be made to protect the reporting member's identity. However, confidential information may be disclosed to the extent required by law or to the degree necessary to conduct an adequate investigation and make a determination regarding a complaint. In some situations, the investigative process may not be complete unless the source of the information and a statement by the member is part of the investigative process.

#### 807.5 SUPERVISOR RESPONSIBILITIES

Supervisors are expected to remain familiar with this policy and ensure that members under their command are aware of its provisions.

The responsibilities of supervisors include, but are not limited to:

- (a) Ensuring complaints of retaliation are investigated as provided in the Personnel Complaints Policy.
- (b) Receiving all complaints in a fair and impartial manner.
- (c) Documenting the complaint and any steps taken to resolve the problem.
- (d) Acknowledging receipt of the complaint, notifying the Chief of Investigations via the chain of command and explaining to the member how the complaint will be handled.
- (e) Taking appropriate and reasonable steps to mitigate any further violations of this policy.
- (f) Monitoring the work environment to ensure that any member making a complaint is not subjected to further retaliation.
- (g) Periodic follow-up with the complainant to ensure that retaliation is not continuing.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Anti-Retaliation*

---

- (h) Not interfering with or denying the right of a member to make any complaint.
- (i) Taking reasonable steps to accommodate requests for assignment or schedule changes made by a member who may be the target of retaliation if it would likely mitigate the potential for further violations of this policy.

#### **807.6 COMMAND STAFF RESPONSIBILITIES**

The Chief of Investigations should communicate to all supervisors the prohibition against retaliation.

Command staff shall treat all complaints as serious matters and shall ensure that prompt actions take place, including but not limited to:

- (a) Communicating to all members the prohibition against retaliation.
- (b) The timely review of complaint investigations.
- (c) Remediation of any inappropriate conduct or condition and instituting measures to eliminate or minimize the likelihood of recurrence.
- (d) The timely communication of the outcome to the complainant.

#### **807.7 WHISTLE-BLOWING**

California law protects members who (Labor Code § 1102.5; Government Code § 53296 et seq.):

- (a) Report a violation of a state or federal statute or regulation to a government or law enforcement agency, including the member's supervisor or any other member with the authority to investigate the reported violation.
- (b) Provide information or testify before a public body if the member has reasonable cause to believe a violation of law occurred.
- (c) Refuse to participate in an activity that would result in a violation of a state or federal statute or regulation.
- (d) File a complaint with a local agency about gross mismanagement or a significant waste of funds, abuse of authority, or a substantial and specific danger to public health or safety. Members shall exhaust all available administrative remedies prior to filing a formal complaint.
- (e) Are family members of a person who has engaged in any protected acts described above.

Members are encouraged to report any legal violations through the chain of command (Labor Code § 1102.5).

Members who believe they have been the subject of retaliation for engaging in such protected behaviors should promptly report it to a supervisor. Supervisors should refer the complaint to the Lieutenant for investigation pursuant to the Personnel Complaints Policy.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Anti-Retaliation*

---

#### **807.7.1 DISPLAY OF WHISTLE-BLOWER LAWS**

The Bureau shall display a notice to members regarding their rights and responsibilities under the whistle-blower laws, including the whistle-blower hotline maintained by the Office of the Attorney General (Labor Code § 1102.8).

#### **807.8 RECORDS RETENTION AND RELEASE**

The Records Manager shall ensure that documentation of investigations is maintained in accordance with the established records retention schedules.

#### **807.9 TRAINING**

The policy should be reviewed with each new member.

All members should receive periodic refresher training on the requirements of this policy.

# Reporting of Arrests, Convictions, and Court Orders

## 808.1 PURPOSE AND SCOPE

The purpose of this policy is to describe the notification requirements and procedures that members must follow when certain arrests, convictions, and court orders restrict their ability to perform the official duties and responsibilities of the Stanislaus County District Attorney's Office. This policy will also describe the notification requirements and procedures that certain retired investigators must follow when an arrest, conviction, or court order disqualifies them from possessing a firearm.

## 808.2 POLICY

The Stanislaus County District Attorney's Office requires disclosure of member arrests, convictions, and certain court orders to maintain the high standards, ethics, and integrity in its workforce, and to ensure compatibility with the duties and responsibilities of the Bureau.

## 808.3 DOMESTIC VIOLENCE CONVICTIONS AND COURT ORDERS

Federal and California law prohibit individuals convicted of, or having an outstanding warrant for, certain offenses and individuals convicted of certain offenses and individuals subject to certain court orders from lawfully possessing firearms. Such convictions and court orders often involve allegations of the use or attempted use of force, or threatened use of a weapon on any individual in a domestic relationship (e.g., spouse, cohabitant, parent, child) (18 USC § 922; Penal Code § 29805).

All members and retired investigators with identification cards issued by the Bureau are responsible for ensuring that they have not been disqualified from possessing firearms by any such conviction or court order, and shall promptly report any such conviction or court order to a supervisor, as provided in this policy.

## 808.4 OTHER CRIMINAL CONVICTIONS AND COURT ORDERS

Government Code § 1029 prohibits any person convicted of a felony from being a peace officer in the State of California. This prohibition applies regardless of whether the guilt was established by way of a verdict, guilty, or nolo contendere plea.

Convictions of certain violations of the Vehicle Code and other provisions of law may also place restrictions on a member's ability to fully perform the duties of the job.

Outstanding warrants as provided in Penal Code § 29805 also place restrictions on a member's ability to possess a firearm.

While legal restrictions may or may not be imposed by statute or by the courts upon conviction of any criminal offense, criminal conduct by members of this bureau may be inherently in conflict with law enforcement duties and the public trust, and shall be reported as provided in this policy.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Reporting of Arrests, Convictions, and Court Orders*

---

#### **808.5 REPORTING**

All members and all retired investigators with an identification card issued by the Bureau shall immediately notify their supervisors (retired investigators should immediately notify the Lieutenant or the Chief of Investigations) in writing of any past or current criminal detention, arrest, charge, or conviction in any state or foreign country, regardless of whether or not the matter was dropped or rejected, is currently pending or is on appeal, and regardless of the penalty or sentence, if any.

All members and all retired investigators with an identification card issued by the Bureau shall further promptly notify their supervisors (retired investigators should immediately notify the Lieutenant or the Chief of Investigations) in writing if they become the subject of a domestic violence-related order or any court order that prevents the member or retired investigator from possessing a firearm or requires suspension or revocation of applicable POST certification.

Any member whose criminal arrest, conviction, or court order restricts or prohibits that member from fully and properly performing their duties, including carrying a firearm, may be disciplined. This includes but is not limited to being placed on administrative leave, reassignment, and/or termination. Any effort to remove such disqualification or restriction shall remain entirely the responsibility of the member, on the member's own time and expense.

Any member failing to provide prompt written notice pursuant to this policy shall be subject to discipline, up to and including termination.

Retired investigators may have their identification cards rescinded or modified, as may be appropriate (see the Retiree Concealed Firearms Policy).

##### **808.5.1 NOTIFICATION REQUIREMENTS**

The Office of the District Attorney Lieutenant shall submit within 10 days of final disposition a notice to POST of a conviction or Government Code § 1029 reason that disqualifies any current peace officer employed by this bureau or any former peace officer if this bureau was responsible for the investigation (11 CCR 1003).

#### **808.6 PROCEDURE FOR RELIEF**

Pursuant to Penal Code § 29855, a peace officer may petition the court for permission to carry a firearm following a conviction under state law. Federal law, however, does not provide for any such similar judicial relief and the granting of a state court petition under Penal Code § 29855 will not relieve one of the restrictions imposed by federal law. Therefore, relief for any employee falling under the restrictions imposed by federal law may only be obtained by expungement of the conviction. Employees shall seek relief from firearm restrictions on their own time and through their own resources.

Pursuant to Family Code § 6389(h), an individual may petition the court for an exemption to any restraining order, which would thereafter permit the individual to carry a firearm or ammunition as a part of the individual's employment. Relief from any domestic violence or other restriction shall also be pursued through the employee's own resources and on the employee's own time.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Reporting of Arrests, Convictions, and Court Orders*

---

Pending satisfactory proof of relief from any legal restriction imposed on an employee's duties, the employee may be placed on administrative leave, reassigned, or disciplined. The Bureau may, but is not required to return an employee to any assignment, reinstate any employee, or reverse any pending or imposed discipline upon presentation of satisfactory proof of relief from any legal restriction set forth in this policy.

# Drug- and Alcohol-Free Workplace

## **809.1 PURPOSE AND SCOPE**

The purpose of this policy is to establish clear and uniform guidelines regarding drugs and alcohol in the workplace (41 USC § 8103).

## **809.2 POLICY**

It is the policy of this bureau to provide a drug- and alcohol-free workplace for all members.

## **809.3 GENERAL GUIDELINES**

Alcohol and drug use in the workplace or on bureau time can endanger the health and safety of bureau members and the public.

Members who have consumed an amount of an alcoholic beverage or taken any medication, or combination thereof, that would tend to adversely affect their mental or physical abilities shall not report for duty. Affected members shall notify the Lieutenant or appropriate supervisor as soon as the member is aware that the member will not be able to report to work. If the member is unable to make the notification, every effort should be made to have a representative contact the supervisor in a timely manner. If the member is adversely affected while on-duty, the member shall be immediately removed and released from work (see the Work Restrictions section in this policy).

### **809.3.1 USE OF MEDICATIONS**

Members should not use any medications that will impair their ability to safely and completely perform their duties. Any member who is medically required or has a need to take any such medication shall report that need to the member's immediate supervisor prior to commencing any on-duty status.

No member shall be permitted to work or drive a vehicle owned or leased by the Bureau while taking any medication that has the potential to impair the member's abilities, without a written release from the member's physician.

### **809.3.2 MEDICAL CANNABIS**

Possession, use, or being under the influence of medical cannabis on-duty is prohibited and may lead to disciplinary action.

## **809.4 MEMBER RESPONSIBILITIES**

Members shall report for work in an appropriate mental and physical condition. Members are prohibited from purchasing, manufacturing, distributing, dispensing, possessing or using controlled substances or alcohol on bureau premises or on bureau time (41 USC § 8103). The lawful possession or use of prescribed medications or over-the-counter remedies is excluded from this prohibition.

Members who are authorized to consume alcohol as part of a special assignment shall not do so to the extent of impairing on-duty performance.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Drug- and Alcohol-Free Workplace*

---

Members shall notify a supervisor immediately if they observe behavior or other evidence that they believe demonstrates that a fellow member poses a risk to the health and safety of the member or others due to drug or alcohol use.

Members are required to notify their immediate supervisors of any criminal drug statute conviction for a violation occurring in the workplace no later than five days after such conviction (41 USC § 8103).

#### **809.5 EMPLOYEE ASSISTANCE PROGRAM**

There may be available a voluntary employee assistance program to assist those who wish to seek help for alcohol and drug problems (41 USC § 8103). Insurance coverage that provides treatment for drug and alcohol abuse also may be available. Employees should contact the Human Resources, their insurance providers or the employee assistance program for additional information. It is the responsibility of each employee to seek assistance before alcohol or drug problems lead to performance problems.

#### **809.6 WORK RESTRICTIONS**

If a member informs a supervisor that he/she has consumed any alcohol, drug or medication that could interfere with a safe and efficient job performance, the member may be required to obtain clearance from his/her physician before continuing to work.

If the supervisor reasonably believes, based on objective facts, that a member is impaired by the consumption of alcohol or other drugs, the supervisor shall prevent the member from continuing work and shall ensure that he/she is safely transported away from the Bureau.

#### **809.7 SCREENING TESTS**

A supervisor may require an employee to submit to a screening under any of the following circumstances:

- (a) The supervisor reasonably believes, based upon objective facts, that the employee is under the influence of alcohol or drugs that are impairing the employee's ability to perform duties safely and efficiently.
- (b) The employee discharges a firearm in the performance of the employee's duties (excluding training or authorized euthanizing of an animal).
- (c) The employee discharges a firearm issued by the Bureau while off-duty, resulting in injury, death, or substantial property damage.
- (d) The employee drives a motor vehicle in the performance of the employee's duties and becomes involved in an incident that results in bodily injury, death, or substantial damage to property.

##### **809.7.1 SUPERVISOR RESPONSIBILITIES**

The supervisor shall prepare a written record documenting the specific facts that led to the decision to require the test, and shall inform the employee in writing of the following:

- (a) The test will be given to detect either alcohol or drugs, or both.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Drug- and Alcohol-Free Workplace*

---

- (b) The result of the test is not admissible in any criminal proceeding against the employee.
- (c) The employee may refuse the test, but refusal may result in dismissal or other disciplinary action.

#### 809.7.2 DISCIPLINE

An employee may be subject to disciplinary action if the employee:

- (a) Fails or refuses to submit to a screening test as requested.
- (b) After taking a screening test that indicates the presence of a controlled substance, fails to provide proof, within 72 hours after being requested, that the employee took the controlled substance as directed, pursuant to a current and lawful prescription issued in the employee's name.

#### **809.8 COMPLIANCE WITH THE DRUG-FREE WORKPLACE ACT**

No later than 30 days following notice of any drug statute conviction for a violation occurring in the workplace involving a member, the Bureau will take appropriate disciplinary action, up to and including dismissal, and/or requiring the member to satisfactorily participate in a drug abuse assistance or rehabilitation program (41 USC § 8104).

#### **809.9 CONFIDENTIALITY**

The Bureau recognizes the confidentiality and privacy due to its members. Disclosure of any information relating to substance abuse treatment, except on a need-to-know basis, shall only be with the express written consent of the member involved or pursuant to lawful process.

The written results of any screening tests and all documents generated by the employee assistance program are considered confidential medical records and shall be maintained in the member's confidential medical file in accordance with the Personnel Records Policy.

## Sick Leave

### 810.1 PURPOSE AND SCOPE

This policy provides general guidance regarding the use and processing of sick leave. The accrual and terms of use of sick leave for eligible employees are detailed in the County personnel manual or applicable collective bargaining agreement.

This policy is not intended to cover all types of sick or other leaves. For example, employees may be entitled to additional paid or unpaid leave for certain family and medical reasons as provided for in the Family and Medical Leave Act (FMLA) (29 USC § 2601 et seq.), the California Family Rights Act, leave for victims of crime or abuse, or for organ or bone marrow donor procedures (29 CFR 825; Government Code § 12945.2; Government Code § 12945.8; Labor Code § 1510).

### 810.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to provide eligible employees with a sick leave benefit.

### 810.3 USE OF SICK LEAVE

Sick leave is intended to be used for qualified absences. Sick leave is not considered vacation. Abuse of sick leave may result in discipline, denial of sick leave benefits, or both.

Employees on sick leave shall not engage in other employment or self-employment or participate in any sport, hobby, recreational activity or other activity that may impede recovery from the injury or illness (see Outside Employment Policy).

Qualified appointments should be scheduled during a member's non-working hours when it is reasonable to do so.

#### 810.3.1 NOTIFICATION

All members should notify the Lieutenant or appropriate supervisor as soon as they are aware that they will not be able to report to work and no less than one hour before the start of their scheduled shifts. If, due to an emergency, a member is unable to contact the supervisor, every effort should be made to have a representative for the member contact the supervisor (Labor Code § 246 ).

When the necessity to be absent from work is foreseeable, such as planned medical appointments or treatments, the member shall, whenever possible and practicable, provide a supervisor notice within a reasonable time period prior to the appointment (Labor Code § 246).

Upon return to work, members are responsible for ensuring their time off was appropriately accounted for, and for completing and submitting the required documentation describing the type of time off used and the specific amount of time taken.

### 810.4 EXTENDED ABSENCE

Members absent from duty for more than three consecutive days may be required to furnish a statement from a health care provider supporting the need to be absent and/or the ability to return

### *Sick Leave*

---

to work. Members on an extended absence shall, if possible, contact their supervisor at specified intervals to provide an update on their absence and expected date of return.

Nothing in this section precludes a supervisor from requiring, with cause, a health care provider's statement for an absence of three or fewer days after the first three days of paid sick leave are used in a 12-month period.

#### **810.5 SUPERVISOR RESPONSIBILITIES**

The responsibilities of supervisors include, but are not limited to:

- (a) Monitoring and regularly reviewing the attendance of those under their command to ensure that the use of sick leave and absences is consistent with this policy.
- (b) Attempting to determine whether an absence of four or more days may qualify as family medical leave and consulting with legal counsel or the Human Resources as appropriate.
- (c) Addressing absences and sick leave use in the member's performance evaluation when excessive or unusual use has:
  - 1. Negatively affected the member's performance or ability to complete assigned duties.
  - 2. Negatively affected bureau operations.
- (d) When appropriate, counseling members regarding excessive absences and/or inappropriate use of sick leave.
- (e) Referring eligible members to an available employee assistance program when appropriate.

#### **810.6 REQUIRED NOTICES**

The Personnel Manager shall ensure:

- (a) Written notice of the amount of paid sick leave available is provided to employees as provided in Labor Code § 246.
- (b) A poster is displayed in a conspicuous place for employees to review that contains information on paid sick leave as provided in Labor Code § 247.

# Communicable Diseases

## 811.1 PURPOSE AND SCOPE

This policy provides general guidelines to assist in minimizing the risk of bureau members contracting and/or spreading communicable diseases.

### 811.1.1 DEFINITIONS

Definitions related to this policy include:

**Communicable disease** - A human disease caused by microorganisms that are present in and transmissible through human blood, bodily fluid, tissue, or by breathing or coughing. These diseases commonly include, but are not limited to, hepatitis B virus (HBV), HIV and tuberculosis.

**Exposure** - When an eye, mouth, mucous membrane or non-intact skin comes into contact with blood or other potentially infectious materials, or when these substances are injected or infused under the skin; when an individual is exposed to a person who has a disease that can be passed through the air by talking, sneezing or coughing (e.g., tuberculosis), or the individual is in an area that was occupied by such a person. Exposure only includes those instances that occur due to a member's position at the Stanislaus County District Attorney's Office. (See the exposure control plan for further details to assist in identifying whether an exposure has occurred.)

## 811.2 POLICY

The Stanislaus County District Attorney's Office is committed to providing a safe work environment for its members. Members should be aware that they are ultimately responsible for their own health and safety.

## 811.3 EXPOSURE PREVENTION AND MITIGATION

### 811.3.1 GENERAL PRECAUTIONS

All members are expected to use good judgment and follow training and procedures related to mitigating the risks associated with communicable disease. This includes, but is not limited to (8 CCR 5193):

- (a) Stocking disposable gloves, antiseptic hand cleanser, CPR masks or other specialized equipment in the work area or bureau vehicles, as applicable.
- (b) Wearing bureau-approved disposable gloves when contact with blood, other potentially infectious materials, mucous membranes and non-intact skin can be reasonably anticipated.
- (c) Washing hands immediately or as soon as feasible after removal of gloves or other PPE.
- (d) Treating all human blood and bodily fluids/tissue as if it is known to be infectious for a communicable disease.
- (e) Using an appropriate barrier device when providing CPR.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Communicable Diseases*

---

- (f) Using a face mask or shield if it is reasonable to anticipate an exposure to an airborne transmissible disease.
- (g) Decontaminating non-disposable equipment (e.g., flashlight, control devices, clothing and portable radio) as soon as possible if the equipment is a potential source of exposure.
  - 1. Clothing that has been contaminated by blood or other potentially infectious materials shall be removed immediately or as soon as feasible and stored/decontaminated appropriately.
- (h) Handling all sharps and items that cut or puncture (e.g., needles, broken glass, razors, knives) cautiously and using puncture-resistant containers for their storage and/or transportation.
- (i) Avoiding eating, drinking, smoking, applying cosmetics or lip balm, or handling contact lenses where there is a reasonable likelihood of exposure.
- (j) Disposing of biohazardous waste appropriately or labeling biohazardous material properly when it is stored.

#### 811.3.2 IMMUNIZATIONS

Members who could be exposed to HBV due to their positions may receive the HBV vaccine and any routine booster at no cost (8 CCR 5193).

### **811.4 POST EXPOSURE**

#### 811.4.1 INITIAL POST-EXPOSURE STEPS

Members who experience an exposure or suspected exposure shall:

- (a) Begin decontamination procedures immediately (e.g., wash hands and any other skin with soap and water, flush mucous membranes with water).
- (b) Obtain medical attention as appropriate.
- (c) Notify a bureau supervisor as soon as practicable.

#### 811.4.2 REPORTING REQUIREMENTS

The bureau supervisor on-duty shall investigate every exposure or suspected exposure that occurs as soon as possible following the incident. The supervisor shall ensure the following information is documented (8 CCR 5193):

- (a) Name and Social Security number of the member exposed
- (b) Date and time of the incident
- (c) Location of the incident
- (d) Potentially infectious materials involved and the source of exposure (e.g., identification of the person who may have been the source)
- (e) Work being done during exposure
- (f) How the incident occurred or was caused

# Stanislaus County District Attorney's Office

## Policy Manual

### *Communicable Diseases*

---

- (g) PPE in use at the time of the incident
- (h) Actions taken post-event (e.g., clean-up, notifications)

The supervisor shall advise the member that disclosing the identity and/or infectious status of a source to the public or to anyone who is not involved in the follow-up process is prohibited. The supervisor should complete the incident documentation in conjunction with other reporting requirements that may apply (see the Occupational Disease and Work-Related Injury Reporting Policy).

#### 811.4.3 MEDICAL CONSULTATION, EVALUATION AND TREATMENT

Bureau members shall have the opportunity to have a confidential medical evaluation immediately after an exposure and follow-up evaluations as necessary (8 CCR 5193).

The Lieutenant should request a written opinion/evaluation from the treating medical professional that contains only the following information:

- (a) Whether the member has been informed of the results of the evaluation.
- (b) Whether the member has been notified of any medical conditions resulting from exposure to blood or other potentially infectious materials which require further evaluation or treatment.

No other information should be requested or accepted by the Lieutenant.

#### 811.4.4 COUNSELING

The Bureau shall provide the member, and his/her family if necessary, the opportunity for counseling and consultation regarding the exposure (8 CCR 5193).

#### 811.4.5 SOURCE TESTING

Testing a person for communicable diseases when that person was the source of an exposure should be done when it is desired by the exposed member or when it is otherwise appropriate (8 CCR 5193). Source testing is the responsibility of a Bureau Lieutenant.

Source testing may be achieved by:

- (a) Obtaining consent from the individual.
- (b) Complying with the statutory scheme of Health and Safety Code § 121060. This includes seeking consent from the person who was the source of the exposure and seeking a court order if consent is not given.
- (c) Testing the exposed member for evidence of a communicable disease and seeking consent from the source individual to either access existing blood samples for testing or for the source to submit to testing (Health and Safety Code § 120262).
- (d) Taking reasonable steps to immediately contact the County Health Officer and provide preliminary information regarding the circumstances of the exposure and the status of the involved individuals to determine whether the County Health Officer will order testing (Penal Code § 7510).

### *Communicable Diseases*

---

- (e) Under certain circumstances, a court may issue a search warrant for the purpose of HIV testing a person when the exposed member qualifies as a crime victim (Penal Code § 1524.1).

Since there is the potential for overlap between the different manners in which source testing may occur, the Lieutenant is responsible for coordinating the testing to prevent unnecessary or duplicate testing.

The Lieutenant should seek the consent of the individual for testing and consult the County Counsel to discuss other options when no statute exists for compelling the source of an exposure to undergo testing if he/she refuses.

#### **811.5 CONFIDENTIALITY OF REPORTS**

Medical information shall remain in confidential files and shall not be disclosed to anyone without the member's written consent (except as required by law). Test results from persons who may have been the source of an exposure are to be kept confidential as well.

#### **811.6 TRAINING**

All members shall participate in training regarding communicable diseases commensurate with the requirements of their position. The training (8 CCR 5193):

- (a) Shall be provided at the time of initial assignment to tasks where an occupational exposure may take place and at least annually after the initial training.
- (b) Shall be provided whenever the member is assigned new tasks or procedures affecting his/her potential exposure to communicable disease.
- (c) Should provide guidance on what constitutes an exposure, what steps can be taken to avoid an exposure and what steps should be taken if a suspected exposure occurs.

# Personnel Complaints

## 813.1 PURPOSE AND SCOPE

This policy provides guidelines for the reporting, investigation and disposition of complaints regarding the conduct of members of the Stanislaus County District Attorney's Office. This policy shall not apply to any questioning, counseling, instruction, informal verbal admonishment or other routine or unplanned contact of a member in the normal course of duty, by a supervisor or any other member, nor shall this policy apply to a criminal investigation.

## 813.2 POLICY

The Stanislaus County District Attorney's Office takes seriously all complaints regarding the service provided by the Bureau and the conduct of its members.

The Bureau will accept and address all complaints of misconduct in accordance with this policy and applicable federal, state and local law, municipal and county rules and the requirements of any collective bargaining agreements.

It is also the policy of this bureau to ensure that the community can report misconduct without concern for reprisal or retaliation.

## 813.3 PERSONNEL COMPLAINTS

Personnel complaints include any allegation of misconduct or improper job performance that, if true, would constitute a violation of bureau policy or of federal, state or local law, policy or rule. Personnel complaints may be generated internally or by the public.

Inquiries about conduct or performance that, if true, would not violate bureau policy or federal, state or local law, policy or rule may be handled informally by a supervisor and shall not be considered a personnel complaint. Such inquiries generally include clarification regarding policy, procedures or the response to specific incidents by the Bureau.

### 813.3.1 COMPLAINT CLASSIFICATIONS

Personnel complaints shall be classified in one of the following categories:

**Informal** - A matter in which the Lieutenant is satisfied that appropriate action has been taken by a supervisor of rank greater than the accused member.

**Formal** - A matter in which a lieutenant determines that further action is warranted. Such complaints may be investigated by a lieutenant or the Chief Investigator, depending on the seriousness and complexity of the investigation.

**Incomplete** - A matter in which the complaining party either refuses to cooperate or becomes unavailable after diligent follow-up investigation. At the discretion of the assigned Lieutenant, such matters may be further investigated depending on the seriousness of the complaint and the availability of sufficient information.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Complaints*

---

#### 813.3.2 SOURCES OF COMPLAINTS

The following applies to the source of complaints:

- (a) Individuals from the public may make complaints in any form, including in writing, by email, in person or by telephone.
- (b) Any bureau member becoming aware of alleged misconduct shall immediately notify a supervisor.
- (c) Supervisors shall initiate a complaint based upon observed misconduct or receipt from any source alleging misconduct that, if true, could result in disciplinary action.
- (d) Anonymous and third-party complaints should be accepted and investigated to the extent that sufficient information is provided.
- (e) Tort claims and lawsuits may generate a personnel complaint.

#### 813.4 AVAILABILITY AND ACCEPTANCE OF COMPLAINTS

##### 813.4.1 COMPLAINT FORMS

Personnel complaint forms will be maintained in a clearly visible location in the public area of the investigator facility and be accessible through the bureau website.

Personnel complaint forms in languages other than English may also be provided, as determined necessary or practicable.

##### 813.4.2 ACCEPTANCE

All complaints will be courteously accepted by any bureau member and promptly given to the appropriate supervisor. Although written complaints are preferred, a complaint may also be filed orally, either in person or by telephone. Such complaints will be directed to a lieutenant. If a lieutenant is not immediately available to take an oral complaint, the receiving member shall obtain contact information sufficient for the supervisor to contact the complainant. The supervisor, upon contact with the complainant, shall complete and submit a complaint form as appropriate.

Although not required, complainants should be encouraged to file complaints in person so that proper identification, signatures, photographs or physical evidence may be obtained as necessary.

A complainant shall be provided with a copy of his/her statement at the time it is filed with the Bureau (Penal Code § 832.7).

##### 813.4.3 AVAILABILITY OF WRITTEN PROCEDURES

The Bureau shall make available to the public a written description of the investigation procedures for complaints (Penal Code § 832.5).

##### 813.4.4 HATE COMPLAINTS AGAINST PEACE OFFICERS

Internal complaints or complaints from the public shall be accepted and investigated in accordance with this policy where it is alleged that an investigator has in the previous seven years, and since 18 years of age, engaged in membership in a hate group, participated in a hate group activity, or advocated any public expression of hate (Penal Code § 13682).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Complaints*

---

#### **813.5 DOCUMENTATION**

Supervisors shall ensure that all formal and informal complaints are documented on a complaint form. The supervisor shall ensure that the nature of the complaint is defined as clearly as possible.

All complaints and inquiries should also be documented in a log that records and tracks complaints. The log shall include the nature of the complaint and the actions taken to address the complaint. On an annual basis, the Bureau should audit the log and send an audit report to the Chief of Investigations or the authorized designee.

#### **813.6 ADMINISTRATIVE INVESTIGATIONS**

Allegations of misconduct will be administratively investigated as follows.

##### **813.6.1 SUPERVISOR RESPONSIBILITIES**

In general, the primary responsibility for the investigation of a personnel complaint shall rest with the member's immediate supervisor, unless the supervisor is the complainant, or the supervisor is the ultimate decision-maker regarding disciplinary action or has any personal involvement regarding the alleged misconduct. The Chief of Investigations or the authorized designee may direct that another supervisor investigate any complaint.

A supervisor who becomes aware of alleged misconduct shall take reasonable steps to prevent aggravation of the situation.

The responsibilities of supervisors include but are not limited to:

- (a) Ensuring that upon receiving or initiating any formal complaint, a complaint form is completed.
  - (a) The original complaint form will be directed to the Lieutenant of the accused member, via the chain of command, who will take appropriate action and/or determine who will have responsibility for the investigation.
- (b) Responding to all complainants in a courteous and professional manner.
- (c) Resolving those personnel complaints that can be resolved immediately.
  - (a) Follow-up contact with the complainant should be made within 24 hours of the Bureau receiving the complaint.
  - (b) If the matter is resolved and no further action is required, the lieutenant will note the resolution on a complaint form and forward the form to the Chief Investigator.
- (d) Ensuring that upon receipt of a complaint involving allegations of a potentially serious nature, the Lieutenant and the Chief of Investigations are notified via the chain of command as soon as practicable.
- (e) Promptly contacting the Human Resources and the Lieutenant for direction regarding their roles in addressing a complaint that relates to sexual, racial, ethnic or other forms of prohibited harassment or discrimination.
- (f) Forwarding unresolved personnel complaints to the Lieutenant, who will determine how to proceed with the investigation.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Complaints*

---

- (g) Informing the complainant of the investigator's name and the complaint number within three days after assignment.
- (h) Investigating a complaint as follows:
  - 1. Making reasonable efforts to obtain names, addresses and telephone numbers of witnesses.
  - 2. When appropriate, ensuring immediate medical attention is provided and photographs of alleged injuries and accessible uninjured areas are taken.
- (i) Ensuring that the procedural rights of the accused member are followed (Government Code § 3303 et seq.).
- (j) Ensuring interviews of the complainant are generally conducted during reasonable hours.

#### 813.6.2 ADMINISTRATIVE INVESTIGATION PROCEDURES

Whether conducted by a lieutenant or the Chief Investigator, the following applies to members covered by the Public Safety Officers Procedural Bill of Rights Act (POBR) (Government Code § 3303):

- (a) Interviews of an accused member shall be conducted during reasonable hours and preferably when the member is on-duty. If the member is off-duty, he/she shall be compensated.
- (b) Unless waived by the member, interviews of an accused member shall be at the Stanislaus County District Attorney's Office or other reasonable and appropriate place.
- (c) No more than two interviewers should ask questions of an accused member.
- (d) Prior to any interview, a member shall be informed of the nature of the investigation, the name, rank and command of the investigator in charge of the investigation, the interviewing officers and all other persons to be present during the interview.
- (e) All interviews shall be for a reasonable period and the member's personal needs should be accommodated.
- (f) No member should be subjected to offensive or threatening language, nor shall any promises, rewards or other inducements be used to obtain answers.
- (g) Any member refusing to answer questions directly related to the investigation may be ordered to answer questions administratively and may be subject to discipline for failing to do so.
  - (a) A member should be given an order to answer questions in an administrative investigation that might incriminate the member in a criminal matter only after the member has been given a *Lybarger* advisement. Administrative investigators should consider the impact that compelling a statement from the member may have on any related criminal investigation and should take reasonable steps to avoid creating any foreseeable conflicts between the two related investigations. This may include conferring with the person in charge of the criminal investigation (e.g., discussion of processes, timing, implications).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Complaints*

---

- (b) No information or evidence administratively coerced from a member may be provided to anyone involved in conducting the criminal investigation or to any prosecutor.
- (h) The interviewer should record all interviews of members and witnesses. The member may also record the interview. If the member has been previously interviewed, a copy of that recorded interview shall be provided to the member prior to any subsequent interview.
- (i) All members subjected to interviews that could result in discipline have the right to have an uninvolved representative present during the interview. However, in order to maintain the integrity of each individual's statement, involved members shall not consult or meet with a representative or attorney collectively or in groups prior to being interviewed.
- (j) All members shall provide complete and truthful responses to questions posed during interviews.
- (k) No member may be requested or compelled to submit to a polygraph examination, nor shall any refusal to submit to such examination be mentioned in any investigation (Government Code § 3307).

No investigation shall be undertaken against any investigator solely because the investigator has been placed on a prosecutor's *Brady* list or the name of the investigator may otherwise be subject to disclosure pursuant to *Brady v. Maryland*. However, an investigation may be based on the underlying acts or omissions for which the investigator has been placed on a *Brady* list or may otherwise be subject to disclosure pursuant to *Brady v. Maryland* (Government Code § 3305.5).

#### 813.6.3 ADMINISTRATIVE INVESTIGATION FORMAT

Formal investigations of personnel complaints shall be thorough, complete and essentially follow this format:

**Introduction** - Include the identity of the members, the identity of the assigned investigators, the initial date and source of the complaint.

**Summary** - Provide a brief summary of the facts giving rise to the investigation.

**Allegation** - List the allegations separately, including applicable policy sections, with a brief summary of the evidence relevant to each allegation. A separate recommended finding should be provided for each allegation. Each allegation should be set forth with the details of the evidence applicable to each allegation provided, including comprehensive summaries of member and witness statements. Other evidence related to each allegation should also be detailed in this section.

**Conclusion** - A recommendation regarding further action or disposition should be provided.

**Addendum** - A separate list of exhibits (e.g., recordings, photos, documents) should be attached to the report.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Complaints*

---

#### 813.6.4 DISPOSITIONS

Each personnel complaint shall be classified with one of the following dispositions:

**Unfounded** - When the investigation discloses that the alleged acts did not occur or did not involve bureau members. Complaints that are determined to be frivolous will fall within the classification of unfounded (Penal Code § 832.8).

**Exonerated** - When the investigation discloses that the alleged act occurred but that the act was justified, lawful and/or proper.

**Not sustained** - When the investigation discloses that there is insufficient evidence to sustain the complaint or fully exonerate the member.

**Sustained** - A final determination by an investigating agency, commission, board, hearing officer, or arbitrator, as applicable, following an investigation and opportunity for an administrative appeal pursuant to Government Code § 3304 and Government Code § 3304.5 that the actions of an investigator were found to violate law or bureau policy (Penal Code § 832.8).

**Closed** - A "closed" disposition will be used for an employee who either resigns or retires prior to the completion of the investigation.

If an investigation discloses misconduct or improper job performance that was not alleged in the original complaint, the investigator shall take appropriate action with regard to any additional allegations.

#### 813.6.5 COMPLETION OF INVESTIGATIONS

Every investigator or supervisor assigned to investigate a personnel complaint or other alleged misconduct shall proceed with due diligence in an effort to complete the investigation within one year from the date of discovery by an individual authorized to initiate an investigation (Government Code § 3304).

In the event that an investigation cannot be completed within one year of discovery, the assigned investigator or supervisor shall ensure that an extension or delay is warranted within the exceptions set forth in Government Code § 3304(d) or Government Code § 3508.1.

#### 813.6.6 NOTICE TO COMPLAINANT OF INVESTIGATION STATUS

The member conducting the investigation should provide the complainant with periodic updates on the status of the investigation, as appropriate. At the conclusion of the Internal Affairs investigation, the Chief Investigator will notify the complainant in writing of the disposition of the complaint.

#### 813.7 ADMINISTRATIVE SEARCHES

Assigned lockers, storage spaces and other areas, including desks, offices and vehicles, may be searched as part of an administrative investigation upon a reasonable suspicion of misconduct.

Such areas may also be searched any time by a supervisor for non-investigative purposes, such as obtaining a needed report, radio or other document or equipment.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Complaints*

---

Lockers and storage spaces may only be administratively searched in the member's presence, with the member's consent, with a valid search warrant or where the member has been given reasonable notice that the search will take place (Government Code § 3309).

#### **813.7.1 DISCLOSURE OF FINANCIAL INFORMATION**

An employee may be compelled to disclose personal financial information under the following circumstances (Government Code § 3308):

- (a) Pursuant to a state law or proper legal process
- (b) Information exists that tends to indicate a conflict of interest with official duties
- (c) If the employee is assigned to or being considered for a special assignment with a potential for bribes or other improper inducements

#### **813.8 ADMINISTRATIVE LEAVE**

When a complaint of misconduct is of a serious nature, or when circumstances indicate that allowing the accused to continue to work would adversely affect the mission of the Bureau, the Chief of Investigations or the authorized designee may temporarily assign an accused employee to administrative leave. Any employee placed on administrative leave:

- (a) May be required to relinquish any bureau badge, identification, assigned weapons and any other bureau equipment.
- (b) Shall be required to continue to comply with all policies and lawful orders of a supervisor.
- (c) May be temporarily reassigned to a different shift, generally a normal business-hours shift, during the investigation. The employee may be required to remain available for contact at all times during such shift, and will report as ordered.

#### **813.9 CRIMINAL INVESTIGATION**

Where a member is accused of potential criminal conduct, a separate supervisor, investigator, or agency shall be assigned to investigate the criminal allegations apart from any administrative investigation. Any separate administrative investigation may parallel a criminal investigation.

The Chief of Investigations shall be notified as soon as practicable when a member is accused of criminal conduct. The Chief of Investigations may request a criminal investigation by an outside law enforcement agency.

A member accused of criminal conduct shall be advised of his/her constitutional rights (Government Code § 3303(h)). The member should not be administratively ordered to provide any information in the criminal investigation.

The Stanislaus County District Attorney's Office may release information concerning the arrest or detention of any member, including an investigator, that has not led to a conviction. No disciplinary action should be taken until an independent administrative investigation is conducted.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Complaints*

---

#### **813.10 POST-ADMINISTRATIVE INVESTIGATION PROCEDURES**

Upon completion of a formal investigation, an investigation report should be forwarded to the Chief of Investigations. The Chief of Investigations may accept or modify any classification or recommendation for disciplinary action.

##### **813.10.1 CHIEF OF INVESTIGATIONS RESPONSIBILITIES**

Upon receipt of any written recommendation for disciplinary action, the Chief of Investigations shall review the recommendation and all accompanying materials. The Chief of Investigations may modify any recommendation and/or may return the file to the Lieutenant for further investigation or action.

Once the Chief of Investigations is satisfied that no further investigation or action is required by staff, the Chief of Investigations shall determine the amount of discipline, if any, that should be imposed. In the event disciplinary action is proposed, the Chief of Investigations shall provide the member with a pre-disciplinary procedural due process hearing (*Skelly*) by providing written notice of the charges, proposed action and reasons for the proposed action. Written notice shall be provided within one year from the date of discovery of the misconduct (Government Code § 3304(d)). The Chief of Investigations shall also provide the member with:

- (a) Access to all of the materials considered by the Chief of Investigations in recommending the proposed discipline.
- (b) An opportunity to respond orally or in writing to the Chief of Investigations within five days of receiving the notice.
  - 1. Upon a showing of good cause by the member, the Chief of Investigations may grant a reasonable extension of time for the member to respond.
  - 2. If the member elects to respond orally, the presentation may be recorded by the Bureau. Upon request, the member shall be provided with a copy of the recording.

Once the member has completed his/her response or if the member has elected to waive any such response, the Chief of Investigations shall consider all information received in regard to the recommended discipline. The Chief of Investigations shall render a timely written decision to the member and specify the grounds and reasons for discipline and the effective date of the discipline. Once the Chief of Investigations has issued a written decision, the discipline shall become effective.

##### **813.10.2 NOTICE OF FINAL DISPOSITION TO THE COMPLAINANT**

The Chief of Investigations or the authorized designee shall ensure that the complainant is notified, in writing, of the disposition (i.e., sustained, not sustained, exonerated, unfounded) of the complaint (Penal Code § 832.7(f)).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Complaints*

---

#### 813.10.3 NOTICE REQUIREMENTS

The disposition of any civilian's complaint shall be released to the complaining party within 30 days of the final disposition. This release shall not include what discipline, if any, was imposed (Penal Code § 832.7(f)).

#### 813.11 PRE-DISCIPLINE EMPLOYEE RESPONSE

The pre-discipline process is intended to provide the accused employee with an opportunity to present a written or oral response to the Chief of Investigations after having had an opportunity to review the supporting materials and prior to imposition of any recommended discipline. The employee shall consider the following:

- (a) The response is not intended to be an adversarial or formal hearing.
- (b) Although the employee may be represented by an uninvolved representative or legal counsel, the response is not designed to accommodate the presentation of testimony or witnesses.
- (c) The employee may suggest that further investigation could be conducted or the employee may offer any additional information or mitigating factors for the Chief of Investigations to consider.
- (d) In the event that the Chief of Investigations elects to cause further investigation to be conducted, the employee shall be provided with the results prior to the imposition of any discipline.
- (e) The employee may thereafter have the opportunity to further respond orally or in writing to the Chief of Investigations on the limited issues of information raised in any subsequent materials.

#### 813.12 RESIGNATIONS/RETIREMENTS PRIOR TO DISCIPLINE

In the event that a member tenders a written resignation or notice of retirement prior to the imposition of discipline, it shall be noted in the file. The tender of a resignation or retirement by itself shall not serve as grounds for the termination of any pending investigation or discipline (Penal Code § 13510.8).

#### 813.13 POST-DISCIPLINE APPEAL RIGHTS

Non-probationary employees have the right to appeal a suspension without pay, punitive transfer, demotion, reduction in pay or step, or termination from employment. The employee has the right to appeal using the procedures established by any collective bargaining agreement, Memorandum of Understanding and/or personnel rules.

In the event of punitive action against an employee covered by the POBR, the appeal process shall be in compliance with Government Code § 3304 and Government Code § 3304.5.

During any administrative appeal, evidence that an investigator has been placed on a *Brady* list or is otherwise subject to *Brady* restrictions may not be introduced unless the underlying allegations of misconduct have been independently established. Thereafter, such *Brady* evidence shall be limited to determining the appropriateness of the penalty (Government Code § 3305.5).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Complaints*

---

#### **813.14 PROBATIONARY EMPLOYEES AND OTHER MEMBERS**

At-will and probationary employees and those members other than non-probationary employees may be released from employment for non-disciplinary reasons (e.g., failure to meet standards) without adherence to the procedures set forth in this policy or any right to appeal. However, any probationary investigator subjected to an investigation into allegations of misconduct shall be entitled to those procedural rights, as applicable, set forth in the POBR (Government Code § 3303; Government Code § 3304).

At-will, probationary employees and those other than non-probationary employees subjected to discipline or termination as a result of allegations of misconduct shall not be deemed to have acquired a property interest in their position, but shall be given the opportunity to appear before the Chief of Investigations or authorized designee for a non-evidentiary hearing for the sole purpose of attempting to clear their name or liberty interest. There shall be no further opportunity for appeal beyond the liberty interest hearing and the decision of the Chief of Investigations shall be final.

#### **813.15 RETENTION OF PERSONNEL INVESTIGATION FILES**

All personnel complaints shall be maintained in accordance with the established records retention schedule and as described in the Personnel Records Policy.

#### **813.16 REQUIRED REPORTING TO POST**

The Chief of Investigations or the authorized designee shall notify POST on the appropriate POST form within 10 days of certain investigator personnel events, including but not limited to (Penal Code § 13510.9):

- (a) Termination or separation from employment or appointment. Separation from employment or appointment includes any involuntary termination, resignation, or retirement.
  - 1. A POST affidavit-of-separation form shall be executed and maintained by the Bureau and submitted to POST as required by Penal Code § 13510.9 and 11 CCR 1003.
- (b) Events that could affect an investigator's POST certification, such as:
  - 1. Complaints, charges, or allegations of serious misconduct (as defined by Penal Code § 13510.8).
  - 2. Findings of civilian review boards.
  - 3. Final dispositions of any investigations.
  - 4. Civil judgments or court findings based on conduct, or settlement of a civil claim against an investigator or the Stanislaus County District Attorney's Office based on allegations of conduct by an investigator.

The Chief of Investigations or the authorized designee shall be responsible for providing POST access to or duplication of investigation documentation (e.g., physical or documentary evidence, witness statements, analysis, conclusions) within the applicable timeframe provided in Penal Code § 13510.9.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Complaints*

---

#### 813.16.1 NOTIFICATIONS TO POST FOR SERIOUS MISCONDUCT

The Chief of Investigations or the authorized designee shall report allegations of serious misconduct by an investigator to POST and the report shall include the following (11 CCR 1207):

- (a) Name of the Bureau
- (b) Administrative case number
- (c) Name, current address, and phone number of the complainant, if available
- (d) Name, POST ID, current address, and phone number of the involved investigator
- (e) A summary of the alleged misconduct including:
  - 1. A narrative of the allegations
  - 2. Date and time of incidents
  - 3. Location of occurrence
  - 4. Any witness information, if available
  - 5. Summary of arrest or indictment of involved investigator
- (f) A change in employment status of the involved investigator (e.g., administrative leave, suspension, termination)
- (g) Name and contact information of the assigned investigator

The Chief of Investigations or the authorized designee shall provide updates of the investigation to POST every 90 days until the final disposition in the method designated by POST (11 CCR 1207).

Upon completion of the investigation, the Chief of Investigations or the authorized designee shall submit to POST the final disposition of the investigation as well as investigation materials and the investigator's service record as provided by 11 CCR 1207.

#### 813.16.2 ADDITIONAL NOTIFICATIONS TO POST FOR SERIOUS MISCONDUCT

Additional notification shall be made to POST (11 CCR 1207):

- (a) If the imposed disciplinary action is pending appeal or other review through an administrative or judicial proceeding:
  - 1. The Bureau shall provide the name of the body conducting the proceeding.
  - 2. The status of the proceeding, if known.
- (b) If criminal charges are pending:
  - 1. The name of the court having jurisdiction over the criminal charges against the investigator.
  - 2. The status of the criminal case, if known.

## Seat Belts

### 814.1 PURPOSE AND SCOPE

This policy establishes guidelines for the use of seat belts and child restraints. This policy will apply to all members operating or riding in bureau vehicles (Vehicle Code § 27315.5).

Guidance for transporting persons in custody may be found in the Transporting Persons in Custody and Handcuffing and Restraints policies.

#### 814.1.1 DEFINITIONS

Definitions related to this policy include:

**Child restraint system** - An infant or child passenger restraint system that meets Federal Motor Vehicle Safety Standards (FMVSS) and Regulations set forth in 49 CFR 571.213.

### 814.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office that members use safety and child restraint systems to reduce the possibility of death or injury in a motor vehicle collision.

### 814.3 WEARING OF SAFETY RESTRAINTS

All members shall wear properly adjusted safety restraints when operating or riding in a seat equipped with restraints, in any vehicle owned, leased or rented by this bureau while on- or off-duty, or in any privately owned vehicle while on-duty. The member driving such a vehicle shall ensure that all other occupants, including non-members, are also properly restrained.

Exceptions to the requirement to wear safety restraints may be made only in exceptional situations where, due to unusual circumstances, wearing a seat belt would endanger the member or the public. Members must be prepared to justify any deviation from this requirement.

### 814.4 TRANSPORTING CHILDREN

Children under the age of 8 shall be transported in compliance with California's child restraint system requirements (Vehicle Code § 27360; Vehicle Code § 27363).

Rear seat passengers in a cage-equipped vehicle may have reduced clearance, which requires careful seating and positioning of seat belts. Due to this reduced clearance, and if permitted by law, children and any child restraint system may be secured in the front seat of such vehicles provided this positioning meets federal safety standards and the vehicle and child restraint system manufacturer's design and use recommendations. In the event that a child is transported in the front seat of a vehicle, the seat should be pushed back as far as possible and the passenger-side airbag should be deactivated. If this is not possible, members should arrange alternate transportation when feasible. A child shall not be transported in a rear-facing child restraint system in the front seat in a vehicle that is equipped with an active frontal passenger airbag (Vehicle Code § 27363).

### *Seat Belts*

---

#### **814.5 INOPERABLE SEAT BELTS**

Bureau vehicles shall not be operated when the seat belt in the driver's position is inoperable. Persons shall not be transported in a seat in which the seat belt is inoperable.

Bureau vehicle seat belts shall not be modified, removed, deactivated or altered in any way, except by the vehicle maintenance and repair staff, who shall do so only with the express authorization of the Chief of Investigations.

Members who discover an inoperable restraint system shall report the defect to the appropriate supervisor. Prompt action will be taken to replace or repair the system.

#### **814.6 VEHICLES MANUFACTURED WITHOUT SEAT BELTS**

Vehicles manufactured and certified for use without seat belts or other restraint systems are subject to the manufacturer's operator requirements for safe use.

#### **814.7 VEHICLE AIRBAGS**

In all vehicles equipped with airbag restraint systems, the system will not be tampered with or deactivated, except when transporting children as written elsewhere in this policy. All equipment installed in vehicles equipped with airbags will be installed as per the vehicle manufacturer specifications to avoid the danger of interfering with the effective deployment of the airbag device.



## Body Armor

### 815.1 PURPOSE AND SCOPE

The purpose of this policy is to provide law enforcement officers with guidelines for the proper use of body armor.

### 815.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to maximize officer safety through the use of body armor in combination with prescribed safety procedures. While body armor provides a significant level of protection, it is not a substitute for the observance of officer safety procedures.

### 815.3 ISSUANCE OF BODY ARMOR

Bureau supervisor's shall ensure that body armor is issued to all investigators when the investigator begins service at the Stanislaus County District Attorney's Office and that, when issued, the body armor meets or exceeds the standards of the National Institute of Justice.

Bureau supervisor's shall remind their personnel to periodically check the dates on their issued body armor to ensure the replacement of the body armor is pursuant to the manufacturers suggested replacement time frame or whenever the body armor becomes worn or damaged to the point that its effectiveness or functionality has been compromised.

#### 815.3.1 USE OF SOFT BODY ARMOR

Generally, the use of body armor is required subject to the following:

- (a) Investigators shall only wear agency-approved body armor.
- (b) Investigators shall wear body armor anytime they are in a situation where they could reasonably be expected to take enforcement action.
- (c) Investigators may be excused from wearing body armor when they are functioning primarily in an administrative or support capacity and could not reasonably be expected to take enforcement action.
- (d) Body armor shall be worn when an investigator is working in uniform or taking part in Bureau range training.
- (e) An investigator may be excused from wearing body armor when he/she is involved in undercover or plainclothes work that his/her supervisor determines could be compromised by wearing body armor, or when a supervisor determines that other circumstances make it inappropriate to mandate wearing body armor.

#### 815.3.2 INSPECTIONS OF BODY ARMOR

Supervisors should ensure that body armor is worn and maintained in accordance with this policy through routine observation and periodic documented inspections. Bureau employees should

# Stanislaus County District Attorney's Office

## Policy Manual

### *Body Armor*

---

routinely inspect their issued body armor for fit, cleanliness, and signs of damage, abuse and wear. Members should report any damage to the body armor to a supervisor immediately.

#### **815.3.3 CARE AND MAINTENANCE OF SOFT BODY ARMOR**

Soft body armor should never be stored for any period of time in an area where environmental conditions (e.g., temperature, light, humidity) are not reasonably controlled (e.g., normal ambient room temperature/humidity conditions), such as in automobiles or automobile trunks.

Soft body armor should be cared for and cleaned pursuant to the manufacturer's care instructions provided with the soft body armor. The instructions can be found on labels located on the external surface of each ballistic panel. The carrier should also have a label that contains care instructions. Failure to follow these instructions may damage the ballistic performance capabilities of the armor. If care instructions for the soft body armor cannot be located, contact the manufacturer to request care instructions.

Soft body armor should not be exposed to any cleaning agents or methods not specifically recommended by the manufacturer, as noted on the armor panel label.

Soft body armor should be replaced in accordance with the manufacturer's recommended replacement schedule.

#### **815.4 RANGEMASTER RESPONSIBILITIES**

The Rangemaster should:

- (a) Monitor technological advances in the body armor industry for any appropriate changes to Bureau approved body armor.
- (b) Assess weapons and ammunition currently in use and the suitability of approved body armor to protect against those threats.
- (c) Provide training that educates investigators about the safety benefits of wearing body armor.

## Personnel Records

### 816.1 PURPOSE AND SCOPE

This policy governs maintenance and access to personnel records. Personnel records include any file maintained under an individual member's name.

### 816.2 POLICY

It is the policy of this bureau to maintain personnel records and preserve the confidentiality of personnel records pursuant to the Constitution and the laws of California (Penal Code § 832.7).

### 816.3 BUREAU FILE

The bureau file shall be maintained as a record of a person's employment/appointment with this bureau. The bureau file should contain, at a minimum:

- (a) Personal data, including photographs, marital status, names of family members, educational and employment history, or similar information. A photograph of the member should be permanently retained.
- (b) Election of employee benefits.
- (c) Personnel action reports reflecting assignments, promotions, and other changes in employment/appointment status. These should be permanently retained.
- (d) Original performance evaluations. These should be permanently retained.
- (e) Discipline records, including copies of sustained personnel complaints (see the Personnel Complaints Policy).
  - 1. Disciplinary action resulting from sustained internally initiated complaints or observation of misconduct shall be maintained pursuant to the established records retention schedule and at least four years (Government Code § 12946).
  - 2. Disciplinary action resulting from a sustained civilian's complaint involving misconduct shall be maintained pursuant to the established records retention schedule and at least 15 years (Penal Code § 832.5).
  - 3. A civilian's complaint involving misconduct that was not sustained shall be maintained pursuant to the established records retention schedule and at least five years (Penal Code § 832.5).
- (f) Adverse comments such as supervisor notes or memos may be retained in the bureau file after the member has had the opportunity to read and initial the comment (Government Code § 3305).
  - 1. Once a member has had an opportunity to read and initial any adverse comment, the member shall be given the opportunity to respond in writing to the adverse comment within 30 days (Government Code § 3306).
  - 2. Any member response shall be attached to and retained with the original adverse comment (Government Code § 3306).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Records*

---

3. If a member refuses to initial or sign an adverse comment, at least one supervisor should note the date and time of such refusal on the original comment and the member should sign or initial the noted refusal. Such a refusal, however, shall not be deemed insubordination, nor shall it prohibit the entry of the adverse comment into the member's file (Government Code § 3305).
- (g) Commendations and awards.
- (h) Any other information, the disclosure of which would constitute an unwarranted invasion of personal privacy.

#### **816.4 BUREAU FILE**

Bureau files may be separately maintained internally by a member's supervisor for the purpose of completing timely performance evaluations. The Bureau file may contain supervisor comments, notes, notices to correct and other materials that are intended to serve as a foundation for the completion of timely performance evaluations.

All materials intended for this interim file shall be provided to the employee prior to being placed in the file in accordance with Government Code § 3305 and Government Code § 3306.

#### **816.5 TRAINING FILE**

An individual training file shall be maintained by the Lieutenant for each member. Training files will contain records of all training; original or photocopies of available certificates, transcripts, diplomas and other documentation; and education and firearms qualifications. Training records may also be created and stored remotely, either manually or automatically (e.g., Daily Training Bulletin (DTB) records).

- (a) The involved member is responsible for providing the Lieutenant or immediate supervisor with evidence of completed training/education in a timely manner.
- (b) The Lieutenant or supervisor shall ensure that copies of such training records are placed in the member's training file.

#### **816.6 INTERNAL AFFAIRS FILE**

Internal affairs files shall be maintained under the exclusive control of the Lieutenant in conjunction with the office of the Chief of Investigations. Access to these files may only be approved by the Chief of Investigations.

These files shall contain the complete investigation of all formal complaints of member misconduct, regardless of disposition (Penal Code § 832.12). Investigations of complaints that result in the following findings shall not be placed in the member's file but will be maintained in the internal affairs file:

- (a) Not sustained
- (b) Unfounded
- (c) Exonerated
- (d) Sustained

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Records*

---

Investigation files arising out of sustained civilian's complaints involving misconduct shall be maintained pursuant to the established records retention schedule and for a period of at least 15 years. Investigations that resulted in other than a sustained finding may not be used by the Bureau to adversely affect an employee's career (Penal Code § 832.5).

Investigation files arising out of internally generated complaints shall be maintained pursuant to the established records retention schedule and for at least four years (Government Code § 12946).

Investigation files arising out of a civilian complaint involving misconduct that was not sustained shall be maintained pursuant to the established records retention schedule and for at least five years (Penal Code § 832.5).

#### **816.7 SECURITY**

Personnel records should be maintained in a secured location and locked either in a cabinet or access-controlled room. Personnel records maintained in an electronic format should have adequate password protection.

Personnel records are subject to disclosure only as provided in this policy, the Records Maintenance and Release Policy or according to applicable discovery procedures.

Nothing in this policy is intended to preclude review of personnel records by the County Executive, County Counsel or other attorneys or representatives of the County in connection with official business.

##### **816.7.1 REQUESTS FOR DISCLOSURE**

Any member receiving a request for a personnel record shall promptly notify the Custodian of Records or other person charged with the maintenance of such records.

Upon receipt of any such request, the responsible person shall notify the affected member as soon as practicable that such a request has been made (Evidence Code § 1043).

The responsible person shall further ensure that an appropriate response to the request is made in a timely manner, consistent with applicable law. In many cases, this may require assistance of available legal counsel.

All requests for disclosure that result in access to a member's personnel records shall be logged in the corresponding file.

##### **816.7.2 RELEASE OF PERSONNEL INFORMATION**

Personnel records shall not be disclosed except as allowed by law (Penal Code § 832.7; Evidence Code § 1043) (see also Records Maintenance and Release Policy).

Any person who maliciously, and with the intent to obstruct justice or the due administration of the laws, publishes, disseminates, or otherwise discloses the residence address or telephone number of any member of this bureau may be guilty of a misdemeanor (Penal Code § 146e).

The Bureau may release any factual information concerning a disciplinary investigation if the member who is the subject of the investigation (or the member's representative) publicly makes

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Records*

---

a statement that is published in the media and that the member (or representative) knows to be false. The disclosure of such information, if any, shall be limited to facts that refute any such false statement (Penal Code § 832.7).

The Bureau may, without a request, disclose to the public the cause of termination for a disclosable incident involving a former investigator, as permitted by law (Penal Code § 832.7(b)(13)).

#### **816.7.3 RELEASE OF LAW ENFORCEMENT GANG INFORMATION**

Information relating to the termination of an investigator from this bureau for participation in a law enforcement gang shall be disclosed to another law enforcement agency that is conducting a pre-employment background investigation except where specifically prohibited by law (Penal Code § 13670).

#### **816.7.4 RELEASE OF PEACE OFFICER RECORDS RELATING TO HATE COMPLAINTS**

Records relating to an investigator for an investigation of a hate complaint described in Penal Code § 13682 with a sustained finding that the investigator engaged in membership in a hate group, participated in a hate group activity, or advocacy of public expressions of hate are not confidential and shall be made available for public inspection through a public records request (Penal Code § 13683).

Records disclosed may be redacted as provided in Penal Code § 13683.

#### **816.8 RELEASE OF PERSONNEL RECORDS AND RECORDS RELATED TO CERTAIN INCIDENTS, COMPLAINTS, AND INVESTIGATIONS OF INVESTIGATORS**

Personnel records and records related to certain incidents, complaints, and investigations of investigators shall be released pursuant to a proper request under the Public Records Act and subject to redaction and delayed release as provided by law.

The Custodian of Records should work as appropriate with the Chief of Investigations or the Lieutenant supervisor in determining what records may qualify for disclosure when a request for records is received and if the requested record is subject to redaction or delay from disclosure.

For purposes of this section, a record includes (Penal Code § 832.7(b)(3):

- All investigation reports.
- Photographic, audio, and video evidence.
- Transcripts or recordings of interviews.
- Autopsy reports.
- All materials compiled and presented for review to the District Attorney or to any person or body charged with determining whether to file criminal charges against an investigator in connection with an incident, whether the investigator's action was consistent with law and bureau policy for purposes of discipline or administrative action, or what discipline to impose or corrective action to take.
- Documents setting forth findings or recommending findings.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Records*

---

- Copies of disciplinary records relating to the incident, including any letters of intent to impose discipline, any documents reflecting modifications of discipline due to the *Skelly* or grievance process, and letters indicating final imposition of discipline or other documentation reflecting implementation of corrective action.

Unless a record or information is confidential or qualifies for delayed disclosure as provided by Penal Code § 832.7(b)(8) or other law, the following records (hereinafter qualifying records) shall be made available for public inspection no later than 45 days from the date of a request (Penal Code § 832.7(b)(1)):

- (a) Records relating to the report, investigation, or findings of:
  1. The discharge of a firearm at another person by an investigator.
  2. The use of force against a person resulting in death or in great bodily injury (as defined by Penal Code § 243(f)(4)) by an investigator.
  3. A sustained finding involving a complaint that alleges unreasonable or excessive force.
  4. A sustained finding that an investigator failed to intervene against another investigator using force that is clearly unreasonable or excessive.
- (b) Records relating to an incident where a sustained finding was made by the Bureau or oversight agency regarding:
  1. An investigator engaged in sexual assault of a member of the public (as defined by Penal Code § 832.7(b)).
  2. Dishonesty of an investigator relating to the reporting, investigation, or prosecution of a crime, or directly relating to the reporting of, or investigation of misconduct by, another investigator, including but not limited to any false statements, filing false reports, destruction, falsifying, or concealing of evidence, or perjury.
  3. An investigator engaged in conduct including but not limited to verbal statements, writings, online posts, recordings, and gestures involving prejudice or discrimination against a person on the basis of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status.
  4. An investigator made an unlawful arrest or conducted an unlawful search.

Qualifying records will be made available regardless of whether the investigator resigns before the Bureau or an oversight agency concludes its investigation (Penal Code § 832.7(b)(3)).

A record from a separate and prior investigation or assessment of a separate incident shall not be released unless it is independently subject to disclosure (Penal Code § 832.7(b)(4)).

When an investigation involves multiple investigators, the Bureau shall not release information about allegations of misconduct or the analysis or disposition of an investigation of an investigator unless it relates to a sustained finding of a qualified allegation as provided by Penal Code §

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Records*

---

832.7(b)(5). However, factual information about the action of the investigator during an incident or the statements of an investigator shall be released if the statements are relevant to a finding of the qualified allegation against another investigator that is subject to release (Penal Code § 832.7(b)(5)).

#### 816.8.1 REDACTION

The Custodian of Records, in consultation with the Chief of Investigations or authorized designee, shall redact the following portions of qualifying records made available for release (Penal Code § 832.7(b)(6)):

- (a) Personal data or information (e.g., home address, telephone number, identities of family members) other than the names and work-related information of investigators
- (b) Information that would compromise the anonymity of whistleblowers, complainants, victims, and witnesses
- (c) Confidential medical, financial, or other information where disclosure is prohibited by federal law or would cause an unwarranted invasion of personal privacy that clearly outweighs the strong public interest in records about possible misconduct and use of force
- (d) Where there is a specific, articulable, and particularized reason to believe that disclosure of the record would pose a significant danger to the physical safety of the investigator or another person

Additionally, a record may be redacted, including redacting personal identifying information, where, on the facts of the particular case, the public interest served by not disclosing the information clearly outweighs the public interest served by disclosing it (Penal Code § 832.7(b)(7)).

#### 816.8.2 DELAY OF RELEASE

Unless otherwise directed by the Chief of Investigations, the Custodian of Records should consult with a supervisor familiar with the underlying investigation to determine whether to delay disclosure of qualifying records due to any of the following conditions (Penal Code § 832.7):

- (a) Active criminal investigations
  - 1. Disclosure may be delayed 60 days from the date the misconduct or use of force occurred or until the District Attorney determines whether to file criminal charges, whichever occurs sooner.
  - 2. After the initial 60 days, delay of disclosure may be continued if the disclosure could reasonably be expected to interfere with a criminal enforcement proceeding against an investigator or against someone other than an investigator who engaged in misconduct or used the force.
- (b) Filed criminal charges
  - 1. When charges are filed related to an incident in which misconduct occurred or force was used, disclosure may be delayed until a verdict on those charges is returned at trial or, if a plea of guilty or no contest is entered, the time to withdraw the plea has passed.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Records*

---

(c) Administrative investigations

1. Disclosure may be delayed until:

- (a) There is a determination from the investigation whether the misconduct or use of force violated law or bureau policy, but no longer than 180 days after the date of the bureau's discovery of the misconduct or use of force or allegation of misconduct or use of force

#### **816.8.3 NOTICE OF DELAY OF RECORDS**

When there is justification for delay of disclosure of qualifying records, the Custodian of Records shall provide written notice of the reason for any delay to a requester as follows (Penal Code § 832.7):

- (a) Provide the specific basis for the determination that the interest in delaying disclosure clearly outweighs the public interest in disclosure. The notice shall also include the estimated date for the disclosure of the withheld information.
- (b) When delay is continued beyond the initial 60 days because of criminal enforcement proceedings against anyone, at 180-day intervals provide the specific basis that disclosure could reasonably be expected to interfere with a criminal enforcement proceeding and the estimated date for disclosure.
1. Information withheld shall be disclosed when the specific basis for withholding the information is resolved, the investigation or proceeding is no longer active, or no later than 18 months after the date of the incident, whichever occurs sooner, unless:
- (a) When the criminal proceeding is against someone other than an investigator and there are extraordinary circumstances to warrant a continued delay due to the ongoing criminal investigation or proceeding, then the Bureau must show by clear and convincing evidence that the interest in preventing prejudice to the active and ongoing criminal investigation or proceeding outweighs the public interest for prompt disclosure of records about misconduct or use of force by investigators.

In cases where an action to compel disclosure is brought pursuant to Government Code § 7923.000, the Bureau may justify delay by filing an application to seal the basis for withholding if disclosure of the written basis itself would impact a privilege or compromise a pending investigation (Penal Code § 832.7(b)(8)).

#### **816.9 MEMBERS' ACCESS TO THEIR PERSONNEL RECORDS**

Any member may request access to the member's own personnel records during the normal business hours of those responsible for maintaining such files. Any member seeking the removal of any item from the member's personnel records shall file a written request to the Chief of Investigations through the chain of command. The Bureau shall remove any such item if appropriate, or within 30 days provide the member with a written explanation of why the contested item will not be removed. If the contested item is not removed from the file, the member's request

# Stanislaus County District Attorney's Office

## Policy Manual

### *Personnel Records*

---

and the written response from the Bureau shall be retained with the contested item in the member's corresponding personnel record (Government Code § 3306.5).

Members may be restricted from accessing files containing any of the following information:

- (a) An ongoing internal affairs investigation to the extent that it could jeopardize or compromise the investigation pending final disposition or notice to the member of the intent to discipline.
- (b) Confidential portions of internal affairs files that have not been sustained against the member.
- (c) Criminal investigations involving the member.
- (d) Letters of reference concerning employment/appointment, licensing, or issuance of permits regarding the member.
- (e) Any portion of a test document, except the cumulative total test score for either a section of the test document or for the entire test document.
- (f) Materials used by the Bureau for staff management planning, including judgments or recommendations concerning future salary increases and other wage treatments, management bonus plans, promotions and job assignments, or other comments or ratings used for department planning purposes.
- (g) Information of a personal nature about a person other than the member if disclosure of the information would constitute a clearly unwarranted invasion of the other person's privacy.
- (h) Records relevant to any other pending claim between the Bureau and the member that may be discovered in a judicial proceeding.

#### **816.10 RETENTION AND PURGING**

Unless provided otherwise in this policy, personnel records shall be maintained in accordance with the established records retention schedule.

- (a) During the preparation of each member's performance evaluation, all personnel complaints and disciplinary actions should be reviewed to determine the relevancy, if any, to progressive discipline, training and career development. Each supervisor responsible for completing the member's performance evaluation should determine whether any prior sustained disciplinary file should be retained beyond the required period for reasons other than pending litigation or other ongoing legal proceedings.
- (b) If a supervisor determines that records of prior discipline should be retained beyond the required period, approval for such retention should be obtained through the chain of command from the Chief of Investigations.
- (c) If, in the opinion of the Chief of Investigations, a personnel complaint or disciplinary action maintained beyond the required retention period is no longer relevant, all records of such matter may be destroyed in accordance with the established records retention schedule.

# Lactation Breaks

## **819.1 PURPOSE AND SCOPE**

The purpose of this policy is to provide guidance regarding reasonable accommodations for lactating members (Labor Code § 1034).

## **819.2 POLICY**

It is the policy of the Stanislaus County District Attorney's Office to provide, in compliance with federal and state law, reasonable accommodations for lactating members. This includes break time and appropriate facilities to accommodate any member desiring to express breast milk for the member's nursing child (29 USC § 218d; 42 USC § 2000gg-1; 29 CFR 1636.3; Labor Code § 1030).

## **819.3 LACTATION BREAK TIME**

A rest period should be permitted each time the member requires a lactation break (29 USC § 218d; 42 USC § 2000gg-1; 29 CFR 1636.3; Labor Code § 1030). In general, lactation breaks that cumulatively total 30 minutes or less during any four-hour work period or major portion of a four-hour work period would be considered reasonable. However, individual circumstances may require more or less time.

Lactation breaks, if feasible, should be taken at the same time as the member's regularly scheduled rest or meal periods. While a reasonable effort will be made to provide additional time beyond authorized breaks, any such time exceeding regularly scheduled and paid break time will be unpaid (Labor Code § 1030).

Members desiring to take a lactation break shall notify the dispatcher or a supervisor prior to taking such a break. Such breaks may be reasonably delayed if they would seriously disrupt bureau operations (Labor Code § 1032).

Once a lactation break has been approved, the break should not be interrupted except for emergency or exigent circumstances.

## **819.4 PRIVATE LOCATION**

The Bureau will make reasonable efforts to accommodate members with the use of an appropriate room or other location to express milk in private. Such room or place should be in proximity to the member's work area and shall be other than a bathroom or toilet stall. The location must be shielded from view, free from intrusion from coworkers and the public, and otherwise satisfy the requirements of federal and state law (29 USC § 218d; 42 USC § 2000gg-1; 29 CFR 1636.3; Labor Code § 1031).

Members occupying such private areas shall either secure the door or otherwise make it clear to others that the area is occupied with a need for privacy. All other members should avoid interrupting a member during an authorized break, except to announce an emergency or other urgent circumstance.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Lactation Breaks*

---

Authorized lactation breaks for members assigned to the field may be taken at the nearest appropriate private area.

#### **819.5 STORAGE OF EXPRESSED MILK**

Any member storing expressed milk in any authorized refrigerated area within the Bureau shall clearly label it as such and shall remove it when the member's shift ends.

##### **819.5.1 STATE REQUIREMENTS**

Members have the right to request lactation accommodations. If a break time or location accommodation cannot be provided, the supervisor shall provide the member with a written response regarding the reasons for the determination (Labor Code § 1034).

Lactation rooms or other locations should comply with the prescribed feature and access requirements of Labor Code § 1031.

Members who believe that their rights have been violated under this policy or have been the subject of discrimination or retaliation for exercising or attempting to exercise their rights under this policy, are encouraged to follow the chain of command in reporting a violation, but may also file a complaint directly with the Labor Commissioner (Labor Code § 1033).

# Overtime Compensation Requests

## 821.1 PURPOSE AND SCOPE

It is the policy of the Bureau to compensate non-exempt salaried employees who work authorized overtime either by payment of wages as agreed and in effect through the Memorandum of Understanding (MOU), or by the allowance of accrual of compensatory time off. In order to qualify for either, the employee must complete and submit their electronic timesheet as soon as practical after overtime is worked.

### 821.1.1 BUREAU POLICY

Because of the nature of the work performed by members of the Bureau,, and the specific needs of the Bureau, a degree of flexibility concerning overtime policies must be maintained.

Non-exempt employees are not authorized to volunteer work time to the Bureau. All requests to work overtime shall be approved in advance by a supervisor. If circumstances do not permit prior approval, then approval shall be sought as soon as practical during the overtime shift and in no case later than the end of shift in which the overtime is worked.

Short periods of work at the end of the normal duty day (e.g., less than one hour in duration) may be handled unofficially between the supervisor and the employee by flexing a subsequent shift schedule to compensate for the time worked rather than by submitting requests for overtime payments. If the supervisor authorizes or directs the employee to complete a form for such a period, the employee shall comply.

The individual employee may request compensatory time in lieu of receiving overtime payment, however, the employee may not exceed the hours of compensatory time as outlined in their association's Memorandum of Understanding (MOU).

## 821.2 REQUEST FOR OVERTIME COMPENSATION

Employees shall submit all overtime compensation requests to their immediate supervisors as soon as practicable for verification.

Failure to submit a request for overtime compensation in a timely manner may result in discipline.

### 821.2.1 EMPLOYEES RESPONSIBILITY

Employees shall complete the requests when time sheets are due and turn them in to their immediate supervisor.

### 821.2.2 SUPERVISORS RESPONSIBILITY

The supervisor who verifies the overtime earned shall verify that the overtime was worked before approving the request.

### *Overtime Compensation Requests*

---

#### **821.3 ACCOUNTING FOR OVERTIME WORKED**

Employees are to record the actual time worked in an overtime status. In some cases, the Memorandum of Understanding provides that a minimum number of hours will be paid, (e.g., two hours for Court, four hours for outside overtime).

##### **821.3.1 VARIATION IN TIME REPORTED**

Where two or more employees are assigned to the same activity, case, or court trial and the amount of time for which payment is requested varies from that reported by the other investigator, the employee's Lieutenant or other approving supervisor may require each employee explain the reason for the variation.

## Outside Employment

### 822.1 PURPOSE AND SCOPE

In order to avoid actual or perceived conflicts of interest for bureau employees engaging in outside employment, all employees shall obtain written approval from the Chief of Investigations prior to engaging in any outside employment. Approval of outside employment shall be at the discretion of the Chief of Investigations in accordance with the provisions of this policy.

#### 822.1.1 DEFINITIONS

**Outside Employment** - Any member of this bureau who receives wages, compensation or other consideration of value from another employer, organization or individual not affiliated directly with this bureau for services, product(s) or benefits rendered. For purposes of this section, the definition of outside employment includes those employees who are self-employed and not affiliated directly with this bureau for services, product(s) or benefits rendered.

**Outside Overtime** - Any member of this bureau who performs duties or services on behalf of an outside organization, company, or individual within this jurisdiction. Such outside overtime shall be requested and scheduled directly through this bureau so that the Bureau may be reimbursed for the cost of wages and benefits.

### 822.2 OBTAINING APPROVAL

No member of this bureau may engage in any outside employment without first obtaining prior written approval of the Chief of Investigations. Failure to obtain prior written approval for outside employment or engaging in outside employment prohibited by this policy may lead to disciplinary action.

In order to obtain approval for outside employment, the employee must complete an Outside Employment Application which shall be submitted to the employee's immediate supervisor. The Outside Employment Application will then be forwarded through channels to the Chief of Investigations for consideration.

If approved, the employee will be provided with approval in writing. Unless otherwise indicated in writing, approval will be valid through the end of the calendar year in which the employment is approved. Any employee seeking to renew an approval shall submit a new Outside Employment memorandum in a timely manner.

Any employee seeking approval of outside employment, whose request has been denied, shall be provided with a written reason for the denial of the application at the time of the denial (Penal Code § 70(e)(3)).

#### 822.2.1 APPEAL OF DENIAL OF OUTSIDE EMPLOYMENT

If an employee's Outside Employment Application is denied or withdrawn by the Bureau, the employee may file a written notice of appeal to the Chief of Investigations within ten days of the date of denial.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Outside Employment*

---

If the employee's appeal is denied, the employee may file a grievance pursuant to the procedure set forth in the current Memorandum of Understanding (MOU).

#### **822.2.2 REVOCATION/SUSPENSION OF OUTSIDE EMPLOYMENT PERMITS**

Any approved outside employment may be revoked or suspended under the following circumstances:

- (a) Should an employee's performance at this bureau decline to a point where it is evaluated by a supervisor as needing improvement to reach an overall level of competency, the Chief of Investigations may, at his or her discretion, revoke any previously approved outside employment. That revocation will stand until the employee's performance has been reestablished at a satisfactory level and his/her supervisor recommends reinstatement of the outside employment.
- (b) Suspension or revocation of a previously approved outside employment request may be included as a term or condition of sustained discipline.
- (c) If, at any time during the term of a valid outside employment, an employee's conduct or outside employment conflicts with the provisions of bureau policy, the permit may be suspended or revoked.
- (d) When an employee is unable to perform at a full duty capacity due to an injury or other condition, any previously approved outside employment permit may be subject to similar restrictions as those applicable to the employee's full time duties until the employee has returned to a full duty status.

#### **822.3 PROHIBITED OUTSIDE EMPLOYMENT**

Consistent with the provisions of Government Code § 1126, the Bureau expressly reserves the right to deny any Outside Employment Application submitted by an employee seeking to engage in any activity which:

- (a) Involves the employee's use of bureau time, facilities, equipment or supplies, the use of the Bureau badge, uniform, prestige or influence for private gain or advantage.
- (b) Involves the employee's receipt or acceptance of any money or other consideration from anyone other than this bureau for the performance of an act which the employee, if not performing such act, would be required or expected to render in the regular course or hours of employment or as a part of the employee's duties as a member of this bureau.
- (c) Involves the performance of an act in other than the employee's capacity as a member of this bureau that may later be subject directly or indirectly to the control, inspection, review, audit or enforcement of any other employee of this bureau.
- (d) Involves time demands that would render performance of the employee's duties for this bureau less efficient.

#### **822.3.1 OUTSIDE SECURITY AND PEACE OFFICER EMPLOYMENT**

Consistent with the provisions of Penal Code § 70, and because it would further create a potential conflict of interest, no member of this bureau may engage in any outside or secondary employment as a private security guard, private investigator or other similar private security position.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Outside Employment*

---

Any private organization, entity or individual seeking special services for security or traffic control from members of this bureau must submit a written request to the Chief of Investigations in advance of the desired service. Such outside extra duty overtime assignments will be assigned, monitored and paid through the Bureau.

- (a) The applicant will be required to enter into an indemnification agreement prior to approval.
- (b) The applicant will further be required to provide for the compensation and full benefits of all employees requested for such outside security services.
- (c) Should such a request be approved, any employee working outside overtime shall be subject to the following conditions:
  - 1. The investigator(s) shall wear the bureau uniform/identification.
  - 2. The investigator(s) shall be subject to the rules and regulations of this bureau.
  - 3. No investigator may engage in such outside employment during or at the site of a strike, lockout, picket, or other physical demonstration of a labor dispute.
  - 4. Compensation for such approved outside security services shall be pursuant to normal overtime procedures.
  - 5. Outside security services shall not be subject to the collective bargaining process.
  - 6. No investigator may engage in outside employment as a peace officer for any other public agency without prior written authorization of the Chief of Investigations.

#### **822.3.2 OUTSIDE OVERTIME ARREST AND REPORTING PROCEDURE**

Any employee making an arrest or taking other official police action while working in an approved outside overtime assignment shall be required to complete all related reports in a timely manner pursuant to bureau policy. Time spent on the completion of such reports shall be considered incidental to the outside overtime assignment.

#### **822.3.3 SPECIAL RESTRICTIONS**

Except for emergency situations or with prior authorization from a Bureau Lieutenant, undercover investigators or investigators assigned to covert operations shall not be eligible to work overtime or other assignments in a uniformed or other capacity which might reasonably disclose the investigator's law enforcement status.

#### **822.4 BUREAU RESOURCES**

Employees are prohibited from using any bureau equipment or resources in the course of or for the benefit of any outside employment. This shall include the prohibition of access to official records or databases of this bureau or other agencies through the use of the employee's position with this bureau.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Outside Employment*

---

#### **822.4.1 REVIEW OF FINANCIAL RECORDS**

Employees approved for outside employment expressly agree that their personal financial records may be requested and reviewed/audited for potential conflict of interest (Government Code § 3308; Government Code § 1126). Prior to providing written approval for an outside employment position, the Bureau may request that an employee provide his/her personal financial records for review/audit in order to determine whether a conflict of interest exists. Failure of the employee to provide the requested personal financial records could result in denial of the off-duty work approval. If, after approving a request for an outside employment position, the Bureau becomes concerned that a conflict of interest exists based on a financial reason, the Bureau may request that the employee provide his/her personal financial records for review/audit. If the employee elects not to provide the requested records, his/her off-duty work approval may be revoked pursuant to the Revocation/Suspension of Outside Employment Permits section of this policy.

#### **822.5 CHANGES IN OUTSIDE EMPLOYMENT STATUS**

If an employee terminates his or her outside employment during the period of a valid approval, the employee shall promptly submit written notification of such termination to the Chief of Investigations through channels. Any subsequent request for renewal or continued outside employment must thereafter be processed and approved through normal procedures set forth in this policy.

Employees shall also promptly submit in writing to the Chief of Investigations any material changes in outside employment including any change in the number of hours, type of duties, or demands of any approved outside employment. Employees who are uncertain whether a change in outside employment is material are advised to report the change.

#### **822.6 OUTSIDE EMPLOYMENT WHILE ON DISABILITY**

Bureau members engaged in outside employment who are placed on disability leave or modified/light-duty shall inform their immediate supervisor in writing within five days whether or not they intend to continue to engage in such outside employment while on such leave or light-duty status. The immediate supervisor shall review the duties of the outside employment along with any related doctor's orders, and make a recommendation to the Chief of Investigations whether such outside employment should continue.

In the event the Chief of Investigations determines that the outside employment should be discontinued or if the employee fails to promptly notify his/her supervisor of his/her intentions regarding their work approval, a notice of revocation of the member's approval will be forwarded to the involved employee, and a copy attached to the original work approval.

Criteria for revoking the outside employment include, but are not limited to, the following:

- (a) The outside employment is medically detrimental to the total recovery of the disabled member, as indicated by the County's professional medical advisors.
- (b) The outside employment performed requires the same or similar physical ability, as would be required of an on-duty member.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Outside Employment*

---

- (c) The employee's failure to make timely notice of their intentions to their supervisor.

When the disabled member returns to full duty with the Stanislaus County District Attorney's Office, a request (in writing) may be made to the Chief of Investigations to restore the approval.

## Personal Appearance Standards

### 824.1 PURPOSE AND SCOPE

In order to project uniformity and neutrality toward the public and other members of the bureau, employees shall maintain their personal hygiene and appearance to project a professional image appropriate for this bureau and for their assignment.

### 824.2 GROOMING STANDARDS

Unless otherwise stated and because deviations from these standards could present officer safety issues, the following appearance standards shall apply to all employees, except those whose current assignment would deem them not appropriate, and where the Chief of Investigations has granted exception.

#### 824.2.1 HAIR

Hairstyles of all investigators shall be clean and neat in appearance. Hair style should be a natural shade and in compliance with the investigator's current assignment.

#### 824.2.2 FACIAL HAIR

Mustaches and beards are to be kept neatly trimmed. The mustache shall not cover or extend over the upper lip or appear bushy. Facial hair shall be in compliance with the investigator's current assignment.

#### 824.2.3 FINGERNAILS

Fingernails extending beyond the tip of the finger can pose a safety hazard to investigators or others. Investigators should be aware of this potential hazard. Investigators must maintain their nails in a professional appearance. Fingernails shall be in compliance with the investigator's current assignment.

#### 824.2.4 JEWELRY

For the purpose of this policy, jewelry refers to rings, earrings, necklaces, bracelets, wristwatches, and tie tacks or tie bars. Jewelry shall present a professional image and may not create a safety concern for the bureau member or others. Jewelry that depicts racial, sexual, discriminatory, gang-related, or obscene language is not allowed.

- (a) Necklaces shall not be visible above the shirt collar.
- (b) Earrings shall be small and worn only in or on the earlobe.
- (c) One ring or ring set may be worn on each hand of the bureau member. No rings should be of the type that would cut or pose an unreasonable safety risk to the member or others during a physical altercation, if the member is assigned to a position where that may occur.
- (d) One small bracelet, including a bracelet identifying a medical condition, may be worn on one arm.
- (e) Wristwatches shall be conservative and present a professional image.

### *Personal Appearance Standards*

---

- (f) Tie tacks or tie bars worn with civilian attire shall be conservative and present a professional image.

#### **824.3 TATTOOS**

No face or neck tattoos are permitted. No visible tattoos with offensive or inappropriate logos, pictures, slogans or that would otherwise violate county policy.

#### **824.4 BODY PIERCING OR ALTERATION**

Body piercing or alteration to any area of the body visible in any authorized uniform or attire that is a deviation from normal anatomical features and which is not medically required is prohibited. Such body alteration includes, but is not limited to:

- (a) Tongue splitting or piercing.
- (b) The complete or transdermal implantation of any material other than hair replacement.
- (c) Abnormal shaping of the ears, eyes, nose or teeth
- (d) Branding or scarification.

#### **824.5 EXEMPTIONS**

Members who seek cultural (e.g., culturally protected hairstyles) or other exemptions to this policy that are protected by law should generally be accommodated (Government Code § 12926). A member with an exemption may be ineligible for an assignment if the individual accommodation presents a security or safety risk. The Chief of Investigations should be advised any time a request for such an accommodation is denied or when a member with a cultural or other exemption is denied an assignment based on a safety or security risk.

# Uniform Regulations

## 825.1 PURPOSE AND SCOPE

The uniform policy of the Stanislaus County District Attorney's Office is established to ensure that uniformed investigators will be readily identifiable to the public through the proper use and wearing of bureau uniforms. Employees should also refer to the following associated policies:

700 Bureau Owned and Personal Property

1012 Body Armor

1023 Personal Appearance Standards

The Uniform and Equipment Specifications manual is maintained and periodically updated by the Chief of Investigations or his/her designee. That manual should be consulted regarding authorized equipment and uniform specifications.

## 825.2 WEARING AND CONDITION OF UNIFORM AND EQUIPMENT

Investigator employees wear the uniform to be identified as the law enforcement authority in society. The uniform also serves an equally important purpose to identify the wearer as a source of assistance in an emergency, crisis, or other time of need.

- (a) Uniform and equipment shall be maintained in a serviceable condition and shall be ready at all times for immediate use. Uniforms shall be neat, clean, and appear professionally pressed.
- (b) All peace officers of this department shall possess and maintain at all times, a serviceable Class B uniform and the necessary equipment to perform uniformed field duty.
- (c) Personnel shall wear only the uniform specified for their rank and assignment (Penal Code § 13655).
- (d) All supervisors will perform periodic inspections of their personnel to ensure conformance to these regulations.
- (e) Uniforms are only to be worn while on duty, while in transit to or from work, for court, or at other official department functions or events.
- (f) If the uniform is worn while in transit, an outer garment shall be worn over the uniform shirt so as not to bring attention to the employee while he/she is off-duty.
- (g) Employees are not to purchase or drink alcoholic beverages while wearing the Class A or Class B uniform.
- (h) Visible jewelry, other than those items listed below, shall not be worn with the uniform unless specifically authorized by the Chief of Investigations or the authorized designee.
  - 1. Wrist watch
  - 2. Wedding ring, class ring, or other ring of tasteful design. A maximum of one ring/set may be worn on each hand

# Stanislaus County District Attorney's Office

## Policy Manual

### *Uniform Regulations*

---

3. Medical alert bracelet and one other jewelry bracelet is allowed.

#### 825.2.1 DEPARTMENT ISSUED IDENTIFICATION

The Department issues each employee an official department identification card bearing the employee's name, identifying information and photo likeness. All employees shall be in possession of their department issued identification card at all times while on duty or when carrying a concealed weapon.

- (a) Whenever on duty or acting in an official capacity representing the department, employees shall display their department issued identification in a courteous manner to any person upon request and as soon as practical.
- (b) Investigators working specialized assignments may be excused from the possession and display requirements when directed by their Lieutenant.

#### 825.3 UNIFORM CLASSES

##### 825.3.1 CLASS A UNIFORM

The Class A uniform is to be worn on special occasions such as funerals, graduations, ceremonies, or as directed. The Class A uniform is not required for sworn personnel. Class A uniforms are not issued to investigators and are not mandatory purchases. The Class A uniform includes the standard issue uniform with:

- (a) 100% wool navy blue long sleeve shirt with tie.
- (b) 100% wool navy blue pants.
- (c) Black leather basketweave belt and accessories with hidden snaps.
- (d) All hardware such as belt buckle, tie bar, nameplate, and rank insignia shall be chrome/silver.
- (e) Polished black leather shoes or boots.

Boots with pointed toes are not permitted.

##### 825.3.2 CLASS B UNIFORM

All investigators will possess and maintain a serviceable Class B uniform at all times.

The Class B uniform will consist of the following:

- (a) Navy blue Hard Drive Graphics brand polo shirt with badge patch sewn to chest. Long or short sleeve is acceptable.
- (b) A white or navy blue crew neck t-shirt worn underneath polo shirt
- (c) Khaki tactical pants 511, FirstTactical, or similar brand.
- (d) Tan or black tactical boots.
- (e) Boots with pointed toes are not permitted

# Stanislaus County District Attorney's Office

## Policy Manual

### *Uniform Regulations*

---

Sworn personnel are permitted to wear the class B polo with business attire such as dress pants and dress shoes. For the purposes of this policy, this is not considered the Class B uniform.

#### **825.3.3 CLASS C UNIFORM**

The Class C uniform is established to allow field personnel the ability to wear under cover clothing during assignments that require a non-uniform presence where citizens should not immediately recognize sworn staff as peace officers. Clothing varies based on assignment but can consist of a t-shirt and jeans as an example.

#### **825.4 INSIGNIA AND PATCHES**

- (a) **Shoulder Patches** - The authorized shoulder patch supplied by the Department shall be machine stitched to the sleeves of all uniform shirts and jackets, three-quarters of an inch below the shoulder seam of the shirt and be bisected by the crease in the sleeve.
- (b) **Service stripes, badge, etc.** - Each service stripe represents 5-years of law enforcement service and may be worn along the left forearm of long sleeved shirts and jackets. They are to be machine stitched onto the uniform. The bottom of the service stripe shall be sewn the width of one and one-half inches above the cuff seam with the rear of the service stripes sewn on the dress of the sleeve. The stripes are to be worn on the left sleeve only.
- (c) **The regulation nameplate, identifying the Criminal Investigator**, shall be worn at all times while in the Class A uniform. The nameplate shall display, at minimum, the employee's last name. Employees have the option to include their first name or initial of their first name on the nameplate. If the employee desires other than the legal first name, the employee must receive approval from the Chief of Investigations. The nameplate shall be worn and placed above the right pocket located in the middle, bisected by the pressed shirt seam, with equal distance from both sides of the nameplate to the outer edge of the pocket.
- (d) **Employees shall have at minimum, their last name embroidered on the Class B uniform polo.**
- (e) **Flag Pin** - A flag pin may be worn, centered above the nameplate.
- (f) **Badge** - The department issued badge, or an authorized sewn on cloth replica, must be worn and visible at all times while in uniform.
- (g) **Rank Insignia** - The designated insignia indicating the employee's rank must be worn at all times while in uniform. The Chief of Investigations may authorize exceptions.

#### **825.4.1 MOURNING BADGE**

Uniformed employees shall wear a black mourning band across the uniform badge whenever a law enforcement officer is killed in the line of duty. The following mourning periods will be observed:

- (a) **An investigator of this department** - From the time of death until midnight on the 14th day after the death.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Uniform Regulations*

---

- (b) An investigator from this or an adjacent county - From the time of death until midnight on the day of the funeral.
- (c) Funeral attendee - While attending the funeral of an out of region fallen officer.
- (d) National Peace Officers Memorial Day (May 15th) - From 0001 hours until 2359 hours.
- (e) As directed by the Chief of Investigations.

#### **825.5 CIVILIAN ATTIRE**

There are assignments within the Department that do not require the wearing of a uniform because recognition and authority are not essential to their function. There are also assignments in which the wearing of civilian attire is necessary.

- (a) All employees shall wear clothing that fits properly, is clean and free of stains, and not damaged or excessively worn.
- (b) All male administrative, investigative and support personnel who elect to wear civilian clothing to work shall wear button style shirts with a collar, slacks or suits that are moderate in style.
- (c) All female administrative, investigative, and support personnel who elect to wear civilian clothes to work shall wear dresses, slacks, shirts, blouses, or suits which are moderate in style.
- (d) The following items shall not be worn on duty:
  - 1. T-shirt alone
  - 2. Open toed sandals or thongs
  - 3. Swimsuit, tube tops, or halter-tops
  - 4. Spandex type pants or see-through clothing
  - 5. Distasteful printed slogans, buttons or pins
- (e) Variations from this order are allowed at the discretion of the Chief of Investigations or designee when the employee's assignment or current task is not conducive to the wearing of such clothing.
- (f) No item of civilian attire may be worn on duty that would adversely affect the reputation of the Stanislaus County District Attorney's Office or the morale of the employees.

#### **825.6 POLITICAL ACTIVITIES, ENDORSEMENTS, AND ADVERTISEMENTS**

Unless specifically authorized by the Chief of Investigations, Stanislaus County District Attorney's Office employees may not wear any part of the uniform, be photographed wearing any part of the uniform, utilize a department badge, patch or other official insignia, or cause to be posted, published, or displayed, the image of another employee, or identify himself/herself as an employee of the Stanislaus County District Attorney's Office to do any of the following (Government Code §§ 3206 and 3302):

- (a) Endorse, support, oppose, or contradict any political campaign or initiative.
- (b) Endorse, support, oppose, or contradict any social issue, cause, or religion.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Uniform Regulations*

---

- (c) Endorse, support, or oppose, any product, service, company or other commercial entity.
- (d) Appear in any commercial, social, or non-profit publication, or any motion picture, film, video, public broadcast, or any website.

#### **825.7 OPTIONAL EQUIPMENT - MAINTENANCE, AND REPLACEMENT**

- (a) Any of the items listed in the Uniform and Equipment Specifications as optional shall be purchased totally at the expense of the employee. No part of the purchase cost shall be offset by the Department for the cost of providing the Department issued item.
- (b) Maintenance of optional items shall be the financial responsibility of the purchasing employee. For example, repairs due to normal wear and tear.
- (c) Replacement of items listed in this order as optional shall be done as follows:
  - 1. When the item is no longer functional because of normal wear and tear, the employee bears the full cost of replacement.
  - 2. When the item is no longer functional because of damage in the course of the employee's duties, it shall be replaced following the procedures for the replacement of damaged personal property (see the Department Owned and Personal Property Policy).

##### **825.7.1 RETIREE BADGES**

The Chief of Investigations may issue identification in the form of a badge, insignia, emblem, device, label, certificate, card or writing that clearly states the person has honorably retired from the Stanislaus County District Attorney's Office. This identification is separate and distinct from the identification authorized by Penal Code § 25455 and referenced in the Retired Investigator CCW Endorsement Policy in this manual.

A badge issued to an honorably retired peace officer that is not affixed to a plaque or other memento will have the words "Honorably Retired" clearly visible on its face. A retiree shall be instructed that any such badge will remain the property of the Stanislaus County District Attorney's Office and will be revoked in the event of misuse or abuse (Penal Code § 538d).

#### **825.8 UNAUTHORIZED UNIFORMS, EQUIPMENT AND ACCESSORIES**

Stanislaus County District Attorney's Office employees may not wear any uniform item, accessory or attachment unless specifically authorized in the Uniform and Equipment Specifications or by the Chief of Investigations or designee.

Stanislaus County District Attorney's Office employees may not use or carry any safety item, tool or other piece of equipment unless specifically authorized in the Uniform and Equipment Specifications or by the Chief of Investigations or designee.

## Nepotism and Conflicting Relationships

### 826.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure equal opportunity and effective employment practices by avoiding actual or perceived favoritism, discrimination or actual or potential conflicts of interest by or between members of this bureau. These employment practices include: recruiting, testing, hiring, compensation, assignment, use of facilities, access to training opportunities, supervision, performance appraisal, discipline and workplace safety and security.

#### 826.1.1 DEFINITIONS

**Business relationship** - Serving as an employee, independent contractor, compensated consultant, owner, board member, shareholder, or investor in an outside business, company, partnership, corporation, venture or other transaction, where the Bureau employee's annual interest, compensation, investment or obligation is greater than \$250.

**Conflict of interest** - Any actual, perceived or potential conflict of interest in which it reasonably appears that a bureau employee's action, inaction or decisions are or may be influenced by the employee's personal or business relationship.

**Nepotism** - The practice of showing favoritism to relatives over others in appointment, employment, promotion or advancement by any public official in a position to influence these personnel decisions.

**Personal relationship** - Includes marriage, cohabitation, dating or any other intimate relationship beyond mere friendship.

**Public official** - A supervisor, officer or employee vested with authority by law, rule or regulation or to whom authority has been delegated.

**Relative** - An employee's parent, stepparent, spouse, domestic partner, significant other, child (natural, adopted or step), sibling or grandparent.

**Subordinate** - An employee who is subject to the temporary or ongoing direct or indirect authority of a supervisor.

**Supervisor** - An employee who has temporary or ongoing direct or indirect authority over the actions, decisions, evaluation and/or performance of a subordinate employee.

### 826.2 RESTRICTED DUTIES AND ASSIGNMENTS

The Bureau will not prohibit all personal or business relationships between employees. However, in order to avoid nepotism or other inappropriate conflicts, the following reasonable restrictions shall apply (Government Code § 12940):

- (a) Employees are prohibited from directly supervising, occupying a position in the line of supervision or being directly supervised by any other employee who is a relative or with whom they are involved in a personal or business relationship.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Nepotism and Conflicting Relationships*

---

1. If circumstances require that such a supervisor/subordinate relationship exist temporarily, the supervisor shall make every reasonable effort to defer matters pertaining to the involved employee to an uninvolved supervisor.
  2. When personnel and circumstances permit, the Bureau will attempt to make every reasonable effort to avoid placing employees in such supervisor/subordinate situations. The Bureau, however, reserves the right to transfer or reassign any employee to another position within the same classification in order to avoid conflicts with any provision of this policy.
- (b) Employees are prohibited from participating in, contributing to or recommending promotions, assignments, performance evaluations, transfers or other personnel decisions affecting an employee who is a relative or with whom they are involved in a personal or business relationship.
  - (c) Whenever possible, Bureau members and other trainers will not be assigned to train relatives. Bureau members and other trainers are prohibited from entering into or maintaining personal or business relationships with any employee they are assigned to train until such time as the training has been successfully completed and the employee is off probation.
  - (d) To avoid actual or perceived conflicts of interest, members of this bureau shall refrain from developing or maintaining personal or financial relationships with victims, witnesses or other individuals during the course of or as a direct result of any official contact.
  - (e) Except as required in the performance of official duties or, in the case of immediate relatives, employees shall not develop or maintain personal or financial relationships with any individual they know or reasonably should know is under criminal investigation, is a convicted felon, parolee, fugitive or registered sex offender or who engages in serious violations of state or federal laws.

#### 826.2.1 EMPLOYEE RESPONSIBILITY

Prior to entering into any personal or business relationship or other circumstance which the employee knows or reasonably should know could create a conflict of interest or other violation of this policy, the employee shall promptly notify his/her supervisor.

Whenever any employee is placed in circumstances that would require the employee to take enforcement action or provide official information or services to any relative or individual with whom the employee is involved in a personal or business relationship, the employee shall promptly notify a Bureau supervisor. In the event that no supervisor is immediately available, the employee shall promptly summons another uninvolved Bureau employee either relieve the involved employee or minimally remain present to witness the action. A written report shall be documented outlining all steps made and forwarded to a Bureau Lieutenant.

#### 826.2.2 SUPERVISOR'S RESPONSIBILITY

Upon being notified of, or otherwise becoming aware of any circumstance that could result in or constitute an actual or potential violation of this policy, a supervisor shall take all reasonable steps

# Stanislaus County District Attorney's Office

## Policy Manual

### *Nepotism and Conflicting Relationships*

---

to promptly mitigate or avoid such violations whenever possible. Supervisors shall also promptly notify the Chief of Investigations of such actual or potential violations.

## Bureau Badges

### 827.1 PURPOSE AND SCOPE

The Stanislaus County District Attorney's Office (SCDA) badge and uniform patch as well as logos and the likeness of these items and the name of the same, are property of the SCDA and their use shall be restricted as set forth in this policy.

### 827.2 POLICY

The SCDA badge shall be issued to criminal investigators and prosecutors. The SCDA badge is a symbol of authority and the use and display of the SCDA badges shall be in strict compliance with this policy. Only authorized badges issued by the SCDA shall be displayed, carried or worn by members while on duty or otherwise acting in an official or authorized capacity.

#### 827.2.1 FLAT BADGE

A SCDA flat badge is capable of being carried in a wallet. The use of the flat badge is subject to all the same provisions in this policy.

- (a) Should the flat badge become lost, damaged, or otherwise removed from the member's control, he/she shall make the proper notifications as outlined in the Policy 700, Owned and Personal Property Policy.
- (b) An honorably retired member may purchase his/her flat badge upon retirement.

#### 827.2.2 RETIREE UNIFORM BADGE

Upon honorable retirement employees may purchase his/her assigned duty badge for display purposes. It is intended that the duty badge be used only as private memorabilia as other uses of the badge may be unlawful or in violation of this policy.

### 827.3 UNAUTHORIZED USE

Except as required for on-duty use by current employees, no badge designed for carry or display in a wallet, badge case or similar holder shall be issued to anyone other than a current or honorably retired criminal investigator or prosecutor.

SCDA badges are issued to criminal investigators and prosecutors for official use only. The SCDA badge, shoulder patch, logo, or the likeness thereof, or the SCDA name shall not be used for personal or private reasons including, but not limited to, letters, memoranda, and electronic communications such as electronic mail or web sites and web pages.

The use of the badge, uniform patch and SCDA name for all material (printed matter, products or other items) developed for SCDA use shall be subject to approval by the District Attorney.

Employees shall not loan his/her SCDA badge or identification card to others and shall not permit the badge or identification card to be reproduced or duplicated.

### *Bureau Badges*

---

#### **827.4 PERMITTED USE BY EMPLOYEE GROUPS**

The likeness of the SCDA badge shall not be used without the expressed authorization of the District Attorney and shall be subject to the following:

- (a) The employee associations may use the likeness of the SCDA badge for merchandise and official association business provided they are used in a clear representation of the association and not the SCDA. The following modifications shall be included:
  - 1. The text on the upper and lower ribbons is replaced with the name of the employee association.
  - 2. The badge number portion displays the acronym of the employee association.
- (b) The likeness of the SCDA badge for endorsement of political candidates shall not be used without the expressed approval of the District Attorney.

# Temporary Modified-Duty Assignments

## 828.1 PURPOSE AND SCOPE

This policy establishes procedures for providing temporary modified-duty assignments. This policy is not intended to affect the rights or benefits of employees under federal or state law, County rules, current memorandums of understanding, or collective bargaining agreements. For example, nothing in this policy affects the obligation of the Bureau to engage in a good faith, interactive process to consider reasonable accommodations for any employee with a temporary or permanent disability or limitation that is protected under federal or state law.

## 828.2 POLICY

Subject to operational considerations, the Stanislaus County District Attorney's Office may identify temporary modified-duty assignments for employees who have an injury or medical condition resulting in temporary work limitations or restrictions. A temporary assignment allows the employee to work, while providing the Bureau with a productive employee during the temporary period.

## 828.3 GENERAL CONSIDERATIONS

Priority consideration for temporary modified-duty assignments will be given to employees with work-related injuries or illnesses that are temporary in nature. Employees having disabilities covered under the Americans with Disabilities Act (ADA) or the California Fair Employment and Housing Act (Government Code § 12940 et seq.) shall be treated equally, without regard to any preference for a work-related injury.

No position in the Stanislaus County District Attorney's Office shall be created or maintained as a temporary modified-duty assignment.

Temporary modified-duty assignments are a management prerogative and not an employee right. The availability of temporary modified-duty assignments will be determined on a case-by-case basis, consistent with the operational needs of the Bureau. Temporary modified-duty assignments are subject to continuous reassessment, with consideration given to operational needs and the employee's ability to perform in a modified-duty assignment.

The Chief of Investigations or the authorized designee may restrict employees working in temporary modified-duty assignments from wearing a uniform, displaying a badge, carrying a firearm, operating an emergency vehicle or engaging in outside employment, or may otherwise limit them in employing their peace officer powers.

Temporary modified-duty assignments shall generally not exceed a cumulative total of 1,040 hours in any one-year period.

## 828.4 PROCEDURE

Employees may request a temporary modified-duty assignment for short-term injuries or illnesses.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Modified-Duty Assignments*

---

Employees seeking a temporary modified-duty assignment should submit a written request to their Lieutenants or the authorized designees. The request should, as applicable, include a certification from the treating medical professional containing:

- (a) An assessment of the nature and probable duration of the illness or injury.
- (b) The prognosis for recovery.
- (c) The nature and scope of limitations and/or work restrictions.
- (d) A statement regarding any required workplace accommodations, mobility aids or medical devices.
- (e) A statement that the employee can safely perform the duties of the temporary modified-duty assignment.

The Lieutenant will make a recommendation through the chain of command to the Chief of Investigations regarding temporary modified-duty assignments that may be available based on the needs of the Bureau and the limitations of the employee. The Chief of Investigations or the authorized designee shall confer with the Human Resources or the County Counsel as appropriate.

Requests for a temporary modified-duty assignment of 20 hours or less per week may be approved and facilitated by the Lieutenant, with notice to the Chief of Investigations.

#### **828.5 ACCOUNTABILITY**

Written notification of assignments, work schedules and any restrictions should be provided to employees assigned to temporary modified-duty assignments and their supervisors. Those assignments and schedules may be adjusted to accommodate bureau operations and the employee's medical appointments, as mutually agreed upon with the Lieutenant.

##### **828.5.1 EMPLOYEE RESPONSIBILITIES**

The responsibilities of employees assigned to temporary modified duty shall include, but not be limited to:

- (a) Communicating and coordinating any required medical and physical therapy appointments in advance with their supervisors.
- (b) Promptly notifying their supervisors of any change in restrictions or limitations after each appointment with their treating medical professionals.
- (c) Communicating a status update to their supervisors no less than once every 30 days while assigned to temporary modified duty.
- (d) Submitting a written status report to the Lieutenant that contains a status update and anticipated date of return to full-duty when a temporary modified-duty assignment extends beyond 60 days.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Modified-Duty Assignments*

---

#### **828.5.2 SUPERVISOR RESPONSIBILITIES**

The employee's immediate supervisor shall monitor and manage the work schedule of those assigned to temporary modified duty.

The responsibilities of supervisors shall include, but not be limited to:

- (a) Periodically apprising the Lieutenant of the status and performance of employees assigned to temporary modified duty.
- (b) Notifying the Lieutenant and ensuring that the required documentation facilitating a return to full duty is received from the employee.
- (c) Ensuring that employees returning to full duty have completed any required training and certification.

#### **828.6 MEDICAL EXAMINATIONS**

Prior to returning to full-duty status, employees shall be required to provide certification from their treating medical professionals stating that they are medically cleared to perform the essential functions of their jobs without restrictions or limitations.

The Bureau may require a fitness-for-duty examination prior to returning an employee to full-duty status, in accordance with the Fitness for Duty Policy.

#### **828.7 PREGNANCY**

If an employee is temporarily unable to perform regular duties due to a pregnancy, childbirth, or a related medical condition, the employee will be treated the same as any other temporarily disabled employee (42 USC § 2000e(k)). A pregnant employee shall not be involuntarily transferred to a temporary modified-duty assignment. Nothing in this policy limits a pregnant employee's right to a temporary modified-duty assignment if required under Government Code § 12945.

If notified by an employee or the employee's representative regarding limitations related to pregnancy, childbirth, or related medical conditions, the Bureau should make reasonable efforts to provide an accommodation for the employee in accordance with federal and state law. The accommodation should be provided without unnecessary delay, as appropriate (42 USC § 2000gg-1; 29 CFR 1636.3; 29 CFR 1636.4; Government Code § 12945).

##### **828.7.1 NOTIFICATION**

Pregnant employees should notify their immediate supervisors as soon as practicable and provide a statement from their medical providers identifying any pregnancy-related job restrictions or limitations. If at any point during the pregnancy it becomes necessary for the employee to take a leave of absence, such leave shall be granted in accordance with the County's personnel rules and regulations regarding family and medical care leave.

#### **828.8 MAINTENANCE OF CERTIFICATION AND TRAINING**

Employees assigned to temporary modified duty shall maintain all certification, training and qualifications appropriate to both their regular and temporary duties, provided that the certification, training or qualifications are not in conflict with any medical limitations or restrictions. Employees

# Stanislaus County District Attorney's Office

## Policy Manual

### *Temporary Modified-Duty Assignments*

---

who are assigned to temporary modified duty shall inform their supervisors of any inability to maintain any certification, training or qualifications.

# Employee Speech, Expression and Social Networking

## 830.1 PURPOSE AND SCOPE

This policy is intended to address issues associated with employee use of social networking sites and to provide guidelines for the regulation and balancing of employee speech and expression with the needs of the Bureau.

Nothing in this policy is intended to prohibit or infringe upon any communication, speech or expression that is protected or privileged under law. This includes speech and expression protected under state or federal constitutions as well as labor or other applicable laws. For example, this policy does not limit an employee from speaking as a private citizen, including acting as an authorized member of a recognized bargaining unit or investigator associations, about matters of public concern, such as misconduct or corruption.

Employees are encouraged to consult with their supervisor regarding any questions arising from the application or potential application of this policy.

### 830.1.1 APPLICABILITY

This policy applies to all forms of communication including but not limited to film, video, print media, public or private speech, use of all internet services, including the World Wide Web, e-mail, file transfer, remote computer access, news services, social networking, social media, instant messaging, blogs, forums, video, and other file-sharing sites.

## 830.2 POLICY

Public employees occupy a trusted position in the community, and thus, their statements have the potential to contravene the policies and performance of this bureau. Due to the nature of the work and influence associated with the law enforcement profession, it is necessary that employees of this bureau be subject to certain reasonable limitations on their speech and expression. To achieve its mission and efficiently provide service to the public, the Stanislaus County District Attorney's Office (SCDA) will carefully balance the individual employee's rights against the Bureau's needs and interests when exercising a reasonable degree of control over its employees' speech and expression.

## 830.3 SAFETY

Employees should consider carefully the implications of their speech or any other form of expression when using the internet. Speech and expression that may negatively affect the safety of the Stanislaus County District Attorney's Office employees, such as posting personal information in a public forum, can result in compromising an employee's home address or family ties. Employees should therefore not disseminate or post any information on any forum or medium that could reasonably be anticipated to compromise the safety of any employee, an employee's family, or associates. Examples of the type of information that could reasonably be expected to compromise safety include:

# Stanislaus County District Attorney's Office

## Policy Manual

### *Employee Speech, Expression and Social Networking*

---

- Disclosing a photograph and name or address of an investigator who is working undercover.
- Disclosing the address of a fellow investigator.
- Otherwise disclosing where another investigator can be located off-duty.

#### **830.4 PROHIBITED SPEECH, EXPRESSION, AND CONDUCT**

To meet the bureau's safety, performance, and public-trust needs, the following are prohibited unless the speech is otherwise protected (for example, an employee speaking as a private citizen, including acting as an authorized member of a recognized bargaining unit or investigator associations, on a matter of public concern):

- (a) Speech or expression made pursuant to an official duty that tends to compromise or damage the mission, function, reputation, or professionalism of the Stanislaus County District Attorney's Office or its employees.
- (b) Speech or expression that, while not made pursuant to an official duty, is significantly linked to, or related to, the Stanislaus County District Attorney's Office and tends to compromise or damage the mission, function, reputation, or professionalism of the Stanislaus County District Attorney's Office or its employees. Examples may include:
  1. Statements that indicate disregard for the law or the state or U.S. Constitution.
  2. Expression that demonstrates support for criminal activity.
  3. Participating in sexually explicit photographs or videos for compensation or distribution.
- (c) Speech or expression that could reasonably be foreseen as having a negative impact on the credibility of the employee as a witness. For example, posting statements or expressions to a website that glorify or endorse dishonesty, unlawful discrimination, or illegal behavior.
- (d) Speech or expression of any form that could reasonably be foreseen as having a negative impact on the safety of the employees of the Bureau. For example, a statement on a blog that provides specific details as to how and when prisoner transportations are made could reasonably be foreseen as potentially jeopardizing employees by informing criminals of details that could facilitate an escape or attempted escape.
- (e) Speech or expression that is contrary to the canons of the Law Enforcement Code of Ethics as adopted by the Stanislaus County District Attorney's Office.
- (f) Use or disclosure, through whatever means, of any information, photograph, video, or other recording obtained or accessible as a result of employment with the Bureau for financial or personal gain, or any disclosure of such materials without the express authorization of the Chief of Investigations or the authorized designee.
- (g) Posting, transmitting, or disseminating any photographs, video or audio recordings, likenesses or images of bureau logos, emblems, uniforms, badges, patches, marked vehicles, equipment, or other material that specifically identifies the Stanislaus County

# Stanislaus County District Attorney's Office

## Policy Manual

### *Employee Speech, Expression and Social Networking*

---

District Attorney's Office on any personal or social networking or other website or web page, without the express authorization of the Chief of Investigations.

Employees must take reasonable and prompt action to remove any content, including content posted by others, that is in violation of this policy from any web page or website maintained by the employee (e.g., social or personal website).

#### **830.4.1 UNAUTHORIZED ENDORSEMENTS AND ADVERTISEMENTS**

While employees are not restricted from engaging in the following activities as private citizens or as authorized members of a recognized bargaining unit or investigator associations, employees may not represent the SCDA or identify themselves in any way that could be reasonably perceived as representing the SCDA in order to do any of the following, unless specifically authorized by the Chief of Investigations or the District Attorney (Government Code § 3206; Government Code § 3302):

- (a) Endorse, support, oppose or contradict any political campaign or initiative.
- (b) Endorse, support, oppose or contradict any social issue, cause or religion.
- (c) Endorse, support or oppose any product, service, company or other commercial entity.
- (d) Appear in any commercial, social or nonprofit publication or any motion picture, film, video, public broadcast or on any website.

Additionally, when it can reasonably be construed that an employee, acting in his/her individual capacity or through an outside group or organization (e.g., bargaining group or investigator associations), is affiliated with this bureau, the employee shall give a specific disclaiming statement that any such speech or expression is not representative of the SCDA.

Employees retain their right to vote as they choose, to support candidates of their choice and to express their opinions as private citizens, including as authorized members of a recognized bargaining unit or investigator associations, on political subjects and candidates at all times while off-duty.

However, employees may not use their official authority or influence to interfere with or affect the result of an election or a nomination for office. Employees are also prohibited from directly or indirectly using their official authority to coerce, command or advise another employee to pay, lend or contribute anything of value to a party, committee, organization, agency or person for political purposes (5 USC § 1502).

#### **830.5 PRIVACY EXPECTATION**

Employees forfeit any expectation of privacy with regard to e-mails, texts, or anything published or maintained through file-sharing software or any internet site (e.g., Facebook) that is accessed, transmitted, received, or reviewed on any county technology system (see the Information Technology Use Policy for additional guidance).

The Bureau shall not require an employee to disclose a personal user name or password for accessing personal social media or to open a personal social website; however, the Bureau may

### *Employee Speech, Expression and Social Networking*

---

request access when it is reasonably believed to be relevant to the investigation of allegations of work-related misconduct (Labor Code § 980).

#### **830.6 CONSIDERATIONS**

In determining whether to grant authorization of any speech or conduct that is prohibited under this policy, the factors that the Chief of Investigations or authorized designee should consider include:

- (a) Whether the speech or conduct would negatively affect the efficiency of delivering public services.
- (b) Whether the speech or conduct would be contrary to the good order of the SCDA or the efficiency or morale of its members.
- (c) Whether the speech or conduct would reflect unfavorably upon the SCDA.
- (d) Whether the speech or conduct would negatively affect the member's appearance of impartiality in the performance of his/her duties.
- (e) Whether similar speech or conduct has been previously authorized.
- (f) Whether the speech or conduct may be protected and outweighs any interest of the SCDA.

#### **830.7 TRAINING**

Subject to available resources, the Bureau should provide training regarding employee speech and the use of social networking to all members of the Bureau.

## Line-of-Duty Deaths

### 832.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance to members of the Stanislaus County District Attorney's Office in the event of the death of a member occurring in the line of duty and to direct the Bureau in providing proper support for the member's survivors.

The Chief of Investigations may also apply some or all of this policy for a non-line-of-duty member death, or in situations where members are injured in the line of duty and the injuries are life-threatening.

#### 832.1.1 DEFINITIONS

Definitions related to this policy include:

**Line-of-duty death** - The death of an investigator during the course of performing law enforcement-related functions while on- or off-duty, or a non-sworn member during the course of performing assigned duties.

For an investigator, a line-of-duty death includes death that is the direct and proximate result of a personal injury sustained in the line of duty (34 USC § 10281).

**Survivors** - Immediate family members of the deceased member, which can include spouse, children, parents, other next of kin, or significant others. The determination of who should be considered a survivor for purposes of this policy should be made on a case-by-case basis given the individual's relationship with the member and whether the individual was previously designated by the deceased member.

### 832.2 POLICY

It is the policy of the Stanislaus County District Attorney's Office to make appropriate notifications and to provide assistance and support to survivors and coworkers of a member who dies in the line of duty.

It is also the policy of this bureau to respect the requests of the survivors when they conflict with these guidelines, as appropriate.

### 832.3 INITIAL ACTIONS BY COMMAND STAFF

- (a) Upon learning of a line-of-duty death, the deceased member's supervisor should provide all reasonably available information to the Lieutenant and SR 911.
  - 1. Communication of information concerning the member and the incident should be restricted to secure networks to avoid interception by the media or others (see the Public Information Officer section of this policy).
- (b) The Lieutenant should ensure that notifications are made in accordance with the Officer-Involved Shootings and Deaths and Major Incident Notification policies as applicable.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Line-of-Duty Deaths*

---

- (c) If the member has been transported to the hospital, the Lieutenant or the authorized designee should respond to the hospital to assume temporary responsibilities as the Hospital Liaison.
- (d) The Chief of Investigations or the authorized designee should assign members to handle survivor notifications and assign members to the roles of Hospital Liaison (to relieve the temporary Hospital Liaison) and the Bureau Liaison as soon as practicable (see the Notifying Survivors section and the Bureau Liaison and Hospital Liaison subsections in this policy).

#### **832.4 NOTIFYING SURVIVORS**

Survivors should be notified as soon as possible in order to avoid the survivors hearing about the incident in other ways.

The Chief of Investigations or the authorized designee should review the deceased member's emergency contact information and make accommodations to respect the member's wishes and instructions specific to notifying survivors. However, notification should not be excessively delayed because of attempts to assemble a notification team in accordance with the member's wishes.

The Chief of Investigations, Lieutenant, or the authorized designee should select at least two members to conduct notification of survivors, one of which may be the Bureau chaplain.

Notifying members should:

- (a) Make notifications in a direct and compassionate manner, communicating as many facts of the incident as possible, including the current location of the member. Information that is not verified should not be provided until an investigation has been completed.
- (b) Determine the method of notifying surviving children by consulting with other survivors and taking into account factors such as the child's age, maturity, and current location (e.g., small children at home, children in school).
- (c) Plan for concerns such as known health concerns of survivors or language barriers.
- (d) Offer to transport survivors to the hospital, if appropriate. Survivors should be transported in bureau vehicles. Notifying members shall inform the Hospital Liaison over a secure network that the survivors are on their way to the hospital. Notifying members should remain at the hospital while the survivors are present.
- (e) When survivors are not at their residences or known places of employment, actively seek information and follow leads from neighbors, other law enforcement, postal authorities, and other sources of information in order to accomplish notification in as timely a fashion as possible. Notifying members shall not disclose the reason for their contact other than a family emergency.
- (f) If making notification at a survivor's workplace, ask a workplace supervisor for the use of a quiet, private room to meet with the survivor. Members shall not inform the workplace supervisor of the purpose of their visit other than to indicate that it is a family emergency.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Line-of-Duty Deaths*

---

- (g) Offer to call other survivors, friends, or clergy to support the survivors and to avoid leaving survivors alone after notification.
- (h) Assist the survivors with meeting child care or other immediate needs.
- (i) Provide other assistance to survivors and take reasonable measures to accommodate their needs, wishes, and desires. Care should be taken not to make promises or commitments to survivors that cannot be met.
- (j) Inform the survivors of the name and phone number of the Survivor Support Liaison (see the Survivor Support Liaison section of this policy), if known, and the Bureau Liaison.
- (k) Provide their contact information to the survivors before departing.
- (l) Document the survivors' names and contact information, as well as the time and location of notification. This information should be forwarded to the Bureau Liaison.
- (m) Inform the Chief of Investigations or the authorized designee once survivor notifications have been made so that other Stanislaus County District Attorney's Office members may be apprised that survivor notifications are complete.

#### **832.4.1 OUT-OF-AREA NOTIFICATIONS**

The Chief Investigator should request assistance from law enforcement agencies in appropriate jurisdictions for in-person notification to survivors who are out of the area.

- (a) The Chief Investigator should contact the appropriate jurisdiction using a secure network and provide the assisting agency with the name and telephone number of the bureau liaison member that the survivors can call for more information following the notification by the assisting agency.
- (b) The Bureau Liaison may assist in making transportation arrangements for the member's survivors, but will not obligate the Bureau to pay travel expenses without the authorization of the Chief of Investigations.

#### **832.5 NOTIFYING BUREAU MEMBERS**

Supervisors or members designated by the Chief of Investigations are responsible for notifying bureau members of the line-of-duty death as soon as possible after the survivor notification is made. Notifications and related information should be communicated in person or using secure networks and should not be transmitted over the radio.

Notifications should be made in person and as promptly as possible to all members on-duty at the time of the incident. Members reporting for subsequent shifts within a short amount of time should be notified in person at the beginning of their shifts. Members reporting for duty from their residences should be instructed to contact their supervisors as soon as practicable. Those members who are working later shifts or are on days off should be notified by phone as soon as practicable.

Members having a close bond with the deceased member should be notified of the incident in person. Supervisors should consider assistance (e.g., peer support, modifying work schedules, approving sick leave) for members who are especially affected by the incident.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Line-of-Duty Deaths*

---

Supervisors should direct members not to disclose any information outside the Bureau regarding the deceased member or the incident.

#### **832.6 LIAISONS AND COORDINATORS**

The Chief of Investigations or the authorized designee should select members to serve as liaisons and coordinators to handle responsibilities related to a line-of-duty death, including but not limited to:

- (a) Bureau Liaison.
- (b) Hospital Liaison.
- (c) Survivor Support Liaison.
- (d) Wellness Support Liaison.
- (e) Funeral Liaison.
- (f) Mutual aid coordinator.
- (g) Benefits Liaison.
- (h) Finance coordinator.

Liaisons and coordinators will be directed by the Bureau Liaison and should be given sufficient duty time to complete their assignments.

Members may be assigned responsibilities of more than one liaison or coordinator position depending on available bureau resources. The Bureau Liaison may assign separate liaisons and coordinators to accommodate multiple family units, if needed. The Bureau should consider seeking assistance from surrounding law enforcement agencies to fill liaison and coordinator positions, as appropriate.

##### **832.6.1 BUREAU LIAISON**

The Bureau Liaison should be a Lieutenant or of sufficient rank to effectively coordinate bureau resources, and should serve as a facilitator between the deceased member's survivors and the Bureau. The Bureau Liaison reports directly to the Chief of Investigations. The Bureau Liaison's responsibilities include but are not limited to:

- (a) Directing the other liaisons and coordinators in fulfilling survivors' needs and requests. Consideration should be given to organizing the effort using the National Incident Management System.
- (b) Establishing contact with survivors within 24 hours of the incident and providing them contact information.
- (c) Advising survivors of the other liaison and coordinator positions and their roles and responsibilities.
- (d) Identifying locations that will accommodate a law enforcement funeral and presenting the options to the appropriate survivors, who will select the location.
- (e) Coordinating all official law enforcement notifications and arrangements.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Line-of-Duty Deaths*

---

- (f) Making necessary contacts for authorization to display flags at half-staff.
- (g) Reminding bureau members of appropriate information-sharing restrictions regarding the release of information that could undermine future legal proceedings.
- (h) Coordinating security checks of the member's residence as necessary and reasonable.
- (i) Serving as a liaison with visiting law enforcement agencies during memorial and funeral services.

#### 832.6.2 HOSPITAL LIAISON

The Hospital Liaison should work with hospital personnel to:

- (a) Establish a command post or incident command system, as appropriate, to facilitate management of the situation and its impact on hospital operations (e.g., influx of people, parking).
- (b) Arrange for appropriate and separate waiting areas for:
  - 1. The survivors and others whose presence is requested by the survivors.
  - 2. Bureau members and friends of the deceased member.
  - 3. Media personnel.
- (c) Ensure, as practicable, that any suspects who are in the hospital and their families or friends are not in proximity to the member's survivors or Stanislaus County District Attorney's Office members (except for members who may be guarding a suspect).
- (d) Arrange for survivors to receive timely updates regarding the member before information is released to others.
- (e) Arrange for survivors to have private time with the member, if requested.
  - 1. The Hospital Liaison or hospital personnel may need to explain the condition of the member to the survivors to prepare them accordingly.
  - 2. The Hospital Liaison should accompany the survivors into the room, if requested.
- (f) Stay with survivors and provide them with other assistance as needed at the hospital.
- (g) If applicable, explain to the survivors why an autopsy may be needed.
- (h) Make arrangements for hospital bills to be directed to the Bureau, that the survivors are not asked to sign as guarantor of payment for any hospital treatment, and that the member's residence address, insurance information, and next of kin are not included on hospital paperwork.

Other responsibilities of the Hospital Liaison include but are not limited to:

- Arranging transportation for the survivors back to their residence.
- Working with investigators to gather and preserve the deceased member's equipment and other items that may be of evidentiary value.
- Documenting their actions at the conclusion of duties.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Line-of-Duty Deaths*

---

#### 832.6.3 SURVIVOR SUPPORT LIAISON

The Survivor Support Liaison should work with the Bureau Liaison to fulfill the immediate needs and requests of the survivors of any member who has died in the line of duty, and serve as the long-term bureau contact for survivors.

The Survivor Support Liaison should be selected by the deceased member's Lieutenant. The following should be considered when selecting the Survivor Support Liaison:

- The liaison should be an individual the survivors know and with whom they are comfortable working.
- The selection may be made from names recommended by the deceased member's supervisor and/or coworkers. The deceased member's partner or close friends may not be the best selections for this assignment because the emotional connection to the member or survivors may impair their ability to conduct adequate liaison duties.
- The liaison must be willing to assume the assignment with an understanding of the emotional and time demands involved.

The responsibilities of the Survivor Support Liaison include but are not limited to:

- (a) Arranging for transportation of survivors to hospitals, places of worship, funeral homes, and other locations, as appropriate.
- (b) Communicating with the Bureau Liaison regarding appropriate security measures for the family residence, as needed.
- (c) If requested by the survivors, providing assistance with instituting methods of screening telephone calls made to their residence after the incident.
- (d) Providing assistance with travel and lodging arrangements for out-of-town survivors.
- (e) Returning the deceased member's personal effects from the Bureau and the hospital to the survivors. The following should be considered when returning the personal effects:
  - 1. Items should not be delivered to the survivors until they are ready to receive the items.
  - 2. Items not retained as evidence should be delivered in a clean, unmarked box.
  - 3. All clothing not retained as evidence should be cleaned and made presentable (e.g., items should be free of blood or other signs of the incident).
  - 4. The return of some personal effects may be delayed due to ongoing investigations.
- (f) Assisting with the return of bureau-issued equipment that may be at the deceased member's residence.
  - 1. Unless there are safety concerns, the return of the equipment should take place after the funeral at a time and in a manner considerate of the survivors' wishes.
- (g) Working with the Wellness Support Liaison for survivors to have access to available counseling services.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Line-of-Duty Deaths*

---

- (h) Coordinating with the bureau's Public Information Officer (PIO) to brief the survivors on pending press releases related to the incident and to assist the survivors with media relations in accordance with their wishes (see the Public Information Officer section of this policy).
- (i) Briefing survivors on investigative processes related to the line-of-duty death, such as criminal, internal, and administrative investigations.
- (j) Informing survivors of any related criminal proceedings and accompanying them to such proceedings.
- (k) Introducing survivors to prosecutors, victim's assistance personnel, and other involved personnel as appropriate.
- (l) Maintaining long-term contact with survivors and taking measures to sustain a supportive relationship (e.g., follow-up visits, phone calls, cards on special occasions, special support during holidays).
- (m) Inviting survivors to bureau activities, memorial services (e.g., as applicable, the Annual Candlelight Vigil at the National Law Enforcement Officers Memorial), or other functions as appropriate.

Survivor Support Liaisons providing services after an incident resulting in multiple members being killed should coordinate with and support each other through conference calls or meetings as necessary.

The Bureau recognizes that the duties of a Survivor Support Liaison will often affect regular assignments over many years, and is committed to supporting members in the assignment.

If needed, the Survivor Support Liaison should be issued a personal communication device (PCD) owned by the Bureau to facilitate communications necessary to the assignment. The bureau-issued PCD shall be used in accordance with the Personal Communication Devices Policy.

#### 832.6.4 WELLNESS SUPPORT LIAISON

The Wellness Support Liaison should work with the bureau wellness coordinator or the authorized designee and other liaisons and coordinators to make wellness support and counseling services available to members and survivors who are impacted by a line-of-duty death. The responsibilities of the Wellness Support Liaison include but are not limited to:

- (a) Identifying members who are likely to be significantly affected by the incident and may have an increased need for wellness support and counseling services, including:
  - 1. Members involved in the incident.
  - 2. Members who witnessed the incident.
  - 3. Members who worked closely with the deceased member but were not involved in the incident.
- (b) Making arrangements for members who were involved in or witnessed the incident to be relieved of bureau responsibilities until they can receive wellness support.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Line-of-Duty Deaths*

---

- (c) Making wellness support and counseling resources (e.g., peer support, Critical Incident Stress Debriefing) available to members as soon as reasonably practicable following the line-of-duty death.
- (d) Coordinating with the Survivor Support Liaison to inform survivors of available wellness support and counseling services and assisting with arrangements as needed.
- (e) Following up with members and the Survivor Support Liaison in the months following the incident to determine if additional wellness support or counseling services are needed.

#### 832.6.5 FUNERAL LIAISON

The Funeral Liaison should work with the Bureau Liaison, Survivor Support Liaison, and survivors to coordinate funeral arrangements to the extent the survivors wish. The Funeral Liaison's responsibilities include but are not limited to:

- (a) Assisting survivors in working with the funeral director regarding funeral arrangements and briefing them on law enforcement funeral procedures.
- (b) Completing funeral notification to other law enforcement agencies.
- (c) Coordinating the funeral activities of the Bureau, including but not limited to the following:
  - 1. Honor Guard
    - (a) Casket watch
    - (b) Color guard
    - (c) Pallbearers
    - (d) Bell/rifle salute
  - 2. Bagpipers/bugler
  - 3. Uniform for burial
  - 4. Flag presentation
  - 5. Last radio call
- (d) Briefing the Chief of Investigations and command staff concerning funeral arrangements.
- (e) Assigning an investigator to remain at the family home during the viewing and funeral.
- (f) Arranging for transportation of the survivors to and from the funeral home and interment site using bureau vehicles and drivers.
- (g) Addressing event-related logistical matters (e.g., parking, visitor overflow, public assembly areas).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Line-of-Duty Deaths*

---

#### 832.6.6 MUTUAL AID COORDINATOR

The mutual aid coordinator should work with the Bureau Liaison and the Funeral Liaison to request and coordinate any assistance from outside law enforcement agencies needed for, but not limited to:

- (a) Traffic control during the deceased member's funeral.
- (b) Area coverage so that as many Stanislaus County District Attorney's Office members can attend funeral services as possible.

The mutual aid coordinator should perform duties in accordance with the Outside Agency Assistance Policy.

Where practicable, the Chief of Investigations should appoint a mutual aid coordinator to identify external resources in advance of any need (e.g., regional honor guard teams, county- or state-wide resources).

#### 832.6.7 BENEFITS LIAISON

The Benefits Liaison should provide survivors with information concerning available benefits and will assist them in applying for benefits. Responsibilities of the Benefits Liaison include but are not limited to:

- (a) Confirming the filing of workers' compensation claims and related paperwork (see the Occupational Disease and Work-Related Injury Reporting Policy).
- (b) Researching and assisting survivors with application for federal government survivor benefits, such as those offered through the following:
  - 1. Public Safety Officers' Benefits Program, including financial assistance available through the Public Safety Officers' Educational Assistance (PSOEA) Program, as applicable (34 USC § 10281 et seq.).
  - 2. Social Security Administration.
  - 3. Department of Veterans Affairs.
- (c) Researching and assisting survivors with application for state and local government survivor benefits, such as:
  - 1. Education benefits (Education Code § 68120).
  - 2. Health benefits (Labor Code § 4856).
  - 3. Workers' compensation death benefit (Labor Code § 4702).
- (d) Researching and assisting survivors with application for other survivor benefits such as:
  - 1. Private foundation survivor benefits programs.
  - 2. Survivor scholarship programs.
- (e) Researching and informing survivors of support programs sponsored by investigator associations and other organizations.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Line-of-Duty Deaths*

---

- (f) Documenting and informing survivors of inquiries and interest regarding public donations to the survivors.
  - 1. If requested, working with the finance coordinator to assist survivors with establishing a process for the receipt of public donations.
- (g) Providing survivors with a summary of the nature and amount of benefits applied for, including the name of a contact person at each benefit office. Printed copies of the summary and benefit application documentation should be provided to affected survivors.
- (h) Maintaining contact with the survivors and assisting with subsequent benefit questions and processes as needed.

#### **832.6.8 FINANCE COORDINATOR**

The finance coordinator should work with the Chief of Investigations and the Bureau Liaison to manage financial matters related to the line-of-duty death. The finance coordinator's responsibilities include, but are not limited to:

- (a) Establishing methods for purchasing and monitoring costs related to the incident.
- (b) Providing information on finance-related issues, such as:
  - 1. Paying survivors' travel costs if authorized.
  - 2. Transportation costs for the deceased.
  - 3. Funeral and memorial costs.
  - 4. Related funding or accounting questions and issues.
- (c) Working with the Benefits Liaison to establish a process for the receipt of public donations to the deceased member's survivors.
- (d) Providing accounting and cost information as needed.

#### **832.7 PUBLIC INFORMATION OFFICER**

In the event of a line-of-duty death, the bureau's PIO should be the bureau's contact point for the media. As such, the PIO should coordinate with the Bureau Liaison to:

- (a) Collect and maintain the most current incident information and determine what information should be released.
- (b) Instruct bureau members to direct any media inquiries to the PIO.
- (c) Prepare necessary press releases.
  - 1. Coordinate with other entities having media roles (e.g., outside agencies involved in the investigation or incident).
  - 2. Disseminate important public information, such as information on how the public can show support for the bureau and deceased member's survivors.
- (d) Arrange for community and media briefings by the Chief of Investigations or the authorized designee as appropriate.
- (e) Respond, or coordinate the response, to media inquiries.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Line-of-Duty Deaths*

---

- (f) If requested, assist the member's survivors with media inquiries.
  - 1. Brief the survivors on handling sensitive issues such as the types of questions that reasonably could jeopardize future legal proceedings.
- (g) Release information regarding memorial services and funeral arrangements to bureau members, other agencies, and the media as appropriate.
- (h) If desired by the survivors, arrange for the recording of memorial and funeral services via photos and/or video.

The identity of deceased members should be withheld until the member's survivors have been notified. If the media have obtained identifying information for the deceased member prior to survivor notification, the PIO should request that the media withhold the information from release until proper notification can be made to survivors. The PIO should notify media when survivor notifications have been made.

#### **832.8 INVESTIGATION OF THE INCIDENT**

The Chief of Investigations should make necessary assignments to conduct thorough investigations of any line-of-duty death and may choose to use the investigation process outlined in the Officer-Involved Shootings and Deaths Policy.

Investigators from other agencies may be assigned to work on any criminal investigation related to line-of-duty deaths. Partners, close friends, or personnel who worked closely with the deceased member should not have any investigative responsibilities because such relationships may impair the objectivity required for an impartial investigation of the incident.

Involved bureau members should be kept informed of the progress of the investigations and provide investigators with any information that may be pertinent to the investigations.

#### **832.9 NON-LINE-OF-DUTY DEATH**

The Chief of Investigations may authorize certain support services for the death of a member not occurring in the line of duty.

## Wellness Program

### 833.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance on establishing and maintaining a proactive wellness program for Stanislaus County District Attorney (SCDA) members.

The wellness program is intended to be a holistic approach to a member's well-being and encompasses aspects such as mental health and overall wellness.

Additional information on member wellness is provided in the:

- Line-of-Duty Deaths Policy.
- Drug- and Alcohol-Free Workplace Policy.

#### 833.1.1 DEFINITIONS

Definitions related to this policy include:

**Critical incident** – An event or situation that may cause a strong emotional, cognitive, or physical reaction that has the potential to interfere with daily life.

**Critical Incident Stress Debriefing (CISD)** – A standardized approach using a discussion format to provide education, support, and emotional release opportunities for members involved in work-related critical incidents.

**Peer support** – Mental and emotional wellness support provided by peers trained to help members cope with critical incidents and certain personal or professional problems.

### 833.2 POLICY

It is the policy of the SCDA to prioritize member wellness to foster fitness for duty and support a healthy quality of life for our members. The SCDA will maintain a wellness program that supports its full-time members with proactive wellness resources, critical incident response, and follow-up support.

### 833.3 WELLNESS COORDINATOR

The Chief of Investigations should appoint a trained wellness coordinator. The coordinator should report directly to the Chief of Investigations or the authorized designee and should collaborate with advisers (e.g., Human Resources, legal counsel, licensed psychotherapist, qualified health professionals), as appropriate, to fulfill the responsibilities of the position, including but not limited to:

- (a) Identifying wellness support providers (e.g., licensed psychotherapists, external peer support providers, physical therapists, dietitians, physical fitness trainers holding accredited certifications).
  1. As appropriate, selected providers should be trained and experienced in providing mental wellness support and counseling to public safety personnel.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Wellness Program*

---

2. When practicable, the Bureau should not use the same licensed psychotherapist for both member wellness support and fitness for duty evaluations.
- (b) Developing management and operational procedures for bureau peer support members, such as:
  1. Peer support member selection and retention.
  2. Training and applicable certification requirements.
  3. Deployment.
  4. Managing potential conflicts between peer support members and those seeking service.
  5. Monitoring and mitigating peer support member emotional fatigue (i.e., compassion fatigue) associated with providing peer support.
  6. Using qualified peer support personnel from other public safety agencies or outside organizations for bureau peer support, as appropriate.
- (c) Verifying members have reasonable access to peer support or licensed psychotherapist support.
- (d) Establishing procedures for CISDs, including:
  1. Defining the types of incidents that may initiate debriefings.
  2. Steps for organizing debriefings.
- (e) Facilitating the delivery of wellness information, training, and support through various methods appropriate for the situation (e.g., phone hotlines, electronic applications).
- (f) Verifying a confidential, appropriate, and timely Employee Assistance Program (EAP) is available for members. This also includes:
  1. Obtaining a written description of the program services.
  2. Providing for the methods to obtain program services.
  3. Providing referrals to the EAP for appropriate diagnosis, treatment, and follow-up resources.
  4. Obtaining written procedures and guidelines for referrals to, or mandatory participation in, the program.
  5. Obtaining training for supervisors in their role and responsibilities, and identification of member behaviors that would indicate the existence of member concerns, problems, or issues that could impact member job performance.
- (g) Assisting members who have become disabled with application for federal government benefits such as those offered through the Public Safety Officers' Benefits Program (34 USC § 10281 et seq.).
  1. The coordinator should work with appropriate bureau liaisons to assist qualified members and survivors with benefits, wellness support, and counseling services, as applicable, when there has been a member death (see the Line-of-Duty Deaths Policy for additional guidance).

### *Wellness Program*

---

#### **833.4 SCDA PEER SUPPORT**

##### **833.4.1 PEER SUPPORT MEMBER SELECTION CRITERIA**

The selection of a SCDA peer support member will be at the discretion of the coordinator. Selection should be based on the member's:

- Desire to be a peer support member.
- Experience or tenure.
- Demonstrated ability as a positive role model.
- Ability to communicate and interact effectively.
- Evaluation by supervisors and any current peer support members.

##### **833.4.2 PEER SUPPORT MEMBER RESPONSIBILITIES**

The responsibilities of SCDA peer support members include:

- (a) Providing pre- and post-critical incident support.
- (b) Presenting SCDA members with periodic training on wellness topics, including but not limited to:
  - 1. Stress management.
  - 2. Suicide prevention.
  - 3. How to access support resources.
- (c) Providing referrals to licensed psychotherapists and other resources, where appropriate.
  - 1. Referrals should be made to SCDA-designated resources in situations that are beyond the scope of the peer support member's training.

##### **833.4.3 PEER SUPPORT MEMBER TRAINING**

A SCDA peer support member should complete authorized and approved training prior to being assigned to peer support responsibilities.

#### **833.5 CRITICAL INCIDENT STRESS DEBRIEFINGS**

A Critical Incident Stress Debriefing should occur as soon as practicable following a critical incident. The coordinator is responsible for organizing the debriefing. Notes and recorded statements shall not be taken because the sole purpose of the debriefing is to help mitigate the stress-related effects of a critical incident.

The debriefing is not part of any investigative process. Care should be taken not to release or repeat any communication made during a debriefing unless otherwise authorized by policy, law, or a valid court order.

Attendance at the debriefing should only include peer support members and those directly involved in the incident.

### *Wellness Program*

---

#### **833.6 PEER SUPPORT COMMUNICATIONS**

Although the SCDA will honor the sensitivity of communications with peer support members, there is no legal privilege to such communications, unless authorized by law (e.g., peer support communications pursuant to a Law Enforcement Peer Support and Crisis Referral Service Program).

#### **833.7 TRAINING**

The Wellness Coordinator or authorized designee should collaborate with HR manager, Training managers for both the Office and the Bureau of Investigation (BI) to provide all members with regular training on topics related to member wellness, including but not limited to:

- The availability and range of wellness support systems.
- Suicide prevention.
- Recognizing and managing mental distress, emotional fatigue, post-traumatic stress, and other possible reactions to trauma.
- Alcohol and substance disorder awareness.
- Countering sleep deprivation and physical fatigue.
- Anger management.
- Marriage and family wellness.
- Benefits of exercise and proper nutrition.
- Effective time and personal financial management skills.

For non-sworn personnel, training materials, curriculum, and attendance records should be forwarded to the HR manager. All training materials for sworn members should be forwarded to the Training Lieutenant in the BI so documentation can be provided to the Peace Officer Standards and Training (POST) records management system.

## **Chapter 9 - Traffic Operations**

## Impaired Driving

### 900.1 PURPOSE AND SCOPE

This policy provides guidance to those bureau members who play a role in the detection and investigation of driving under the influence (DUI).

### 900.2 POLICY

The Stanislaus County District Attorney's Office is committed to the safety of the roadways and the community and will pursue fair but aggressive enforcement of California's impaired driving laws.

### 900.3 INVESTIGATIONS

Investigators should not enforce DUI laws to the exclusion of their other duties unless specifically assigned to DUI enforcement. All investigators are expected to enforce these laws with due diligence.

The XXX will develop and maintain, in consultation with the prosecuting attorney, report forms with appropriate checklists to assist investigating investigators in documenting relevant information and maximizing efficiency. Any DUI investigation will be documented using these forms. Information documented elsewhere on the form does not need to be duplicated in the report narrative. Information that should be documented includes, at a minimum:

- (a) The field sobriety tests (FSTs) administered and the results.
- (b) The investigator's observations that indicate impairment on the part of the individual, and the investigator's health-related inquiries that may help to identify any serious health concerns (e.g., diabetic shock).
- (c) Sources of additional information (e.g., reporting party, witnesses) and their observations.
- (d) Information about any audio and/or video recording of the individual's driving or subsequent actions.
- (e) The location and time frame of the individual's vehicle operation and how this was determined.
- (f) Any prior related convictions in California or another jurisdiction.

### 900.4 FIELD TESTS

The XXX should identify standardized FSTs and any approved alternate tests for investigators to use when investigating violations of DUI laws.

### 900.5 CHEMICAL TESTS

A person implies consent to a chemical test or tests, and to providing the associated chemical sample, under any of the following (Vehicle Code § 23612):

- (a) The person is arrested for driving a vehicle while under the influence, pursuant to Vehicle Code § 23152.



# Stanislaus County District Attorney's Office

## Policy Manual

### *Impaired Driving*

---

- (b) The person is under 21 years of age and is arrested by an investigator having reasonable cause to believe that the person's blood alcohol content is 0.05 or more (Vehicle Code § 23140).
- (c) The person is under 21 years of age and detained by an investigator having reasonable cause to believe that the person was driving a vehicle while having a blood alcohol content of 0.01 or more (Vehicle Code § 23136).
- (d) The person was operating a vehicle while under the influence and proximately caused bodily injury to another person (Vehicle Code § 23153).

If a person withdraws this implied consent, or is unable to withdraw consent (e.g., the person is unconscious), the investigator should consider implied consent revoked and proceed as though the person has refused to provide a chemical sample.

#### 900.5.1 STATUTORY NOTIFICATIONS

Investigators requesting that a person submit to chemical testing shall provide the person with the mandatory warning pursuant to Vehicle Code § 23612(a)(1)(D) and Vehicle Code § 23612(a)(4).

#### 900.5.2 PRELIMINARY ALCOHOL SCREENING

Investigators may use a preliminary alcohol screening (PAS) test to assist in establishing reasonable cause to believe a person is DUI. The investigator shall advise the person that the PAS test is being requested to assist in determining whether the person is under the influence of alcohol or drugs, or a combination of the two. Unless the person is under the age of 21, the person shall be advised that the PAS test is voluntary. The investigator shall also advise the person that submitting to a PAS test does not satisfy the person's obligation to submit to a chemical test as otherwise required by law (Vehicle Code § 23612).

#### 900.5.3 PRELIMINARY ALCOHOL SCREENING FOR A PERSON UNDER AGE 21

If an investigator lawfully detains a person under 21 years of age who is driving a motor vehicle and the investigator has reasonable cause to believe that the person has a blood alcohol content of 0.01 or more, the investigator shall request that the person take a PAS test to determine the presence of alcohol in the person, if a PAS test device is immediately available. If a PAS test device is not immediately available, the investigator may request the person to submit to chemical testing of the person's blood, breath, or urine, conducted pursuant to Vehicle Code § 23612 (Vehicle Code § 13388).

If the person refuses to take or fails to complete the PAS test or other chemical test, or if the result of either test reveals a blood alcohol content of 0.01 or more, the investigator shall proceed to serve the person with a notice of order of suspension pursuant to this policy (Vehicle Code § 13388).

#### 900.5.4 CHOICE OF TESTS

Investigators shall respect a viable choice of chemical test made by an arrestee, as provided for by law (e.g., breath will not be acceptable for suspected narcotics influence).

# Stanislaus County District Attorney's Office

## Policy Manual

### *Impaired Driving*

---

A person arrested for DUI has the choice of whether the test is of the person's blood or breath, and the investigator shall advise the person that the person has that choice. If the person arrested either is incapable, or states that the person is incapable, of completing the chosen test, the person shall submit to the remaining test.

If the person chooses to submit to a breath test and there is reasonable cause to believe that the person is under the influence of a drug or the combined influence of alcohol and any drug, the investigator may also request that the person submit to a blood test. If the person is incapable of completing a blood test, the person shall submit to and complete a urine test (Vehicle Code § 23612(a)(2)(C)).

#### 900.5.5 BREATH SAMPLES

The XXX should ensure that all devices used for the collection and analysis of breath samples are properly serviced and tested, and that a record of such service and testing is properly maintained.

Investigators obtaining a breath sample should monitor the device for any sign of malfunction. Any anomalies or equipment failures should be noted in the appropriate report and promptly reported to the XXX.

When the arrested person chooses a breath test, the handling investigator shall advise the person that the breath-testing equipment does not retain a sample, and the person may, if desired, provide a blood or urine specimen, which will be retained to facilitate subsequent verification testing (Vehicle Code § 23614).

The investigator should also require the person to submit to a blood test if the investigator has a clear indication that a blood test will reveal evidence of any drug or the combined influence of an alcoholic beverage and any drug. Evidence of the investigator's belief shall be included in the investigator's report (Vehicle Code § 23612(a)(2)(C)).

#### 900.5.6 BLOOD SAMPLES

Only persons authorized by law to draw blood shall collect blood samples (Vehicle Code § 23158). The blood draw should be witnessed by the assigned investigator. No investigator, even if properly certified, should perform this task.

Investigators should inform an arrestee that if the arrestee chooses to provide a blood sample, a separate sample can be collected for alternate testing. Unless medical personnel object, two samples should be collected and retained as evidence, so long as only one puncture is required.

The blood sample shall be packaged, marked, handled, stored, and transported as required by the testing facility.

If an arrestee cannot submit to a blood draw because the arrestee has a bleeding disorder or has taken medication that inhibits coagulation, the arrestee shall not be required to take a blood test. Such inability to take a blood test should not be considered a refusal. However, that arrestee may be required to complete another available and viable test.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Impaired Driving*

---

#### 900.5.7 URINE SAMPLES

If a urine test will be performed, the arrestee should be promptly transported to the appropriate testing site. The investigator shall follow any directions accompanying the urine evidence collection kit.

Urine samples shall be collected and witnessed by an investigator or jail staff member of the same sex as the individual giving the sample. The arrestee should be allowed sufficient privacy to maintain the arrestee's dignity, to the extent possible, while still ensuring the accuracy of the sample (Vehicle Code § 23158(i)).

The sample shall be packaged, marked, handled, stored, and transported as required by the testing facility.

#### 900.6 REFUSALS

When an arrestee refuses to provide a viable chemical sample, investigators should:

- (a) Advise the arrestee of the requirement to provide a sample (Vehicle Code § 23612).
- (b) Audio- and/or video-record the admonishment when it is practicable.
- (c) Document the refusal in the appropriate report.

#### 900.6.1 STATUTORY NOTIFICATIONS UPON REFUSAL

Upon refusal to submit to a chemical test as required by law, investigators shall personally serve the notice of order of suspension upon the arrestee and take possession of any state-issued license to operate a motor vehicle that is held by that individual (Vehicle Code § 23612(e); Vehicle Code § 23612(f)).

#### 900.6.2 BLOOD SAMPLE WITHOUT CONSENT

A blood sample may be obtained from a person who refuses a chemical test when any of the following conditions exist:

- (a) A search warrant has been obtained (Penal Code § 1524).
- (b) The investigator can articulate that exigent circumstances exist. Exigency does not exist solely because of the short time period associated with the natural dissipation of alcohol or controlled or prohibited substances in the person's bloodstream. Exigency can be established by the existence of special facts such as a lengthy time delay in obtaining a blood sample due to an accident investigation or medical treatment of the person.

#### 900.6.3 FORCED BLOOD SAMPLE

If an arrestee indicates by word or action that the person will physically resist a blood draw, the investigator should request a supervisor to respond.

The responding supervisor should:

- (a) Evaluate whether using force to obtain a blood sample is appropriate under the circumstances.

# Stanislaus County District Attorney's Office

## Policy Manual

### *Impaired Driving*

---

- (b) Ensure that all attempts to obtain a blood sample through force cease if the person agrees to, and completes a viable form of testing in a timely manner.
- (c) Advise the person of the person's duty to provide a sample (even if this advisement was previously done by another investigator) and attempt to persuade the individual to submit to such a sample without physical resistance.
  - 1. This dialogue should be recorded on audio and/or video if practicable.
- (d) Ensure that the blood sample is taken in a medically approved manner.
- (e) Ensure the forced blood draw is recorded on audio and/or video when practicable.
- (f) Monitor and ensure that the type and level of force applied appears reasonable under the circumstances:
  - 1. Unless otherwise provided in a warrant, force should generally be limited to handcuffing or similar restraint methods.
  - 2. In misdemeanor cases, if the arrestee becomes violent or more resistant, no additional force will be used and a refusal should be noted in the report.
  - 3. In felony cases, force which reasonably appears necessary to overcome the resistance to the blood draw may be permitted.
- (g) Ensure the use of force and methods used to accomplish the collection of the blood sample are documented in the related report.

If a supervisor is unavailable, investigators are expected to use sound judgment and perform as a responding supervisor, as set forth above.

### **900.7 ARREST AND INVESTIGATION**

#### **900.7.1 WARRANTLESS ARREST**

In addition to the arrest authority granted to investigators pursuant to Penal Code § 836, an investigator may make a warrantless arrest of a person that the investigator has reasonable cause to believe has been driving under the influence of an alcoholic beverage or any drug, or under the combined influence of the same when (Vehicle Code § 40300.5):

- (a) The person is involved in a traffic crash.
- (b) The person is observed in or about a vehicle that is obstructing the roadway.
- (c) The person will not be apprehended unless immediately arrested.
- (d) The person may cause injury to themselves or damage property unless immediately arrested.
- (e) The person may destroy or conceal evidence of a crime unless immediately arrested.

#### **900.7.2 INVESTIGATOR RESPONSIBILITIES**

The investigator serving the arrested person with a notice of an order of suspension shall immediately (Vehicle Code § 23612):

### *Impaired Driving*

---

- (a) Forward a copy of the completed notice of suspension or revocation form and any confiscated driver's license to the Department of Motor Vehicles (DMV).
- (b) Forward a sworn report to DMV that contains the required information in Vehicle Code § 13380.
- (c) Forward the results to the appropriate forensic laboratory if the person submitted to a blood or urine test.

#### **900.8 ADMINISTRATIVE HEARINGS**

The Records Manager will ensure that all appropriate reports and documents related to administrative license suspensions are reviewed and forwarded to DMV.

Any investigator who receives notice of required attendance to an administrative license suspension hearing should promptly notify the prosecuting attorney.

An investigator called to testify at an administrative hearing should document the hearing date and DMV file number in a supplemental report. Specific details of the hearing generally should not be included in the report unless errors, additional evidence or witnesses are identified.

#### **900.8 RECORDS BUREAU RESPONSIBILITIES**

The Records Manager will ensure that all case-related records are transmitted according to current records procedures and as required by the prosecuting attorney's office.

#### **900.9 TRAINING**

The Lieutenant should ensure that investigators participating in the enforcement of DUI laws receive regular training. Training should include, at minimum, current laws on impaired driving, investigative techniques and rules of evidence pertaining to DUI investigations. The Lieutenant should confer with the prosecuting attorney's office and update training topics as needed.

Stanislaus County District  
Attorney's Office Policy Manual  
Policy Manual

## **Attachments**

## **Statutes and Legal Requirements.pdf**

---

## Statutes and Legal Requirements

Items listed in this section include sections from the California Penal Code (CPC), Welfare and Institutions Code (WI) and Government Code (GC).

### *Definitions*

CPC 422.55 - Provides general definition of hate crimes in California.

CPC 422.56- Provides definitions of terms included in hate crimes statutes.

GC 12926- Disability-related definitions applicable to some hate crime statutes.

## Felonies

### *Hate Crimes*

CPC 422.7 - Commission of a crime for the purpose of interfering with another's exercise of civil rights.

### *Related Crimes*

CPC 190.2(a)(16) - Homicide penalties related to certain hate crime related acts.

CPC 190.03(a) - Homicide penalties related to certain hate crime related acts.

CPC 288(b)(2) - Sexual assault of dependent person by caretaker

CPC 368(b) - Dependent adult abuse generally - may apply as disability-related hate crime.

CPC 594.3 - Vandalism of places of worship.

CPC 11412 - Causing or attempting to cause other to refrain from exercising religion by threat.

CPC 11413 - Arson or destructive device at place of worship.

## Misdemeanors

### *Hate Crimes*

CPC 422.6 - Use of force, threats, or destruction of property to interfere with another's exercise of civil rights.

CPC 422.77 - Violation of civil order (Bane Act) protecting the exercise of civil rights

### *Related Crimes*

CPC 302 - Disorderly conduct during an assemblage of people gathered for religious worship at a tax-exempt place of worship.

CPC 538(c) - Unauthorized insertion of advertisements in newspapers and redistribution to the public.

CPC 640.2 - Placing handbill, notice of advertisement on a consumer product or product packaged without authorization.

CPC 11411 - Terrorism of owner or occupant of real property. Placement or display of sign, symbol, or other physical impression without authorization, engagement in pattern of conduct, or burning or desecration of religious symbols.



---

## Enhancements

**CPC 190.2(a)(16)** - Special circumstances imposing the Death Penalty or Life Without Possibility of Parole, if the victim was intentionally killed because of sexual orientation, gender, or disability.

**CPC 190.3** - Special circumstances imposing LWOP if the victim was intentionally killed because of sexual orientation, gender, or disability.

**CPC 422.75** - Penalty for felony committed because of victim's race, color, religion, nationality, country or origin, ancestry, disability, or sexual orientation shall be enhanced one, two, or three years in prison, if the person acts alone; and two, three, or four years if the person commits the act with another.

**CPC 1170.8** - Enhancement for robbery or assault at a place of worship.

**CPC 1170.85(b)** - Felony assault or battery enhancement due to age or disability.

## Reporting

**CPC 13023**- Requirement for law enforcement agencies to report hate crime data to DOJ.

**WI 15630** – Elder and Dependent Adult Abuse Mandated Reporting (may apply in disability-related hate crimes).

## Training and Policy Requirements

**CPC 422.87** - Hate crimes policy adoption and update requirements (AB 1985, Effective January 1, 2019).

**CPC 13519.6** - Defines hate crime training requirements for peace officers.

**CPC 13519.41** - Training requirements on sexual orientation and gender identity-related hate crimes for peace officers and dispatchers (AB 2504, Effective January 1, 2019).

## Miscellaneous Provisions

**CPC 422.78** - Responsibility for prosecution of stay away order violations.

**CPC 422.86** - Public policy regarding hate crimes.

**CPC 422.89** - Legislative intent regarding violations of civil rights and hate crimes

**CPC 422.92** - Hate crimes victims brochure requirement for law enforcement agencies.

**CPC 422.93** - Protection of victims and witnesses from being reported to immigration authorities.

**GC 6254** - Victim confidentiality.

**epo001.pdf**

**EMERGENCY PROTECTIVE ORDER** (See reverse for important notices.)**1. PROTECTED PERSONS** (insert names of all persons protected by this Order):  
\_\_\_\_\_

**2. RESTRAINED PERSON (name):** \_\_\_\_\_ Gender: ☐ M ☐ F ☐ X  
 Ht.: \_\_\_\_\_ Wt.: \_\_\_\_\_ Hair color: \_\_\_\_\_ Eye color: \_\_\_\_\_ Race: \_\_\_\_\_ Age: \_\_\_\_\_ Date of birth: \_\_\_\_\_

**3. TO THE RESTRAINED PERSON:**

- a. ☐ **YOU MUST NOT** harass, attack, strike, threaten, assault (sexually or otherwise), hit, follow, stalk, molest, destroy personal property of, keep under surveillance, impersonate, block movements of, annoy by phone or other electronic means (including repeatedly contact), or disturb the peace of (including coercive control), any person named in item 1.
- b. ☐ **YOU MUST NOT** contact, either directly or indirectly, by any means, including but not limited to by telephone, mail, e-mail or other electronic means, any person named in item 1.
- c. ☐ **YOU MUST** ☐ stay away at least: \_\_\_\_\_ yards from each person named in item 1.  
☐ stay away at least: \_\_\_\_\_ yards from ☐ move out immediately from:  
 (address): \_\_\_\_\_
- d. **YOU MUST NOT** take any action, directly or through others, to obtain the addresses or locations of any person named in item 1.
- e. **YOU MUST NOT** own, possess, purchase, receive, or attempt to purchase or receive any firearm (gun), firearm parts (receiver, frame, or unfinished receiver or frame (Penal Code section 16531)), or ammunition. You must immediately surrender these items if asked by law enforcement. If not asked by law enforcement to surrender immediately, you must turn them in to a law enforcement agency or sell them to, or store them with, a licensed gun dealer within 24 hours of receiving this order.
4. ☐ (Name): \_\_\_\_\_ is given temporary care and control of the following  
 minor children of the parties (names and ages): \_\_\_\_\_

5. Order Expires on (date): \_\_\_\_\_ at (time): \_\_\_\_\_ EXPIRES ON THE 5TH COURT DAY OR 7TH CALENDAR DAY, WHICHEVER IS EARLIER. DO NOT COUNT THE DAY THE ORDER IS GRANTED.

6. To Person in 1: To ask for a longer restraining order, ask for help at your local court. If there is an open juvenile case, file in that case. (Name and address of court): \_\_\_\_\_

7. Reasonable grounds for the issuance of this Order exist, and an emergency protective order is necessary to prevent the occurrence or recurrence of domestic violence, child abuse, child abduction, elder or dependent adult abuse, or stalking.

8. Judicial officer (name): \_\_\_\_\_ granted this Order on (date): \_\_\_\_\_ at (time): \_\_\_\_\_

**APPLICATION**

9. The events that caused the protected person to fear immediate and present danger of domestic violence, child abuse, child abduction, elder or dependent adult abuse (except solely financial abuse), or stalking are (give facts and dates; specify weapons):  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_
10. ☐ Firearms or ammunition were (check all that apply): ☐ observed ☐ reported ☐ physically searched for ☐ seized
11. ☐ The persons in 1 and 2 live together. The person in 1 asks that the person in 2 immediately move out from the address in item 3c.
12. ☐ The person in 1 has minor children in common with the person in 2, and a temporary custody order is requested because of the facts alleged in item 9. A custody order ☐ does exist. ☐ does not exist.

By: \_\_\_\_\_ (PRINT NAME OF LAW ENFORCEMENT OFFICER)  (SIGNATURE OF LAW ENFORCEMENT OFFICER)

Agency: \_\_\_\_\_ Telephone No.: \_\_\_\_\_ Badge No.: \_\_\_\_\_

**PROOF OF SERVICE**

13. I personally delivered (served) copies of this Order to the person named in 2 on: (date): \_\_\_\_\_ at (time): \_\_\_\_\_  
 Address where person in 2 was served: \_\_\_\_\_
14. At the time of service, I was at least 18 years of age and not a party to this cause. ☐ I am a California law enforcement officer.
15. My name, address, and telephone number are (this does not have to be server's home telephone number or address):  
 \_\_\_\_\_

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Date: \_\_\_\_\_

\_\_\_\_\_  
 (TYPE OR PRINT NAME OF SERVER)

 \_\_\_\_\_  
 (SIGNATURE OF SERVER)

# EMERGENCY PROTECTIVE ORDER WARNINGS AND INFORMATION

EPO-001

**TO THE RESTRAINED PERSON:** VIOLATION OF THIS ORDER IS A MISDEMEANOR PUNISHABLE BY A \$1,000 FINE, ONE YEAR IN JAIL, OR BOTH, OR IT MAY BE PUNISHABLE AS A FELONY. THIS PROTECTIVE ORDER MUST BE ENFORCED BY ALL LAW ENFORCEMENT OFFICERS IN THE STATE OF CALIFORNIA WHO ARE AWARE OF OR SHOWN A COPY OF THE ORDER. THE TERMS AND CONDITIONS OF THIS ORDER REMAIN ENFORCEABLE REGARDLESS OF THE ACTS OF THE PARTIES; IT MAY BE CHANGED ONLY BY ORDER OF THE COURT (PENAL CODE SECTION 13710(b)).

**YOU ARE PROHIBITED FROM OWNING, POSSESSING, PURCHASING, RECEIVING, OR ATTEMPTING TO PURCHASE OR RECEIVE ANY ITEM LISTED IN 3e. (PENAL CODE SECTIONS 29825(a), 30305(a).) A VIOLATION IS SUBJECT TO A \$1,000 FINE AND IMPRISONMENT OR BOTH. YOU MUST IMMEDIATELY SURRENDER THE ITEMS IN 3e IF ASKED BY LAW ENFORCEMENT. IF NOT ASKED BY LAW ENFORCEMENT TO SURRENDER, YOU MUST TURN IN THE ITEMS IN 3e TO LAW ENFORCEMENT, OR SELL THEM TO, OR STORE THEM WITH, A LICENSED GUN DEALER WITHIN 24 HOURS OF RECEIVING THIS ORDER. PROOF OF SURRENDER, SALE, OR STORAGE MUST BE FILED WITH THE COURT WITHIN 48 HOURS OF RECEIPT OF THIS ORDER.**

**To the restrained person:** This order will last until the date and time in item 5 on the reverse. The protected person may, however, obtain a more permanent restraining order from the court. You may seek the advice of an attorney on any matter connected with this order. The attorney should be consulted promptly so that the attorney may assist you in responding to the order.

**A la persona bajo restricción judicial:** Esta orden durará hasta la fecha y hora indicada en el punto 5 al dorso. La persona protegida puede, sin embargo, obtener una orden de entredicho (restricción judicial) más permanente de la corte. Usted puede consultar a un abogado en conexión con cualquier asunto relacionado con esta orden. Debe consultar al abogado inmediatamente para que él o ella le pueda ayudar a responder a la orden.

**To the protected person:** This order will last only until the date and time noted in item 5 on the reverse. If you wish to seek continuing protection, you will have to apply for an order from the court at the address in item 6. You may apply for a protective order free of charge. In the case of an endangered child, you may also apply for a more permanent order at the address in item 6, or if there is a juvenile dependency action pending, you may apply for a more permanent order under section 213.5 of the Welfare and Institutions Code. In the case of a child being abducted, you may apply for a *Child Custody and Visitation Order* from the court. You may seek the advice of an attorney on any matter connected with your application for any future court orders. The attorney should be consulted promptly so that the attorney may assist you in making your application. You do not have to have an attorney to get the protective order.

**A la persona protegida:** Esta orden durará sólo hasta la fecha y hora indicada en el punto 5 al dorso. Si usted desea que la protección continúe, tendrá que solicitar una orden de la corte en la dirección indicada en el punto 6. La solicitud de la orden de protección es gratis. En el caso de que un niño o una niña se encuentre en peligro, puede solicitar una orden más permanente en la dirección indicada en el punto 6, o si hay una acción legal pendiente de tutela juvenil, puede solicitar una orden más permanente conforme a la sección 213.5 del código titulado en inglés **Welfare and Institutions Code**. En el caso del secuestro de un niño o una niña, usted puede solicitar de la corte una orden para la guarda del niño o de la niña (*Child Custody and Visitation Order*). Puede consultar a un abogado en conexión con cualquier asunto relacionado con las solicitudes de órdenes de la corte que usted presente en el futuro. Debe consultar un abogado inmediatamente para que él o ella le pueda ayudar a presentar su solicitud. Para obtener la orden de protección no es necesario que un abogado le represente.

**If a child is in danger of being abducted:** This order will last only until the date and time noted in item 5 on the reverse. You may apply for a child custody order from the court.

**En el caso de peligro de secuestro de un niño o de una niña:** Esta orden será válida sólo hasta la hora y fecha indicada en el punto 5 al dorso. Usted puede solicitar de la corte una orden para la guarda del niño o de la niña (*Child Custody and Visitation Order*).

**To law enforcement:** The emergency protective order shall be served upon the restrained person by the officer, if the restrained person can reasonably be located, and a copy shall be given to the protected person. A copy shall be filed with the court as soon as practicable after issuance. Also, the officer shall have the order entered into CLETS (CARPOS). The availability of an emergency protective order shall not be affected by the fact that the endangered person has vacated the household to avoid abuse. A law enforcement officer shall use every reasonable means to enforce an emergency protective order. A law enforcement officer who acts in good faith to enforce an emergency protective order shall not be held civilly or criminally liable.

This emergency protective order is effective when made. This order shall expire on the date and time specified in item 5 on the reverse. The provisions of this emergency protective order take precedence in enforcement over provisions of other existing protective orders between the same protected and restrained persons to the extent the provisions of this order are more restrictive. In other words, the provisions in this emergency protective order take precedence over the provisions in any other protective order, including a criminal protective order, if (1) the person to be protected is already protected by the other protective order, (2) the person to be restrained is subject to that other order, and (3) the provisions in this emergency order are more restrictive than the provisions in that other order. The provisions in another existing protective order remain in effect and take precedence if they are more restrictive than the provisions in this emergency protective order.

## **Addendum B\_Countywide Strangulation Form.pdf**

# STRANGULATION REPORT

Case No. \_\_\_\_\_ Officer: \_\_\_\_\_ Page \_\_\_\_ of \_\_\_\_

## STRANGULATION METHOD

- ♦ **Method and/or Manner (how was Victim strangled):** ☐ One Hand (R) ☐ One Hand (L) ☐ Two Hands ☐ Forearm ☐ Knee/Foot ☐ Chokehold ☐ Ligature ☐ Other (explain): \_\_\_\_\_
- ♦ **Suspect right or left handed?** ☐ Right Handed ☐ Left Handed
- ♦ **Estimate how long you were strangled?** \_\_\_\_\_ **Multiple times?** ☐ No ☐ Yes # \_\_\_\_\_
- ♦ **Suffocated?** ☐ Yes ☐ No **How long?** \_\_\_\_\_ **What was used?** \_\_\_\_\_
- ♦ **What did Suspect say during strangulation/suffocation?** \_\_\_\_\_

- ♦ **Describe Suspect's demeanor during strangulation/suffocation?** \_\_\_\_\_
- ♦ **Describe how Suspect's face looked during strangulation/suffocation?** \_\_\_\_\_
- ♦ **What made Suspect stop?** \_\_\_\_\_
- ♦ **What did Suspect say after strangulation/suffocation?** \_\_\_\_\_
- ♦ **What did Victim think was going to happen during strangulation/suffocation?** \_\_\_\_\_

- ♦ **Describe how Suspect and Victim were positioned** (Suspect straddling Victim? Behind Victim? Was Victim restrained?): \_\_\_\_\_

- ♦ **Did you or did you attempt to physically stop the strangulation?** ☐ No ☐ Yes **Describe:** \_\_\_\_\_

- ♦ **Has Suspect strangled/suffocated you before?** ☐ No ☐ Yes **If yes, how many times?** \_\_\_\_\_

## VICTIM'S SYMPTOMS

SYMPTOMS	DURING	AFTER	VOICE CHANGES	SWALLOWING
Vision Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Painful to speak	<input type="checkbox"/> Neck tenderness
Difficult Breathing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Raspy/hoarse voice	<input type="checkbox"/> Trouble swallowing
Physical Pain	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Coughing	<input type="checkbox"/> Painful swallowing
Rapid Breathing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Unable to speak	<input type="checkbox"/> Neck pain
Shallow Breathing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Whispering	<input type="checkbox"/> Other
Coughing up Blood	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Other	
Vomiting/Dry Heave	<input type="checkbox"/>	<input type="checkbox"/>	<b>Explain other:</b> _____ _____ _____ _____	
Dizziness	<input type="checkbox"/>	<input type="checkbox"/>		
Headache	<input type="checkbox"/>	<input type="checkbox"/>		
Feeling Faint	<input type="checkbox"/>	<input type="checkbox"/>		
Disoriented	<input type="checkbox"/>	<input type="checkbox"/>		

- ♦ **Loss of consciousness?** ☐ Yes ☐ No ☐ Unsure **Unexplained Injury?** Describe: \_\_\_\_\_
- ♦ **Any change or loss of hearing during/after strangulation/suffocation?** ☐ Yes ☐ No Describe: \_\_\_\_\_
- ♦ **Any change or loss of vision during/after strangulation/suffocation?** ☐ Yes ☐ No Describe: \_\_\_\_\_
- ♦ **How did your body/head feel during/after strangulation/suffocation?** \_\_\_\_\_
- ♦ **Did the victim:** ☐ Urinate ☐ Defecate ☐ **Feel the urge to do one or both?** \_\_\_\_\_

FACE	EYES AND EYELIDS	NOSE	EARS
<input type="checkbox"/> Red or flushed <input type="checkbox"/> Petechiae <input type="checkbox"/> Scratch(es) or abrasion(s) <input type="checkbox"/> Sweating <input type="checkbox"/> Bruising <input type="checkbox"/> Other: _____	<input type="checkbox"/> Petechiae to R eye <input type="checkbox"/> Petechiae to L eye <input type="checkbox"/> Petechiae to R eyelid <input type="checkbox"/> Petechiae to L eyelid <input type="checkbox"/> Blood in eyeball(s) <input type="checkbox"/> Other: _____	<input type="checkbox"/> Petechiae <input type="checkbox"/> Scratch(es) or abrasion(s) <input type="checkbox"/> Swelling <input type="checkbox"/> Other: _____	<input type="checkbox"/> Petechiae on ear(s) <input type="checkbox"/> Bleeding from ear(s) <input type="checkbox"/> Bruising/discoloration/petechiae behind ear(s) <input type="checkbox"/> Swelling <input type="checkbox"/> Other: _____
MOUTH	UNDER CHIN	CHEST	SHOULDERS
<input type="checkbox"/> Bruise(s) <input type="checkbox"/> Swollen tongue <input type="checkbox"/> Swollen lip(s) <input type="checkbox"/> Scratche(s)/Abrasions <input type="checkbox"/> Petechiae <input type="checkbox"/> Other: _____	<input type="checkbox"/> Redness <input type="checkbox"/> Lacerations <input type="checkbox"/> Bruise(s) <input type="checkbox"/> Scratche(s)/Abrasions <input type="checkbox"/> Petechiae <input type="checkbox"/> Other: _____	<input type="checkbox"/> Redness <input type="checkbox"/> Lacerations <input type="checkbox"/> Bruise(s) <input type="checkbox"/> Scratche(s)/Abrasions <input type="checkbox"/> Petechiae <input type="checkbox"/> Other: _____	<input type="checkbox"/> Redness <input type="checkbox"/> Lacerations <input type="checkbox"/> Bruise(s) <input type="checkbox"/> Scratche(s)/Abrasions <input type="checkbox"/> Petechiae <input type="checkbox"/> Other: _____
NECK		HEAD	
<input type="checkbox"/> Redness <input type="checkbox"/> Tenderness/pain <input type="checkbox"/> Finger mark(s) <input type="checkbox"/> Fingernail impressions <input type="checkbox"/> Petechiae <input type="checkbox"/> Other: _____		<input type="checkbox"/> Ligature <input type="checkbox"/> Lacerations <input type="checkbox"/> Bruise(s) <input type="checkbox"/> Scratche(s)/Abrasions <input type="checkbox"/> Swelling <input type="checkbox"/> Hair pulled <input type="checkbox"/> Lacerations <input type="checkbox"/> Petechiae on scalp/head <input type="checkbox"/> Scratche(s)/Abrasions <input type="checkbox"/> Bumps <input type="checkbox"/> Hair pulled <input type="checkbox"/> Other: _____	

### OFFICER CHECKLIST

- ☐ Photograph all injuries and physical evidence.
- ☐ If strangulation was done using an object, photograph and collect the object.
- ☐ Document where all evidence items were found.
- ☐ Determine if jewelry was worn by either party during the incident. If so, photograph it and, when feasible, look for pattern injuries.
- ☐ If defecation or urination in clothing, collect the clothing as evidence.
- ☐ If victim vomited, take photos of the vomit.
- ☐ Take photographs of BOTH parties to document injuries and/or lack of injuries. Include hands, arms, face, chest, neck and all other areas the parties claim injury or physical contact occurred.
- ☐ Obtain evidence from hospital, if available, or follow-up to retrieve.

## **MedicalReleaseFormInv .pdf**





**Office of the District Attorney  
Stanislaus County**

**Jeff Laugero  
District Attorney**

**Assistant District Attorney  
Mark Zahner**

**Chief Deputies**  
Marlisa Ferreira  
Wendell Emerson  
Michael D. Houston  
Rick Mury  
Joseph Chavez

**Bureau of Investigation**  
Chief Terry L. Seese

---

**AUTHORIZATION FOR RELEASE OF RECORDS**

Patient \_\_\_\_\_  
Chart # \_\_\_\_\_  
DOB \_\_\_\_\_  
SSN \_\_\_\_\_

I hereby authorize \_\_\_\_\_ to release medical information to the  
following person(s) or entity:

\_\_\_\_\_  
\_\_\_\_\_

(Address of where information is to be sent)

The information released shall be limited to the following:

<input type="checkbox"/> All available information	Only the following:
___ History and Physical Exam	___ X-ray reports - films (Circle one)
___ Surgery reports	___ Lab
___ All information subsequent to _____	___ Other _____
___ Exclude specifically the following _____	

The information shall be used for the purpose of \_\_\_\_\_

I understand I am entitled to a copy of this authorization upon request. This authorization may be  
revoked by me at any time in writing.

\_\_\_\_\_  
Signature of patient or legal guardian

\_\_\_\_\_  
Witness

\_\_\_\_\_  
Dated

This form is not valid for records covered under 42 CFR, part II

## **Addendum A\_Countywide DV Form.pdf**

# DOMESTIC VIOLENCE REPORT

Case No. _____	Reporting Officer _____	Page ____ of ____
----------------	-------------------------	-------------------

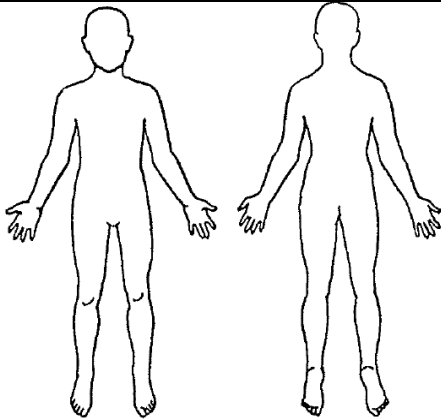
RELATIONSHIP	PRIOR HISTORY OF DV	EVIDENCE
<i>Check all that apply:</i> <input type="checkbox"/> Spouse <input type="checkbox"/> Former Spouse <input type="checkbox"/> Cohabitants <input type="checkbox"/> Former Cohabitants  <input type="checkbox"/> Same Sex <input type="checkbox"/> Dating/Engaged <input type="checkbox"/> Co-Parent  <b>LENGTH OF RELATIONSHIP:</b> ____ years ____ months  <b>DATE RELATIONSHIP ENDED:</b> _____	PRIOR HISTORY OF DV? <input type="checkbox"/> Yes <input type="checkbox"/> No PRIOR HISTORY OF DV DOCUMENTED? <input type="checkbox"/> Yes <input type="checkbox"/> No NUMBER OF PRIOR INCIDENTS: _____ DATE(S): _____ CASE NOS: _____ INVESTIGATING AGENCY: _____ <i>If undocumented ask about prior incidents and describe in narrative.</i>	VIDEOTAPED STATEMENTS? <input type="checkbox"/> Yes <input type="checkbox"/> No PHOTOS VICTIM'S INJURIES? <input type="checkbox"/> Yes <input type="checkbox"/> No PHOTOS SUSPECT'S INJURIES? <input type="checkbox"/> Yes <input type="checkbox"/> No PHOTOS OF CRIME SCENE? <input type="checkbox"/> Yes <input type="checkbox"/> No AUDIO RECORDING? <input type="checkbox"/> Yes <input type="checkbox"/> No SURVEILLANCE VIDEO? <input type="checkbox"/> Yes <input type="checkbox"/> No TYPE OF CAMERA? <input type="checkbox"/> 35mm <input type="checkbox"/> Digital

WITNESSES/CHILDREN	RESTRAINING ORDERS
<i>List children, CPS, first person V spoke to, interpreters, and RP in witness box.</i> WITNESSES PRESENT DURING DV? <input type="checkbox"/> Yes <input type="checkbox"/> No STATEMENT(S) TAKEN? <input type="checkbox"/> Yes <input type="checkbox"/> No CHILDREN PRESENT DURING DV? <input type="checkbox"/> Yes <input type="checkbox"/> No FOCUS NOTIFICATION MADE? <input type="checkbox"/> Yes <input type="checkbox"/> No CPS NOTIFIED? <input type="checkbox"/> Yes <input type="checkbox"/> No VICTIM CALL 911? <input type="checkbox"/> Yes <input type="checkbox"/> No ❖ IF NO, RP INTERVIEWED? <input type="checkbox"/> Yes <input type="checkbox"/> No INTERPRETER SERVICES PROVIDED? <input type="checkbox"/> Yes <input type="checkbox"/> No LANGUAGE: _____	<b>EPO ISSUED?</b> Judge: _____ <input type="checkbox"/> Yes Expires On: _____ <input type="checkbox"/> No Reason for No: _____ <b>EPO SERVED?</b> <input type="checkbox"/> Yes - all terms explained <input type="checkbox"/> No - at large/attached to I&B <b>PROTECTIVE ORDERS?</b> <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> Current <input type="checkbox"/> Expired <input type="checkbox"/> Served <input type="checkbox"/> Not Verified <input type="checkbox"/> Attached County: _____ Docket # _____

WEAPONS (PC 18250)	ARREST MADE/I&B
<i>Describe Weapon Use in Narrative</i> <input type="checkbox"/> FIREARM: _____ WEAPONS RECOVERED? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> BLUNT OBJECT: _____ FIREARMS IMPOUNDED FOR SAFETY? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> CUTTING INSTRUMENT/KNIFE _____ PROPERTY RECEIPT ISSUED? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> POISON _____ SUSPECT ON PROBATION FOR DV? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> PERSONAL (hands, feet, etc.) _____ <input type="checkbox"/> OTHER: _____	If no arrest is made or suspect not on scene, make sure you have Victim identify Suspect using CAL DMV, booking photo, family photo, or ask Vic if s/he has photos on phone. ARREST MADE? <input type="checkbox"/> Yes <input type="checkbox"/> No I&B ISSUED? <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT ID'D? <input type="checkbox"/> Yes <input type="checkbox"/> No METHOD OF ID: _____

LETHALITY ASSESSMENT	DOMESTIC VIOLENCE CHECKLIST
<i>Provide detailed explanation in narrative.</i> GUN PRESENT IN THE HOME/ACCESSIBLE TO SUSPECT <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT HAS USED OR THREATENED TO USE WEAPON <input type="checkbox"/> Yes <input type="checkbox"/> No RECENT SEPARATION OR THREATENED SEPARATION <input type="checkbox"/> Yes <input type="checkbox"/> No when? _____ SUSPECT THREATENED TO KILL VIC OR CHILDREN <input type="checkbox"/> Yes <input type="checkbox"/> No INCREASE IN FREQUENCY OR SEVERITY OF VIOLENCE <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT JEALOUS OR CONTROLS DAILY ACTIVITIES <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT PREVIOUSLY TRIED TO STRANGLE VIC <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT HAS ACCUSED VIC OF CHEATING <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT HAS DESTROYED CHERISHED PERSONAL ITEMS <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT HAS FORCED SEX WHEN VIC DID NOT WANT TO <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT HAS SAID "IF I CAN'T HAVE YOU, NO ONE CAN" <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT HAS DIRECTED VIOLENCE WHILE VIC PREGNANT <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT THREATENED OR ATTEMPTED SUICIDE <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT LOST JOB OR STATUS IN COMMUNITY <input type="checkbox"/> Yes <input type="checkbox"/> No SUSPECT ABUSES DRUGS OR ALCOHOL <input type="checkbox"/> Yes <input type="checkbox"/> No which? _____	BROCHURE + MARSY'S LAW PROVIDED + EXPLAINED <input type="checkbox"/> Yes <input type="checkbox"/> No VIC CONFIDENTIALITY EXPLAINED + FORM SIGNED <input type="checkbox"/> Yes <input type="checkbox"/> No RESTRAINING ORDERS EXPLAINED TO VIC <input type="checkbox"/> Yes <input type="checkbox"/> No PRIVATE PERSON'S ARREST EXPLAINED <input type="checkbox"/> Yes <input type="checkbox"/> No VIC REQUESTED + TRANSPORTED TO ANOTHER LOCATION <input type="checkbox"/> Yes <input type="checkbox"/> No VIC WANTS NOTIFICATION WHEN SUSPECT IS RELEASED <input type="checkbox"/> Yes <input type="checkbox"/> No VIC NOTIFICATION FORM COMPLETED + GIVEN TO JAIL <input type="checkbox"/> Yes <input type="checkbox"/> No VICTIM ADVOCATE CONTACT REQUESTED <input type="checkbox"/> Yes <input type="checkbox"/> No PRIOR CALLS TO LOCATION OR BETWEEN PARTIES <input type="checkbox"/> Yes <input type="checkbox"/> No BOL ISSUED DESCRIBING SUSPECT AND/OR WEAPONS <input type="checkbox"/> Yes <input type="checkbox"/> No

## VICTIM

<b>DEMEANOR</b> <input type="checkbox"/> Angry <input type="checkbox"/> Apologetic <input type="checkbox"/> Crying <input type="checkbox"/> Fearful <input type="checkbox"/> Hysterical <input type="checkbox"/> Calm <input type="checkbox"/> Upset <input type="checkbox"/> Nervous <input type="checkbox"/> Irrational <input type="checkbox"/> Threatening <input type="checkbox"/> Other: _____ _____	<b>INJURIES</b> <input type="checkbox"/> Complaint of Pain <input type="checkbox"/> Bruise(s) <input type="checkbox"/> Abrasion(s) <input type="checkbox"/> Minor Cut(s) <input type="checkbox"/> Laceration(s) <input type="checkbox"/> Fracture(s) <input type="checkbox"/> Concussion <input type="checkbox"/> Red mark(s) <input type="checkbox"/> Other: _____ _____ _____	<b>HEIGHT:</b> _____ <b>WEIGHT:</b> _____	<b>FRONT</b> <input type="checkbox"/> NONE VISIBLE		<b>BACK</b> <input type="checkbox"/> NONE VISIBLE
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------	-------------------------------------------------------	------------------------------------------------------------------------------------	------------------------------------------------------

**MEDICAL TREATMENT:**  
☐ NONE  
☐ EMT  
☐ WILL SEEK OWN  
☐ FIRST AID RENDERED  
☐ HOSPITAL  
☐ DECLINED  
☐ **PATIENT SIGNED FOR MEDICAL RECORDS TO BE RELEASED**

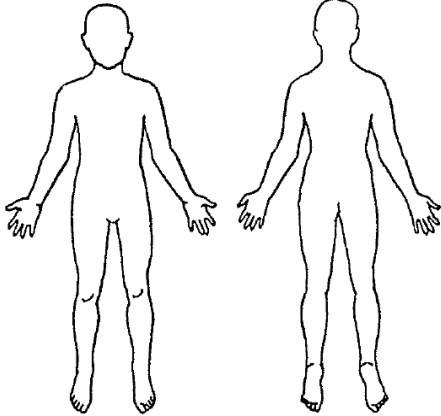
Transported by: \_\_\_\_\_ Names + #s of Treating EMTs/Paramedics: \_\_\_\_\_

Hospital: \_\_\_\_\_ Admitted? ☐ Yes ☐ No   Names + #s of Treating Physician/Nurse: \_\_\_\_\_

**ALCOHOL/CONTROLLED SUBSTANCE USED AT TIME OF INCIDENT:**  
☐ ALCOHOL  
☐ CONTROLLED SUBSTANCE  
*(Detail what + how in narrative)*

List Objective Symptoms of Intoxication Observed: \_\_\_\_\_

## SUSPECT

<b>DEMEANOR</b> <input type="checkbox"/> Angry <input type="checkbox"/> Apologetic <input type="checkbox"/> Crying <input type="checkbox"/> Fearful <input type="checkbox"/> Hysterical <input type="checkbox"/> Calm <input type="checkbox"/> Upset <input type="checkbox"/> Nervous <input type="checkbox"/> Irrational <input type="checkbox"/> Threatening <input type="checkbox"/> Other: _____ _____	<b>INJURIES</b> <input type="checkbox"/> Complaint of Pain <input type="checkbox"/> Bruise(s) <input type="checkbox"/> Abrasion(s) <input type="checkbox"/> Minor Cut(s) <input type="checkbox"/> Laceration(s) <input type="checkbox"/> Fracture(s) <input type="checkbox"/> Concussion <input type="checkbox"/> Red mark(s) <input type="checkbox"/> Other: _____ _____ _____	<b>HEIGHT:</b> _____ <b>WEIGHT:</b> _____	<b>FRONT</b> <input type="checkbox"/> NONE VISIBLE		<b>BACK</b> <input type="checkbox"/> NONE VISIBLE
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------	-------------------------------------------------------	--------------------------------------------------------------------------------------	------------------------------------------------------

☐ **SUSPECT FLED SCENE**

**MEDICAL TREATMENT:**  
☐ NONE  
☐ EMT  
☐ WILL SEEK OWN  
☐ FIRST AID RENDERED  
☐ HOSPITAL  
☐ DECLINED  
☐ **PATIENT SIGNED FOR MEDICAL RECORDS TO BE RELEASED**

Transported by: \_\_\_\_\_ Names + #s of Treating EMTs/Paramedics: \_\_\_\_\_

Hospital: \_\_\_\_\_ Admitted? ☐ Yes ☐ No   Names + #s of Treating Physician/Nurse: \_\_\_\_\_

**ALCOHOL/CONTROLLED SUBSTANCE USED AT TIME OF INCIDENT:**  
☐ ALCOHOL  
☐ CONTROLLED SUBSTANCE  
*(Detail what + how in narrative)*

List Objective Symptoms of Intoxication Observed: \_\_\_\_\_

**Personnel Manual TAB 8 Drug  
Free Workplace Policy.pdf**

PERSONNEL MANUAL  
TAB 08  
DRUG FREE WORKPLACE POLICY

INDEX

• Purpose .....	1
• Policy .....	1
• Process .....	2
• Application .....	3
• Employee Responsibilities .....	3
• Management Responsibilities and Guidelines .....	5
• Results of Drug and Alcohol Testing .....	6
• Confidentiality .....	6



## PERSONNEL MANUAL DRUG FREE WORKPLACE POLICY

Revised 6/2/15

### A. PURPOSE

It is the intention of this policy to eliminate substance abuse and its effects in the workplace. While Stanislaus County does not intend to intrude into the private lives of its employees, involvement with drugs and alcohol off the job can take its toll on job performance and employee safety. Our concern is that employees are in a condition to perform their duties safely and efficiently, in the interests of their fellow workers and the public as well as themselves. The presence and influence of drugs and alcohol on the job, and the influence of these substances on employees during working hours, are inconsistent with this objective.

Employees who think they may have an alcohol or drug usage problem are urged to voluntarily seek confidential assistance from the Employee Assistance Program. The County acknowledges that significant psychological and physical alcohol and drug dependency is an illness and pursuit of treatment by the employee is the preferable resolution to associated performance problems caused by such dependency. While the County will be supportive of those who seek help voluntarily, the County will be firm in identifying and disciplining those employees who do not seek help and are found to be impaired by drugs or alcohol during working hours.

This policy provides guidelines for the detection and deterrence of alcohol and drug abuse. It also outlines the responsibilities of County managers and employees. To that end, the County will act to prevent the use of alcohol or drugs which impair an employee's ability to safely and effectively perform the functions of the particular job. All persons covered by this policy should be aware that violation of the policy may result in discipline up to and including termination.

In recognition of the public service responsibilities entrusted to County employees, and that drug and alcohol usage can impair an employee's ability both mentally and physically to perform the duties and functions safely and effectively, the following policy against drug and alcohol impairment is hereby adopted by the County.

### B. POLICY

Definition – The term “drug” or “drugs” whenever used in this policy means any controlled substance that is not legally obtainable under State or Federal law, a prescription drug obtained or used without benefit of a valid prescription by a medical provider licensed to prescribe medications, and marijuana even if prescribed by a medical provider licensed to prescribe medications.

- Employees shall not be impaired by alcohol or drugs, nor possess alcohol or drugs at the assigned worksite. This policy also applies to employees working on-call duty.
- The illegal or unauthorized use of prescription drugs is prohibited. It is a violation of this policy to intentionally misuse and/or abuse prescription medications.
- Employees shall not sell or provide drugs or alcohol to any other employee while such employee is on duty.
- No alcoholic beverages are permitted at the assigned worksite or in County Vehicles other than at special events authorized by the Chief Executive Officer. County employees who reside on premises provided by the County shall be exempt from the restriction of this policy from possessing alcohol where they reside.
- "Probable cause" is such a state of facts as would lead a supervisor of ordinary care and prudence to believe, or to entertain an honest and strong suspicion that an employee is under the influence of drugs or alcohol so that the employee's ability to perform the functions of the job is impaired or so that the employee is not able to physically and/or mentally perform the duties of his or her position in a proper manner.

### C. PROCESS

The County reserves the right to search without employee consent all areas and property in which the County maintains control, or joint control, with the employee. Controlled and jointly controlled areas include County vehicles, offices, desks, file cabinets, etc. Notwithstanding the above, no employee shall have his or her locker or other space for storage that is owned or leased by the County that may be assigned to him or her, searched except under one of the following conditions: in his or her presence; with his/her consent; if a valid search warrant has been obtained; or, where he/she has been notified that a search will be conducted. Employee requests to be present during the search shall be honored if the employee is able to return to the worksite within one hour of notification of the search. All such searches shall be based upon probable cause to search. Probable cause forming the basis of the search shall be provided to the employee in writing. The written document shall be given to the employee prior to the search or, if that is not possible, within twenty-four hours after the search.

Any applicable privileges or confidentiality of files or documents will be honored by the County. If the County desires to search such documents or records, or the area where such documents are located, the appropriate process for searches and seizures as defined by California law will be followed. The County may notify the appropriate law enforcement agency that an employee may have drugs in his or her possession or in an area not jointly or fully controlled by the County.



Refusal to submit immediately for drug and/or alcohol testing, based upon probable cause of drug or alcohol impairment while on duty when ordered by the Department Head or his/her designee in accordance with County Code Section 3.08.050 may constitute insubordination and may be grounds for discipline. For the purpose of this policy, designee shall be defined as the assistant department head or other County manager who is assigned the authority to act for the Department Head during his or her absence.

Employees reasonably believed to be impaired by alcohol and/or drugs shall be prevented from engaging in further work and shall be detained for a reasonable time until they can be safely transported from the work site.

The County is committed to providing reasonable accommodation to those employees whose drug or alcohol problem classifies them as disabled under Federal and/or State law. The County is also committed to providing reasonable accommodation to employees who use lawfully prescribed medication(s) to treat or control a disability and who may need an accommodation because of the side effects of the medication(s).

The County has established a voluntary Employee Assistance Program (EAP) to assist those employees who voluntarily seek help for alcohol or drug problems. Employees should contact their supervisors, Human Resources, or the EAP Counselor for additional information. Information about the County's EAP is also available on the County's website at <http://www.stancounty.com/riskmgmt/risk-eb-eap-sub-main.shtm>

The provisions of this policy do not act to limit or restrict in any manner a law enforcement officer's ability to enforce all appropriate state and federal laws. No department shall have any rule or policy which contravenes or which is in conflict with this Drug Free Work Place Policy.

#### **D. APPLICATION**

This policy applies to all County employees. This policy applies to alcohol and drugs which could impair an employee's ability physically and/or mentally to effectively and safely perform the functions and duties of the employee's position.

#### **E. EMPLOYEE RESPONSIBILITIES**

1. An employee must not report to work or be subject to duty while his/her physical and/or mental ability to perform job duties is impaired due to on or off duty alcohol or drug use.
2. An employee must not possess drugs or alcohol as defined by this policy during working hours or while subject to duty, on breaks, or at any time while at the assigned worksite. An exception exists for those employees whose duties require possession of

drugs and/or alcohol in the course and scope of job duties (i.e., undercover, narcotics investigators).

3. An employee must not directly or through a third party sell or provide drugs or alcohol to any person, including any employee, while either employee or both employees are on duty.
4. Prescription and over-the-counter medications are not prohibited when taken in standard dosage and/or according to a physician's prescription. However, an employee taking prescribed or over-the-counter medications will be responsible for consulting the prescribing physician and/or pharmacist and/or the medication label to ascertain whether the medication may interfere with the ability to safely and effectively perform his or her job. If the use of a medication could compromise the safety of the employee, fellow employees, or the public, it is the employee's responsibility to notify the supervisor or manager (e.g., call in sick, use leave, request change of duty) to avoid any unsafe workplace practices. Unless the employee is working in a position affecting public safety, the employee, is not required to reveal the existence of a disability or disclose the medications the employee is taking if the employee can manage the medications through the use of leave or benefits available to all employees without formally requesting a reasonable accommodation.
5. An employee must submit immediately to an alcohol or drug test when ordered, in writing, by a Department Head or his/her designee when probable cause exists that the employee is impaired by drugs and/or alcohol.
6. An employee may be required to submit to a fitness for duty examination where there is a reasonable and objective belief that an employee may be impaired while on duty by prescription or over-the-counter medications that the employee is taking to treat or control a disability. The purpose of the fitness for duty examination will be limited to determining whether the employee can safely perform the essential functions of the job with or without accommodation. Such fitness for duty examinations will be conducted in compliance with the limitations set forth under State and Federal law.
7. An employee must provide within two (2) working days of request bona fide verification of a current valid prescription in the employee's name for any potentially impairing medication identified when a drug screening/test is positive. Extensions of time beyond the two working days may be granted upon the showing of good cause. An employee must abide by the regulations of the Federal Drug-Free Workplace Act of 1988. Thus, such employees who are convicted after March 18, 1989 of any criminal drug statute for a violation occurring in the workplace must notify the Chief Executive Officer no later than five (5) days after the conviction. Once the County is notified of the conviction, the County must then notify the appropriate Federal agency of the conviction. With respect to any employee so convicted, the County will take appropriate personnel action up to and including termination. As a condition of

continued employment, the County may require the convicted employee to satisfactorily participate in an approved drug abuse rehabilitation program.

#### **F. MANAGEMENT RESPONSIBILITIES AND GUIDELINES**

1. Department Heads or their designees are responsible for reasonable enforcement of this policy.
2. Department Head or his/her designee may order an employee in writing to submit to an alcohol or drug test following the County's Ordered for Cause Alcohol and Drug Testing procedure including notifying the employee of their right to representation in accordance with this policy. When a Department Head or his/her designee has probable cause that an employee is intoxicated or impaired by drugs or alcohol while on the job or receiving compensation for on-call duty and thereby subject to being called, and is not physically and/or mentally able to perform the duties of his/her position. Should employee be a Department of Transportation (DOT) driver acting in the course and scope of employment, the Department Head or designee should refer to DOT policy for additional information.
3. Prior to the request for the alcohol or drug test, a Department Head or his/her designee ordering an employee to undergo an alcohol or drug test shall document in writing the facts constituting probable cause that the employee in question is intoxicated or impaired by alcohol or drugs.
4. Any Department Head or his/her designee encountering an employee who refuses an order to submit to an alcohol or drug test shall remind the employee of the requirements and disciplinary consequences of this policy. Where there is probable cause that the employee is then impaired by alcohol or drugs, the Department Head or his/her designee should detain the employee for a reasonable time until the employee can be safely transported home or removed to another appropriate location.
5. Any Department Head or his/her designee shall not physically search the person of employees; nor shall they search the personal possession of employees without the freely given written consent by the employee, unless such search is authorized by County Ordinance or policy.
6. Managers and supervisors shall notify their Department Head or designee when there is probable cause to believe that an employee may have drugs or alcohol in his or her possession or in an area not jointly or fully controlled by the County. If the Department Head or designee concurs that there is probable cause of alcohol or drug possession, the Department Head shall notify the appropriate parties, including Human Resources and County Counsel.

7. The Department Head or his/her designee shall give due consideration to the employee's completion of any generally recognized treatment plan, including that treatment as may be recommended by the Employee's Assistance Program when determining whether disciplinary action shall be taken and/or the appropriate level of discipline.

#### **G. RESULTS OF DRUG AND ALCOHOL TESTING**

1. A positive result from a drug and/or alcohol test may result in disciplinary action, up to and including termination.
2. If the alcohol or drug test is positive, the County shall conduct an investigation to gather all relevant facts. The decision to discipline or discharge will be carried out in conformance with the County's discipline procedures and policies.
3. Testing and reporting of test results will follow the guidelines and all subsequent amendments as established by the Department of Health and Human Services as promulgated in Volume 53, No. 69 of the Federal Register and as incorporated herein and made a part of this policy by reference.

#### **H. CONFIDENTIALITY**

Medical or laboratory reports or test results shall not appear in an employee's general personnel file unless they result in discipline. Information of this nature will be contained in a separate confidential medical folder that will be securely kept under the control of the Chief Executive Officer/Director of Personnel or designee. The reports or test results may be disclosed to County management on a strictly need-to-know basis and to the employee upon request. Disclosures without employee consent may also occur when: (1) the information is compelled by law or by judicial or administrative process; (2) the information has been placed at issue in a formal dispute between the employer and employee; (3) the information is needed by medical personnel for the diagnosis or treatment of the employee who is unable to authorize disclosure; (4) when requested by DOT or any state or local officials with regulatory authority over the County or any of its safety-sensitive employees.

## **Supplemental Hate Crime Report.pdf**

☐ Hate incident (No Crime Committed)

☐ Hate Crime (422.6 PC, 51.7 CC, 52.1 CC)

### VICTIM

#### VICTIM TYPE

☐ Individual

Legal name (Last, First): \_\_\_\_\_

Date of Birth	Age	Sex	Race

☐ School, business or organization

Name: \_\_\_\_\_

Type: \_\_\_\_\_  
(e.g., non-profit, private, public school)

☐ Faith-based organization

Name: \_\_\_\_\_

Faith: \_\_\_\_\_

☐ Other

Name: \_\_\_\_\_

Type: \_\_\_\_\_

Address: \_\_\_\_\_

Date and time of incident: \_\_\_\_\_

Location of incident: \_\_\_\_\_

Date and time of report: \_\_\_\_\_

Location of report: \_\_\_\_\_

Agency Case #: \_\_\_\_\_

#### NATURE OF CALL FOR SERVICE (check all that apply)

☐ Crime against persons

☐ Crime against property

☐ Gang activity

☐ Other \_\_\_\_\_

### BIAS

#### TYPE OF BIAS

(Check all characteristics that apply)

☐ Disability

☐ Gender

☐ Gender identity/expression

☐ Sexual orientation

☐ Race

☐ Ethnicity

☐ Nationality

☐ Religion

☐ Significant day of offense

(e.g., 9/11, holy days)

☐ Association with a person or group with  
one or more of these characteristics  
(actual or perceived)

☐ Other: \_\_\_\_\_

#### ACTUAL OR PERCEIVED BIAS – VICTIM'S STATEMENT

☐ Actual bias [Victim has the indicated characteristic(s)].

☐ Perceived bias [Suspect believed victim had the indicated  
characteristic(s)].

#### REASON FOR BIAS:

Do you feel you were targeted based on one of these characteristics?

☐ Yes ☐ No

Do you know what motivated the suspect to commit this crime?

☐ Yes ☐ No

Do you feel you were targeted because you associated yourself with an  
individual or a group?

☐ Yes ☐ No

Are there indicators the suspect is affiliated with a Hate Group  
(i.e., literature/tattoos)?

☐ Yes ☐ No

Are there Indicators the suspect is affiliated with a criminal street gang?

☐ Yes ☐ No

#### BIAS INDICATORS (CHECK ALL THAT APPLY):

☐ Hate speech

☐ Acts/gestures

☐ Property damage

☐ Symbol used

☐ Written/electronic communication

☐ Graffiti/spray paint

☐ Other: \_\_\_\_\_

**SUPPLEMENTAL HATE CRIME REPORT**

POST 2-365 (01/2023) Page 2 of 2

**HISTORY****SUSPECT INFORMATION**Legal name (Last, First):  
\_\_\_\_\_Other Names used (AKA):  
\_\_\_\_\_

Date of Birth	Age	Sex	Race

Relationship to Victim:  
\_\_\_\_\_**RELATIONSHIP BETWEEN SUSPECT & VICTIM**Suspect known to victim: ☐ Yes ☐ NoNature of relationship:  
\_\_\_\_\_

Length of relationship: \_\_\_\_\_

☐ Prior reported incidents with suspect: *Total #* \_\_\_\_\_

Prior unreported incidents with suspect:

☐ Yes ☐ No ☐ Unknown**WEAPONS/FORCE**Weapon(s) used during incident? ☐ Yes ☐ No Type: \_\_\_\_\_Force used during incident? ☐ Yes ☐ No Type: \_\_\_\_\_**EVIDENCE**Witnesses present during incident? ☐ Yes ☐ No Statements taken? ☐ Yes ☐ NoEvidence collected? ☐ Yes ☐ No Recordings: ☐ Video ☐ Audio ☐ BookedPhotos taken? ☐ Yes ☐ No Suspect identified: ☐ Field ID ☐ By photo/video ☐ Known**RESOURCES**Resources offered at scene: ☐ Yes ☐ No☐ Marsy's Law Handout ☐ Hate Crimes Brochure ☐ Other: \_\_\_\_\_**MEDICAL****Victim****Suspect**☐☐

Declined medical treatment

☐☐

Will seek own medical treatment

☐☐

Received medical treatment

☐☐

Injuries observed

**Completed by****Date**

Name/Title/ID number

## **Complaint and Greivance Procedure.pdf**





## PERSONNEL MANUAL COMPLAINT AND GRIEVANCE PROCEDURES

Revised 8/04

The following is the County procedure for settling grievances. Exceptions to this procedure, which provided for Binding Arbitration, exist in a number of Memoranda of Understanding. Please refer to the applicable MOU or check with the Personnel Department if there are questions.

### PROCEDURE FOR SETTLING GRIEVANCES

#### A. Intent:

It is the intent of this ordinance to provide orderly and equitable procedures for the presentation and resolution of misunderstandings and disputes between the County and its employees. It is further intended that the exercises of these rights in good faith be available to all County employees, (except as herein provided) without fear of reprisal or coercion.

#### B. Definitions:

1. Grievance - A grievance is defined as an employee initiated allegation that a term or condition of employment established by State Law, County Ordinance, Resolution, Memorandum of Understanding or Written Departmental Policy is being violated provided, however, that such term or condition of employment is not subject to the discretion of the County or is not a subject outside of the scope of representation as defined in Section 3500 et. seq. of the Government Code or the County's Employee Relations Ordinance. This grievance procedure shall not apply to matters within the scope of applicable Federal or State grievance procedures.
2. Complaint - A complaint is defined as an employee initiated allegation or dispute concerning terms and conditions of employment which are not grievances as defined above. Complaints shall be handled as herein provided except that a complaint may not be appealed to the Chief Executive Officer.

#### C. Exclusion of Disciplinary Appeals and Equal Employment Opportunity Grievances - Appeals from disciplinary actions or grievances alleging violation of the County's policies of equal employment opportunity or affirmative action or involving allegations of employment discrimination will be handled pursuant to the County's Equal Employment Opportunity Grievance Procedure.

#### D. Representation - In presenting and resolving grievances, employees may represent themselves on County time, or may designate a representative of their own choosing. Costs associated with such representation, if any, will be borne by the employee.

E. Time Limits - The time limits herein specified may be extended to a definite date by mutual consent of the parties. Failure to meet time limits by the employee shall constitute withdrawal of the grievance. Such failure by the County shall entitle the employee to request the next step in the procedure.

F. Grievance Procedure Steps:

1. Informal Discussion - Every effort should be made to settle grievances at the lowest level of supervision possible. The employee should advise his immediate supervisors that a grievance is present and explain it to the immediate supervisor no later than fifteen working days after he becomes or should become aware of the issue. The immediate supervisor shall thereafter hear, and decide the matter informing the employee of the decision orally within seven working days.
2. Written Grievances - If the grievance is not resolved through informal discussion, the employee may within seven working days from the date of the supervisor's informal decision, submit a written grievance to said supervisor with a copy submitted to the Department Head and the Chief Executive Officer. Such a written grievance, signed by the employee shall set forth the facts at issue, the relief sought and the time of occurrence of any alleged incident or violations precipitating the grievance. The supervisor shall thereafter further investigate and consider the grievance and deliver a written decision to the employee within seven working days after receiving the grievance.
3. Department Head Review - If the grievance is not resolved by the written decision of the supervisor, the employee may request in writing within seven working days after delivery of prior written decision that the grievance be reviewed by the Department Head. If such a request is received, the Department Head or his designee shall conduct such meeting(s) with the employee, informal hearings or investigations as are appropriate in his judgment and deliver to the employee a written decision within seven working days after receipt of the review request.
4. Advisory Opinion of Chief Executive Officer - At any point in this procedure after filing a written grievance or complaint, the Chief Executive Officer may offer, or either party may request, the non-binding advisory opinion verbal or in writing of the Chief Executive Officer concerning resolution of the grievance or complaint.
5. Grievance Appeal - If the employee wishes to appeal the decision of the Department Head, he may do so, in writing to the Chief Executive Officer within seven working days after receipt of the Department Head decision. The Chief Executive Officer shall thereafter conduct an informal hearing, and any other meetings or investigations as are appropriate in his judgment. Upon the request of either party or motion of the Chief Executive Officer, such hearing and other investigations shall be conducted by a designee(s) selected by the Chief Executive Officer with the consent of the parties. The

written decision of the Chief Executive Officer shall be delivered to the employee within fifteen working days after receipt of the appeal. The decision of the Chief Executive Officer shall be the final step in the County's procedure for settling grievances except in the case of an elected Department Head, the decision of the Chief Executive Officer may be appealed by the Department Head to the Board of Supervisors within seven working days after receipt of the decision.

#### PROCEDURE FOR SETTLING GRIEVANCES INCLUDING BINDING ARBITRATION (MOU PROVISION)

(The following procedure has been negotiated and applies only to those employees assigned to the following bargaining units: Mid-management/Supervisory; Office Worker/Clerical; Crafts/Maintenance/Institutional; Technical Services; Community and Health Services; Attorneys; Registered Nurses; Deputy Probation Officers, Communications Dispatchers and Fire Safety. Please refer to the MOU with the Deputy Sheriff's Association for the Binding Arbitration procedure applicable to that represented unit.)

A. Intent: It is the intent of this provision of the Memorandum of Understanding to provide orderly and equitable procedures for the presentation and resolution of misunderstandings and disputes between the County and its employees. It is further intended that the exercises of these rights in good faith be available to all County employees, (except as herein provided) without fear of reprisal or coercion.

B. Definitions:

1. Grievance - A grievance is defined as an employee initiated allegation that a term or condition of employment established by State Law, County Ordinance, Resolution, Memorandum of Understanding or Written Departmental Policy is being violated provided, however, that such term or condition of employment is not subject to the discretion of the County or is not a subject outside of the scope of representation as defined in Section 3500 et. seq. of the Government Code or the County's Employee Relations Ordinance. This grievance procedure shall not apply to matters within the scope of applicable Federal or State grievance procedures.
2. Complaints - A complaint is defined as an employee initiated allegation or dispute concerning terms and conditions of employment which are not grievances as defined above. Complaints shall be handled as herein provided except that a complaint may not be appealed to the Chief Executive Officer or to arbitration.

C. Exclusion of Disciplinary Appeals and Equal Employment Opportunity

Grievances - Appeals from disciplinary actions or grievances alleging violation of the County's policies of equal employment opportunity or affirmative action or involving allegations of employment discrimination will be handled pursuant to the County's Equal

Employment Opportunity Grievance Procedure and does not include Binding Arbitration as the final step in the procedure.

- D. Representation - In presenting and resolving grievances, employees may represent themselves on County time, within reason, or may designate a representative of their own choosing. Costs associated with such representation, if any, will be borne by the employee.
- E. Time Limits - The time limits herein specified may be extended to a definite date by mutual consent of the parties. Failure to meet time limits by the employee shall constitute withdrawal of the grievance. Such failure by the County shall entitle the employee to request the next step in the procedure.

VI. Grievance Procedure Steps:

- A. Informal Discussion - Every effort should be made to settle grievances at the lowest level of supervision possible. The employee should advise his immediate supervisor that a grievance is present and explain it to the immediate supervisor no later than fifteen (15) working days after he/she becomes or should become aware of the issue. The immediate supervisor shall thereafter hear, and decide the matter informing the employee of the decision orally within seven (7) working days.
- B. Written Grievances - If the grievance is not resolved through informal discussion, the employee may within seven (7) working days from the date of the supervisor's informal decision, submit a written grievance to said supervisor with a copy submitted to the Department Head and the Director of Personnel. Such a written grievance, signed by the employee shall set forth the facts at issue, the relief sought and time of occurrence of any alleged incident or violations precipitating the grievance. The supervisor shall thereafter further investigate and consider the grievance and deliver a written decision to the employee within seven (7) working days after receiving the grievance.
- C. Department Head Review - If the grievance is not resolved by the written decision of the supervisor, the employee may request in writing within seven (7) working days after delivery of prior written decision that the grievance be reviewed by the Department Head. If such a request is received, the Department Head or his/her designee shall conduct such meeting(s) with the employee, informal hearings or investigations as are appropriate in his/her judgment and deliver to the employee a written decision within seven (7) working days after receipt of the review request.
- D. Advisory Opinion of Director of Personnel - At any point in this procedure after filing a written grievance or complaint, the Director of Personnel may offer, or either party may request, the non-binding advisory opinion verbal or in writing of the Director of Personnel concerning resolution of the grievance or complaint.

- E. Grievance Appeal - If the employee wishes to appeal the Department Head's decision, he/she shall do so in writing to the Director of Personnel within ten working days after receipt of the Department Head's decision. The employee may elect to submit the grievance for final decision to the Chief Executive Officer. If the employee is represented by the recognized employee representative of the assigned bargaining unit, through the elected representative only, the grievance may be submitted for Binding Arbitration. Within the specified time period the employee and/or the elected representative as specified herein, shall specify in writing to the Director of Personnel whether the grievance should be submitted to the Chief Executive Officer or Binding Arbitration. The decision to utilize Binding Arbitration shall be the prerogative of the recognized employee organization only, with the employee's concurrence; access to only one of the two procedures for the purpose of resolving the alleged grievance shall be given the employee(s); the option of procedure utilized shall be binding and irrevocable upon the employee and the employee's recognized employee organization; and the procedure utilized shall be limited to grievances only as defined in Section II, Subsection A "Definitions, Grievance" herein, excluding complaints.

1. Submission of the Grievance Appeal to the Chief Executive Officer

If the employee wishes to appeal the Department Head's decision to the Chief Executive Officer, in lieu of Binding Arbitration, the employee shall do so in writing to the Director of Personnel specifically stating this option, within ten working days after receipt of the Department Head's decision. The Chief Executive Officer or his/her designee shall thereafter conduct an informal hearing, and any other meetings or investigations as are appropriate in his/her judgment. The written decision of the Chief Executive Office or his/her designee shall be delivered to the employee within fifteen working days after receipt of the appeal. The decision of the Chief Executive Officer or his/her designee shall be the final step in the County's procedure for settling grievances. For the purpose of this section, the Director of Personnel shall not serve as the designee if the Director of Personnel has rendered an advisory opinion concerning the grievance. This does not preclude the Chief Executive Officer from utilizing the advisory opinion of the Director of Personnel.

2. Submission of the Grievance Appeal to Binding Arbitration

If the employee wishes to appeal the Department Head's decision and elects to not refer the matter to the Chief Executive Officer for final resolution, the employee may through the recognized representative of the employee's assigned bargaining unit only, elect Binding Arbitration by writing to the Director of Personnel within ten working days after receipt of the Department Head's decision. Prior to the selection of the Arbitrator and submission of the grievance for hearing by an Arbitrator, the Director of Personnel shall informally review the grievance and determine whether said grievance may be

adjusted to the satisfaction of the parties. The Director of Personnel shall have ten (10) working days in which to review and seek amicable resolution of the grievance.

a. Selection of Arbitrator

If the required steps of the grievance procedure have been exhausted and the grievance remains unresolved and is subject to arbitration, the Arbitrator may be selected by mutual agreement between the Director of Personnel and the grievant's recognized representative of the assigned bargaining unit. However, should the parties fail to mutually agree on an Arbitrator they shall make a joint request of the State Conciliation Service for a list of five qualified arbitrators. The Arbitrator shall be selected from the list by the parties alternately striking names with the first strike determined by chance, until only one name remains, and that person shall serve as Arbitrator.

b. Arbitration Issues

The parties shall, within 15 working days following the informal review of the Director of Personnel, exchange in writing their understanding of the questions to be submitted to arbitration. Thereafter, the parties to the arbitration shall use their best efforts to exchange a written summary of the evidence they intend to offer and to reach agreement on and reduce to writing the question or questions to be submitted to arbitration. The agreed upon question or questions, if agreement is reached, together with the exchanged summaries of evidence and a list of witnesses to be used by each side, shall be submitted to each other and the Arbitrator no later than five (5) working days prior to the arbitration hearing.

c. Arbitration Expenses Shares

The cost of employing the Arbitrator shall be borne equally by the parties to the arbitration. All other costs such as, but not limited to, attorney's fees shall be borne only by the party incurring that cost. If both parties agree to the use of a Court Reporter, or if the Arbitrator requires the use of a Court Reporter, the cost of the Court Reporter shall be shared equally. Absent mutual agreement, the side requesting use of the Court Reporter shall absorb the cost. The cost of the transcript, if one is prepared, shall be absorbed by the party requesting the transcript, unless both parties mutually agree to share the cost of the transcript. If the Arbitrator requests that a copy of the transcript be prepared both parties shall equally share the cost of the transcript.

d. Duty of Arbitrator

The Arbitrator shall conduct an informal hearing, and any other meetings or investigations as are appropriate in his/her judgment. The Arbitrator shall not have the right to amend, modify, nullify, ignore, add to, or subtract from the provisions of the Memorandum of Understanding, County Ordinance, Resolution, or Written Departmental Policy. He/she shall consider and make a decision with respect to only the specific issue(s) submitted, and shall not have authority to make a decision on any other issue not so submitted. In the event, the Arbitrator finds a violation of the Memorandum of Understanding, applicable State or Federal law, County Ordinance, Board Resolution or Written Departmental Policy, he/she shall decide the appropriate resolution. The Arbitrator shall have no authority to substitute his/her judgment for that of the County as to any matter within the County's discretion. The decision and award of the Arbitrator shall be based solely upon the evidence and arguments presented to the Arbitrator by the respective parties. Proposals to add to or change the Memorandum of Understanding or written agreements or addenda supplementary hereto shall not be arbitrable and no proposal to modify, amend or terminate this Memorandum of Understanding, nor any matter or subject arising out of or in connection with such proposals, may be referred to arbitration under this Section.

e. Binding Decision

The decision of the Arbitrator shall be binding upon the employee, the employee's duly recognized employee organization and the County.

Based upon significant financial impact of the arbitrator's decision upon the County, within 15 working days of receipt of the arbitrator's decision the County may request that the Union meet with the County to discuss the financial impact of the decision. The Union agrees to meet and consult with the County over the impact upon the County of the decision. Absent agreement between the parties to modify or mitigate the impact of the arbitrator's decision, the decision of the Arbitrator shall be final and binding on the parties.

f. Arbitrator's Decision Due

Unless the parties agree otherwise, the Arbitrator shall render the decision in writing within 30 days following the close of the hearing to the Director of Personnel. The Director of Personnel shall immediately provide a copy of the decision to the employee, the employee's duly elected representative and the Department Head. If requested by either party, the decision shall be accompanied by findings of fact and conclusions of law.

g. Non-Employee Organization Representation

In the event that an employee chooses to represent himself/herself, or arranges for representation independent of the recognized employee organization, arbitration as provided herein shall not be available to the employee.



## **CJIS Security Policy v5\_5\_20160601 (2) (1).pdf**



# **Criminal Justice Information Services (CJIS) Security Policy**

Version 5.5

06/01/2016

CJISD-ITS-DOC-08140-5.5



Prepared by:  
CJIS Information Security Officer

Approved by:  
CJIS Advisory Policy Board

## EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

## CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5.0	Policy Rewrite	Security Policy Working Group	02/09/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	07/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	08/09/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	08/04/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/06/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2016	APB & Compact Council

## SUMMARY OF CHANGES

Version 5.5

### APB Approved Changes

1. Section 5.2 Policy Area 2: Security Awareness Training: added language, Spring 2015, APB20, SA2, Security Awareness Training Requirements.
2. Section 5.2.1.1 All Personnel: change section title to “Level One Security Awareness Training”, modify language and required training topics, Spring 2015, APB20, SA2, Security Awareness Training Requirements.
3. Section 5.2.1.2 Personnel with Physical and Logical Access: change section title to “Level Two Security Awareness Training”, modify language and moved required training topics from previous Section 5.2.1.1, Spring 2015, APB20, SA2, Security Awareness Training Requirements.
4. Section 5.2.1.3 Personnel with Information Technology Roles: change section title to “Level Three Security Awareness Training”, modify language and moved required training topics from previous Section 5.2.1.2, Spring 2015, APB20, SA2, Security Awareness Training Requirements.
5. Section 5.2.1.4 Level Four Security Awareness Training: added section and moved required training topics from previous Section 5.2.1.3, Spring 2015, APB20, SA2, Security Awareness Training Requirements.
6. Section 5.2 Figure 4: changed figure title and added a use case for each level of security awareness training, Fall 2015, APB12, SA4, Security Awareness Training Requirements.
7. Section 5.3 Incident Response: modified language to indicate any incident involving criminal justice information, Fall 2015, APB12, SA3, Security Incident Response Reporting.
8. Section 5.6.2.2 Advanced Authentication: add language describing the use of out-of-band authenticator, Spring 2015, APB 20, SA4, Clarification of Out-of-Band Authentication for Advanced Authentication (AA).
9. Section 5.9.1 Physically Secure Location: modified language to include security awareness training reference, Spring 2015, APB20, SA2, Security Awareness Training Requirements.
10. Section 5.10.2 Facsimile Transmission of CJI: modified language and introduced a new requirement, Fall 2015, APB12, SA1, Faxing Requirements in the CJIS Security Policy.
11. Section 5.11.2 Audits by the CSA: add language allowing CSA audits of vendor facilities, Spring 2015, APB 20, SA3, CJIS Systems Agency (CSA) Audit of Contractor Facilities.
12. Section 5.12.1.1(7) Minimum Screening Requirements for Individuals Requiring Access to CJI: add language allowing CSO delegation of continuing access determination for non-felony offenses, Spring 2015, APB 20, SA5, CJIS Systems Officer (CSO) Delegation of Personnel Screening Requirements.
13. Section 5.13 Policy Area 13: Mobile Devices: modify language throughout the entire section based on Mobile Security Task Force recommendations, Fall 2015, APB12, SA2, Request to Modify CJIS Security Policy Section 5.13 Mobile Devices.
14. Appendix A Terms and Definitions: add definitions for “Out-of-band” and “In-band”, Spring 2015, APB 20, SA4, Clarification of Out-of-Band Authentication for Advanced Authentication (AA).

15. Appendix A Terms and Definitions: add definition for “Facsimile (Fax)”, Fall 2015, APB12, SA1, Faxing Requirements in the CJIS Security Policy.
16. Appendix A Terms and Definitions: add definitions for “Full-feature Operating System”, “Limited-feature Operating System”, “Mobile (WiFi) Hotspot”, “Wireless Access Point”, and “Wireless (WiFi) Hotspot”, Fall 2015, APB12, SA2, Request to Modify CJIS Security Policy Section 5.13 Mobile Devices.
17. Appendix F.1 Security Incident Response Form: modified form to indicate any incident involving criminal justice information, Fall 2015, APB12, SA3, Security Incident Response Reporting.
18. Appendix K Criminal Justice Agency Supplemental Guidance: replace current appendix with new appendix, Spring 2015, APB 20, SA8, Evaluation of Appendix K.

#### Administrative Changes<sup>1</sup>

1. Figure 14 – A Local Police Department’s Information Systems & Communications Protections: change the title of the figure and add use faxing cases. *Security and Access Subcommittee requested the use cases be added.*
2. Appendix C Network Topology Diagrams, Figures C.1-A, B, C, and D: added required information from Section 5.7.1.2 Network Diagram to diagrams. *Sample diagrams did not contain the required elements of agency name, effective date of drawing, and “For Official Use Only” marking.*
3. Appendix G Best Practices: added new Appendix G.5 Administrator Accounts for Least Privilege and Separation of Duties, Spring 2015, SA6 (info only). *Security and Access Subcommittee approved the appendix to be added under the APB approved ISO latitude for administrative changes.*

KEY TO APB APPROVED CHANGES (e.g. “Fall 2013, APB11, SA6, Future CSP for Mobile Devices”):

Fall 2013 – Advisory Policy Board cycle and year

APB## – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Topic Title

---

<sup>1</sup> Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

# TABLE OF CONTENTS

<b>Executive Summary .....</b>	<b>i</b>
<b>Change Management .....</b>	<b>ii</b>
<b>Summary of Changes.....</b>	<b>iii</b>
<b>Table of Contents .....</b>	<b>v</b>
<b>List of Figures.....</b>	<b>x</b>
<b>1 Introduction.....</b>	<b>1</b>
1.1 Purpose.....	1
1.2 Scope.....	1
1.3 Relationship to Local Security Policy and Other Policies .....	1
1.4 Terminology Used in This Document.....	2
1.5 Distribution of the CJIS Security Policy.....	2
<b>2 CJIS Security Policy Approach .....</b>	<b>3</b>
2.1 CJIS Security Policy Vision Statement.....	3
2.2 Architecture Independent.....	3
2.3 Risk Versus Realism .....	3
<b>3 Roles and Responsibilities .....</b>	<b>4</b>
3.1 Shared Management Philosophy.....	4
3.2 Roles and Responsibilities for Agencies and Parties .....	4
3.2.1 CJIS Systems Agencies (CSA) .....	5
3.2.2 CJIS Systems Officer (CSO).....	5
3.2.3 Terminal Agency Coordinator (TAC).....	6
3.2.4 Criminal Justice Agency (CJA).....	6
3.2.5 Noncriminal Justice Agency (NCJA).....	6
3.2.6 Contracting Government Agency (CGA) .....	7
3.2.7 Agency Coordinator (AC).....	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO) .....	7
3.2.9 Local Agency Security Officer (LASO) .....	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO) .....	8
3.2.11 Repository Manager .....	9
3.2.12 Compact Officer.....	9
<b>4 Criminal Justice Information and Personally Identifiable Information .....</b>	<b>10</b>
4.1 Criminal Justice Information (CJI) .....	10
4.1.1 Criminal History Record Information (CHRI).....	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information.....	11
4.2.1 Proper Access, Use, and Dissemination of CHRI.....	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information.....	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information.....	11
4.2.3.1 For Official Purposes .....	11
4.2.3.2 For Other Authorized Purposes .....	12
4.2.3.3 CSO Authority in Other Circumstances .....	12
4.2.4 Storage.....	12
4.2.5 Justification and Penalties .....	12

4.2.5.1	Justification .....	12
4.2.5.2	Penalties .....	12
4.3	Personally Identifiable Information (PII).....	12
<b>5</b>	<b>Policy and Implementation .....</b>	<b>14</b>
5.1	Policy Area 1: Information Exchange Agreements .....	15
5.1.1	Information Exchange .....	15
5.1.1.1	Information Handling.....	15
5.1.1.2	State and Federal Agency User Agreements .....	15
5.1.1.3	Criminal Justice Agency User Agreements .....	16
5.1.1.4	Interagency and Management Control Agreements .....	16
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum.....	16
5.1.1.6	Agency User Agreements .....	17
5.1.1.7	Outsourcing Standards for Channelers .....	17
5.1.1.8	Outsourcing Standards for Non-Channelers .....	18
5.1.2	Monitoring, Review, and Delivery of Services .....	18
5.1.2.1	Managing Changes to Service Providers .....	18
5.1.3	Secondary Dissemination.....	18
5.1.4	Secondary Dissemination of Non-CHRI CJI .....	18
5.1.5	References/Citations/Directives .....	19
5.2	Policy Area 2: Security Awareness Training.....	20
5.2.1	Awareness Topics .....	20
5.2.1.1	Level One Security Awareness Training .....	20
5.2.1.2	Level Two Security Awareness Training .....	20
5.2.1.3	Level Three Security Awareness Training .....	20
5.2.1.4	Level Four Security Awareness Training .....	21
5.2.2	Security Training Records.....	22
5.2.3	References/Citations/Directives .....	22
5.3	Policy Area 3: Incident Response .....	24
5.3.1	Reporting Security Events.....	24
5.3.1.1	Reporting Structure and Responsibilities.....	24
5.3.1.1.1	FBI CJIS Division Responsibilities .....	24
5.3.1.1.2	CSA ISO Responsibilities.....	24
5.3.2	Management of Security Incidents.....	25
5.3.2.1	Incident Handling.....	25
5.3.2.2	Collection of Evidence.....	25
5.3.3	Incident Response Training.....	25
5.3.4	Incident Monitoring.....	25
5.3.5	References/Citations/Directives .....	26
5.4	Policy Area 4: Auditing and Accountability.....	27
5.4.1	Auditable Events and Content (Information Systems).....	27
5.4.1.1	Events.....	27
5.4.1.1.1	Content.....	28
5.4.2	Response to Audit Processing Failures .....	28
5.4.3	Audit Monitoring, Analysis, and Reporting.....	28
5.4.4	Time Stamps.....	28
5.4.5	Protection of Audit Information .....	28



5.4.6	Audit Record Retention.....	28
5.4.7	Logging NCIC and III Transactions.....	29
5.4.8	References/Citations/Directives .....	29
5.5	Policy Area 5: Access Control.....	30
5.5.1	Account Management .....	30
5.5.2	Access Enforcement.....	30
5.5.2.1	Least Privilege .....	31
5.5.2.2	System Access Control .....	31
5.5.2.3	Access Control Criteria.....	31
5.5.2.4	Access Control Mechanisms.....	31
5.5.3	Unsuccessful Login Attempts .....	32
5.5.4	System Use Notification.....	32
5.5.5	Session Lock .....	32
5.5.6	Remote Access .....	33
5.5.6.1	Personally Owned Information Systems.....	33
5.5.6.2	Publicly Accessible Computers .....	34
5.5.7	References/Citations/Directives .....	34
5.6	Policy Area 6: Identification and Authentication .....	35
5.6.1	Identification Policy and Procedures.....	35
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges .....	35
5.6.2	Authentication Policy and Procedures .....	35
5.6.2.1	Standard Authenticators.....	36
5.6.2.1.1	Password .....	36
5.6.2.1.2	Personal Identification Number (PIN).....	36
5.6.2.2	Advanced Authentication.....	37
5.6.2.2.1	Advanced Authentication Policy and Rationale .....	37
5.6.2.2.2	Advanced Authentication Decision Tree .....	38
5.6.3	Identifier and Authenticator Management .....	39
5.6.3.1	Identifier Management.....	40
5.6.3.2	Authenticator Management.....	40
5.6.4	Assertions .....	40
5.6.5	References/Citations/Directives .....	40
5.7	Policy Area 7: Configuration Management .....	46
5.7.1	Access Restrictions for Changes .....	46
5.7.1.1	Least Functionality.....	46
5.7.1.2	Network Diagram.....	46
5.7.2	Security of Configuration Documentation .....	46
5.7.3	References/Citations/Directives .....	46
5.8	Policy Area 8: Media Protection.....	48
5.8.1	Media Storage and Access .....	48
5.8.2	Media Transport .....	48
5.8.2.1	Digital Media during Transport .....	48
5.8.2.2	Physical Media in Transit .....	48
5.8.3	Digital Media Sanitization and Disposal.....	48
5.8.4	Disposal of Physical Media.....	48

5.8.5	References/Citations/Directives .....	49
5.9	Policy Area 9: Physical Protection .....	50
5.9.1	Physically Secure Location .....	50
5.9.1.1	Security Perimeter.....	50
5.9.1.2	Physical Access Authorizations.....	50
5.9.1.3	Physical Access Control .....	50
5.9.1.4	Access Control for Transmission Medium .....	50
5.9.1.5	Access Control for Display Medium .....	50
5.9.1.6	Monitoring Physical Access .....	51
5.9.1.7	Visitor Control .....	51
5.9.1.8	Delivery and Removal .....	51
5.9.2	Controlled Area .....	51
5.9.3	References/Citations/Directives .....	51
5.10	Policy Area 10: System and Communications Protection and Information Integrity .....	52
5.10.1	Information Flow Enforcement .....	52
5.10.1.1	Boundary Protection .....	52
5.10.1.2	Encryption.....	53
5.10.1.3	Intrusion Detection Tools and Techniques .....	54
5.10.1.4	Voice over Internet Protocol.....	55
5.10.1.5	Cloud Computing.....	55
5.10.2	Facsimile Transmission of CJJ.....	55
5.10.3	Partitioning and Virtualization .....	55
5.10.3.1	Partitioning.....	56
5.10.3.2	Virtualization .....	56
5.10.4	System and Information Integrity Policy and Procedures.....	57
5.10.4.1	Patch Management.....	57
5.10.4.2	Malicious Code Protection.....	57
5.10.4.3	Spam and Spyware Protection .....	57
5.10.4.4	Security Alerts and Advisories .....	58
5.10.4.5	Information Input Restrictions.....	58
5.10.5	References/Citations/Directives .....	58
5.11	Policy Area 11: Formal Audits .....	60
5.11.1	Audits by the FBI CJIS Division.....	60
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division .....	60
5.11.1.2	Triennial Security Audits by the FBI CJIS Division .....	60
5.11.2	Audits by the CSA.....	60
5.11.3	Special Security Inquiries and Audits .....	61
5.11.4	References/Citations/Directives .....	61
5.12	Policy Area 12: Personnel Security .....	62
5.12.1	Personnel Security Policy and Procedures .....	62
5.12.1.1	Minimum Screening Requirements for Individuals Requiring Access to CJJ:.....	62
5.12.1.2	Personnel Screening for Contractors and Vendors .....	63
5.12.2	Personnel Termination .....	63
5.12.3	Personnel Transfer.....	64
5.12.4	Personnel Sanctions.....	64
5.12.5	References/Citations/Directives .....	64

5.13 Policy Area 13: Mobile Devices .....	65
5.13.1 Wireless Communications Technologies .....	65
5.13.1.1 802.11 Wireless Protocols .....	65
5.13.1.2 Cellular Devices .....	66
5.13.1.2.1 Cellular Service Abroad.....	67
5.13.1.2.2 Voice Transmissions Over Cellular Devices .....	67
5.13.1.3 Bluetooth.....	67
5.13.1.4 Mobile Hotspots.....	67
5.13.2 Mobile Device Management (MDM) .....	68
5.13.3 Wireless Device Risk Mitigations .....	68
5.13.4 System Integrity .....	69
5.13.4.1 Patching/Updates .....	69
5.13.4.2 Malicious Code Protection.....	69
5.13.4.3 Personal Firewall .....	69
5.13.5 Incident Response .....	70
5.13.6 Access Control .....	70
5.13.7 Identification and Authentication.....	70
5.13.7.1 Local Device Authentication .....	70
5.13.7.2 Advanced Authentication.....	70
5.13.7.2.1 Compensating Controls.....	71
5.13.7.3 Device Certificates.....	71
<b>Appendices.....</b>	<b>A-1</b>
<b>Appendix A Terms and Definitions .....</b>	<b>A-1</b>
<b>Appendix B Acronyms .....</b>	<b>B-1</b>
<b>Appendix C Network Topology Diagrams .....</b>	<b>C-1</b>
<b>Appendix D Sample Information Exchange Agreements .....</b>	<b>D-1</b>
D.1 CJIS User Agreement .....	D-1
D.2 Management Control Agreement.....	D-9
D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding.....	D-10
D.4 Interagency Connection Agreement .....	D-16
<b>Appendix E Security Forums and Organizational Entities.....</b>	<b>E-1</b>
<b>Appendix F Sample Forms.....</b>	<b>F-1</b>
F.1 Security Incident Response Form .....	F-2
<b>Appendix G Best practices .....</b>	<b>G-1</b>
G.1 Virtualization .....	G-1
G.2 Voice over Internet Protocol .....	G-4
G.3 Cloud Computing.....	G-15
G.4 Mobile Appendix .....	G-30
G.5 Administrator Accounts for Least Privilege and Separation of Duties.....	G-51
<b>Appendix H Security Addendum .....</b>	<b>H-1</b>
<b>Appendix I References .....</b>	<b>I-1</b>
<b>Appendix J Noncriminal Justice Agency Supplemental Guidance .....</b>	<b>J-1</b>
<b>Appendix K Criminal Justice Agency Supplemental Guidance .....</b>	<b>K-1</b>

## LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components .....	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department .....	19
Figure 4 – Security Awareness Training Use Cases .....	22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department .....	26
Figure 6 – Local Police Department's Use of Audit Logs .....	29
Figure 7 – A Local Police Department's Access Controls .....	34
Figure 8 – Advanced Authentication Use Cases.....	40
Figure 9 – Authentication Decision for Known Location .....	44
Figure 10 – Authentication Decision for Unknown Location .....	45
Figure 11 – A Local Police Department's Configuration Management Controls .....	47
Figure 12 – A Local Police Department's Media Management Policies.....	49
Figure 13 – A Local Police Department's Physical Protection Measures.....	51
Figure 14 – System and Communications Protection and Information Integrity Use Cases.....	58
Figure 15 – The Audit of a Local Police Department.....	61
Figure 16 – A Local Police Department's Personnel Security Controls .....	64

# 1 INTRODUCTION

---

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

## 1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

## 1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

## 1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies

and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

## **1.4 Terminology Used in This Document**

The following terms are used interchangeably throughout this document:

- **Agency and Organization:** The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- **Information and Data:** Both terms refer to CJI.
- **System, Information System, Service, or named applications like NCIC:** all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.

Appendix A and B provide an extensive list of the terms and acronyms.

## **1.5 Distribution of the CJIS Security Policy**

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

## **2 CJIS SECURITY POLICY APPROACH**

---

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

### **2.1 CJIS Security Policy Vision Statement**

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

### **2.2 Architecture Independent**

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Integrated Automated Fingerprint Identification System (IAFIS) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

### **2.3 Risk Versus Realism**

Every “shall” statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

## 3 ROLES AND RESPONSIBILITIES

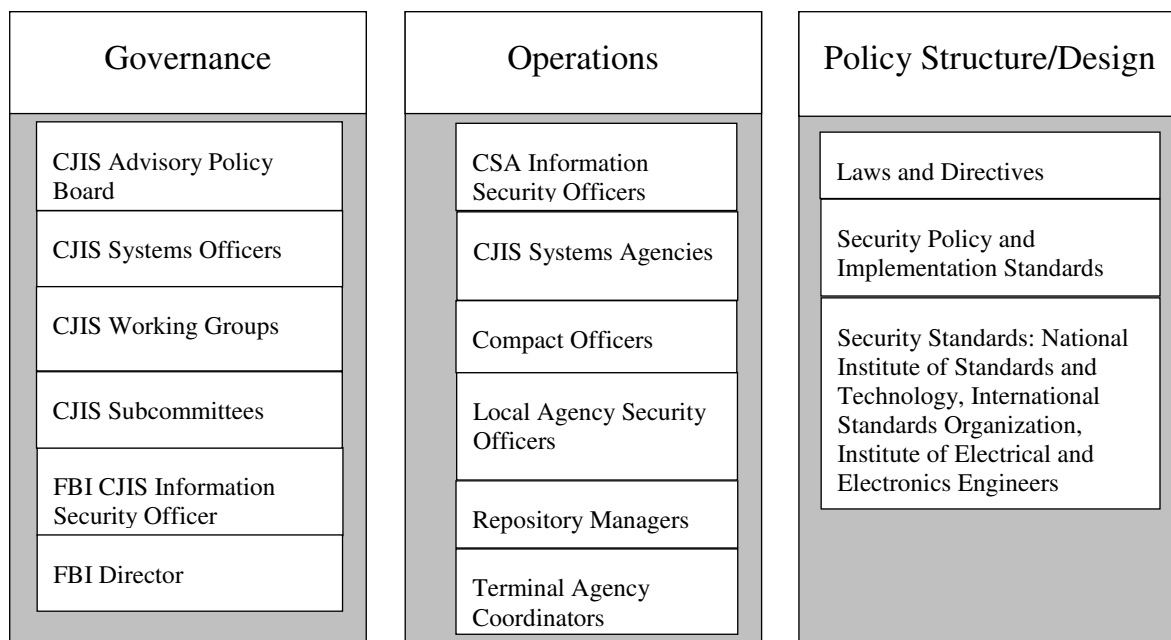
### 3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

### 3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.



**Figure 1 – Overview Diagram of Strategic Functions and Policy Components**



This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

### **3.2.1 CJIS Systems Agencies (CSA)**

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

### **3.2.2 CJIS Systems Officer (CSO)**

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
  - a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
  - b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

- c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
  - d. The CSO, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.
  - e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
  - f. Approve access to FBI CJIS systems.
  - g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
  - h. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
3. Outsourcing of Criminal Justice Functions
- a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
  - b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

### **3.2.3 Terminal Agency Coordinator (TAC)**

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

### **3.2.4 Criminal Justice Agency (CJA)**

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

### **3.2.5 Noncriminal Justice Agency (NCJA)**

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

### **3.2.6 Contracting Government Agency (CGA)**

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

### **3.2.7 Agency Coordinator (AC)**

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

### **3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)**

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

### **3.2.9 Local Agency Security Officer (LASO)**

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

### **3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)**

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

### **3.2.11 Repository Manager**

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

### **3.2.12 Compact Officer**

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

## **4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION**

---

### **4.1 Criminal Justice Information (CJI)**

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. **Biometric Data**—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. **Identity History Data**—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
3. **Biographic Data**—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. **Property Data**—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. **Case/Incident History**—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules.

#### **4.1.1 Criminal History Record Information (CHRI)**

Criminal History Record Information (CHRI), sometimes informally referred to as “restricted data”, is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

## **4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information**

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

### **4.2.1 Proper Access, Use, and Dissemination of CHRI**

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

### **4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information**

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

### **4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information**

#### **4.2.3.1 For Official Purposes**

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

#### **4.2.3.2 For Other Authorized Purposes**

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

#### **4.2.3.3 CSO Authority in Other Circumstances**

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

#### **4.2.4 Storage**

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

#### **4.2.5 Justification and Penalties**

##### **4.2.5.1 Justification**

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

##### **4.2.5.2 Penalties**

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

### **4.3 Personally Identifiable Information (PII)**

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for



example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

**Figure 2 – Dissemination of restricted and non-restricted NCIC data**

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

## 5 POLICY AND IMPLEMENTATION

---

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices

## **5.1 Policy Area 1: Information Exchange Agreements**

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

### **5.1.1 Information Exchange**

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

#### **5.1.1.1 Information Handling**

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to – employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

#### **5.1.1.2 State and Federal Agency User Agreements**

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

#### **5.1.1.3 Criminal Justice Agency User Agreements**

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

#### **5.1.1.4 Interagency and Management Control Agreements**

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or inter-agency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an inter-agency agreement. An example of an NCJA (government) is a city information technology (IT) department.

#### **5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum**

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors

who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

#### **5.1.1.6 Agency User Agreements**

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.

#### **5.1.1.7 Outsourcing Standards for Channelers**

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

#### **5.1.1.8 Outsourcing Standards for Non-Channelers**

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

### **5.1.2 Monitoring, Review, and Delivery of Services**

As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

#### **5.1.2.1 Managing Changes to Service Providers**

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

### **5.1.3 Secondary Dissemination**

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

#### **5.1.4 Secondary Dissemination of Non-CHRI CJI**

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

### **5.1.5 References/Citations/Directives**

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

#### **Figure 3 – Information Exchange Agreements Implemented by a Local Police Department**

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

## **5.2 Policy Area 2: Security Awareness Training**

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

### **5.2.1 Awareness Topics**

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

#### **5.2.1.1 Level One Security Awareness Training**

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

#### **5.2.1.2 Level Two Security Awareness Training**

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

#### **5.2.1.3 Level Three Security Awareness Training**

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.



2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating “shoulder surfing”), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

#### **5.2.1.4 Level Four Security Awareness Training**

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.
3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

## 5.2.2 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

## 5.2.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

### Figure 4 – Security Awareness Training Use Cases

#### ***Use Case 1 - Security Awareness Training Program Implementation by a Local Police Department***

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

#### ***Use Case 2 - Level One Security Awareness Training***

***A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.***

#### ***Use Case 3 – Level Two Security Awareness Training***

***A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1 and 5.2.1.2.***

#### ***Use Case 4 – Level Three Security Awareness Training***

***A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.***

#### ***Use Case 5 – Level Four Security Awareness Training***

***The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing***

*systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems, and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, 5.2.1.3, and 5.2.1.4.*

## **5.3 Policy Area 3: Incident Response**

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

### **5.3.1 Reporting Security Events**

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

#### **5.3.1.1 Reporting Structure and Responsibilities**

##### **5.3.1.1.1 FBI CJIS Division Responsibilities**

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

##### **5.3.1.1.2 CSA ISO Responsibilities**

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

### **5.3.2 Management of Security Incidents**

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

#### **5.3.2.1 Incident Handling**

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

#### **5.3.2.2 Collection of Evidence**

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

### **5.3.3 Incident Response Training**

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

#### **5.3.4 Incident Monitoring**

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

### 5.3.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

#### **Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department**

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

## **5.4 Policy Area 4: Auditing and Accountability**

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJI.

### **5.4.1 Auditable Events and Content (Information Systems)**

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

#### **5.4.1.1 Events**

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
  - a. access permission on a user account, file, directory or other system resource;
  - b. create permission on a user account, file, directory or other system resource;
  - c. write permission on a user account, file, directory or other system resource;
  - d. delete permission on a user account, file, directory or other system resource;
  - e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
  - a. access the audit log file;
  - b. modify the audit log file;

- c. destroy the audit log file.

#### **5.4.1.1.1 Content**

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

#### **5.4.2 Response to Audit Processing Failures**

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

#### **5.4.3 Audit Monitoring, Analysis, and Reporting**

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

#### **5.4.4 Time Stamps**

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

#### **5.4.5 Protection of Audit Information**

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

#### **5.4.6 Audit Record Retention**

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.



#### **5.4.7 Logging NCIC and III Transactions**

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

#### **5.4.8 References/Citations/Directives**

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

#### **Figure 6 – Local Police Department's Use of Audit Logs**

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

## **5.5 Policy Area 5: Access Control**

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.7 for additional access control requirements related to mobile devices used to access CJI.

### **5.5.1 Account Management**

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

### **5.5.2 Access Enforcement**

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

#### **5.5.2.1 Least Privilege**

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

#### **5.5.2.2 System Access Control**

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

#### **5.5.2.3 Access Control Criteria**

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

#### **5.5.2.4 Access Control Mechanisms**

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

### **5.5.3 Unsuccessful Login Attempts**

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

### **5.5.4 System Use Notification**

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

- (i) the system use information is available and when appropriate, is displayed before granting access;
- (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
- (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

### **5.5.5 Session Lock**

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user

reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

### **5.5.6 Remote Access**

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

#### **5.5.6.1 Personally Owned Information Systems**

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

#### **5.5.6.2 Publicly Accessible Computers**

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

#### **5.5.7 References/Citations/Directives**

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

#### **Figure 7 – A Local Police Department’s Access Controls**

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA’s CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client’s executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

## **5.6 Policy Area 6: Identification and Authentication**

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

### **5.6.1 Identification Policy and Procedures**

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

#### **5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges**

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

### **5.6.2 Authentication Policy and Procedures**

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not

further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

### **5.6.2.1 Standard Authenticators**

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, tokens, biometrics, and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

#### **5.6.2.1.1 Password**

Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

#### **5.6.2.1.2 Personal Identification Number (PIN)**

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
  - a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.



**EXCEPTION:** When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

### **5.6.2.2 Advanced Authentication**

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to “activate” that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

#### **5.6.2.2.1 Advanced Authentication Policy and Rationale**

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

**EXCEPTION:**

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. **EXAMPLES:**

- a. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.

- b. A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

#### **5.6.2.2.2 Advanced Authentication Decision Tree**

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Can request's physical originating location be determined?

If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 2.

- a. The IP address is attributed to a physical structure; or
- b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is "no". Skip to question number 4.

2. Does request originate from within a physically secure location as described in Section 5.9.1?

If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 3.

- a. The IP address is attributed to a physically secure location; or
- b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

3. Are all required technical controls implemented at this location or at the controlling agency?

If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA requirement waived.

- a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or
- b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.

4. Does request originate from an agency-controlled user device?

If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 5.

- a. The static IP address or MAC address can be traced to registered device; or
- b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

5. Is the agency managed user device associated with and located within a criminal justice conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to Figure 9 Step 3.

- a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or
- b. The certificate presented is associated with a device associated with a criminal justice conveyance; or
- c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is “no”. Skip to question number 7.

6. Is the user device an agency-issued and controlled smartphone or tablet?

If both (a) and (b) below are true, the answer to the above question is “yes.” Proceed to question number 7.

- a. The law enforcement agency issued the device to an individual; and
- b. The device is subject to administrative management control of the issuing agency.

If either (a) or (b) above is false, then the answer is “no.” Decision tree completed. AA required.

7. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented?

If (a) and (b) below are true, the answer to the above question is “yes.” Decision tree completed. AA requirement is waived.

- a. An agency cannot meet a requirement due to legitimate technical or business constraints; and
- b. The CSO has given written approval permitting AA compensating controls to be implemented in lieu of the required AA control measures.

If either (a) or (b) above is false then the answer is “no.” Decision tree completed. AA required.

### **5.6.3 Identifier and Authenticator Management**

The agency shall establish identifier and authenticator management processes.

### **5.6.3.1 Identifier Management**

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.
5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

### **5.6.3.2 Authenticator Management**

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

### **5.6.4 Assertions**

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

### **5.6.5 References/Citations/Directives**

Appendix C contains all of the references used in this Policy and may contain additional sources that apply to this section.

## **Figure 8 – Advanced Authentication Use Cases**

#### Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password (“something you know”), and a one-time password OTP (“something you have”) from a hardware token to satisfy the requirement for advanced authentication. Once the detective’s credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

#### Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to Criminal Justice Information (CJI) then enters the proper username (identification) and password (“something you know”). Once prompted, the user connects the smart card (“something you have”) to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

#### Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user’s agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP (“something you have”) then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

#### Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a one-time password (OTP) is sent to the user’s agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This

method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user's identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

#### Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password ("something you know"). The RBA detects this computer has not previously been used by the user, is not listed under the user's profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. The CJIS Security Policy requirements for RBA have been satisfied.

#### Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password ("something you know"). The RBA detects this computer has not previously been used by the user and is not listed under the user's profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user's profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. Using this collected data, the RBA presents challenge/response questions when changes to the user's profile are noted versus every time the user logs in.

### Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user's job functions.

An audit by the CSA identifies the agency's use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

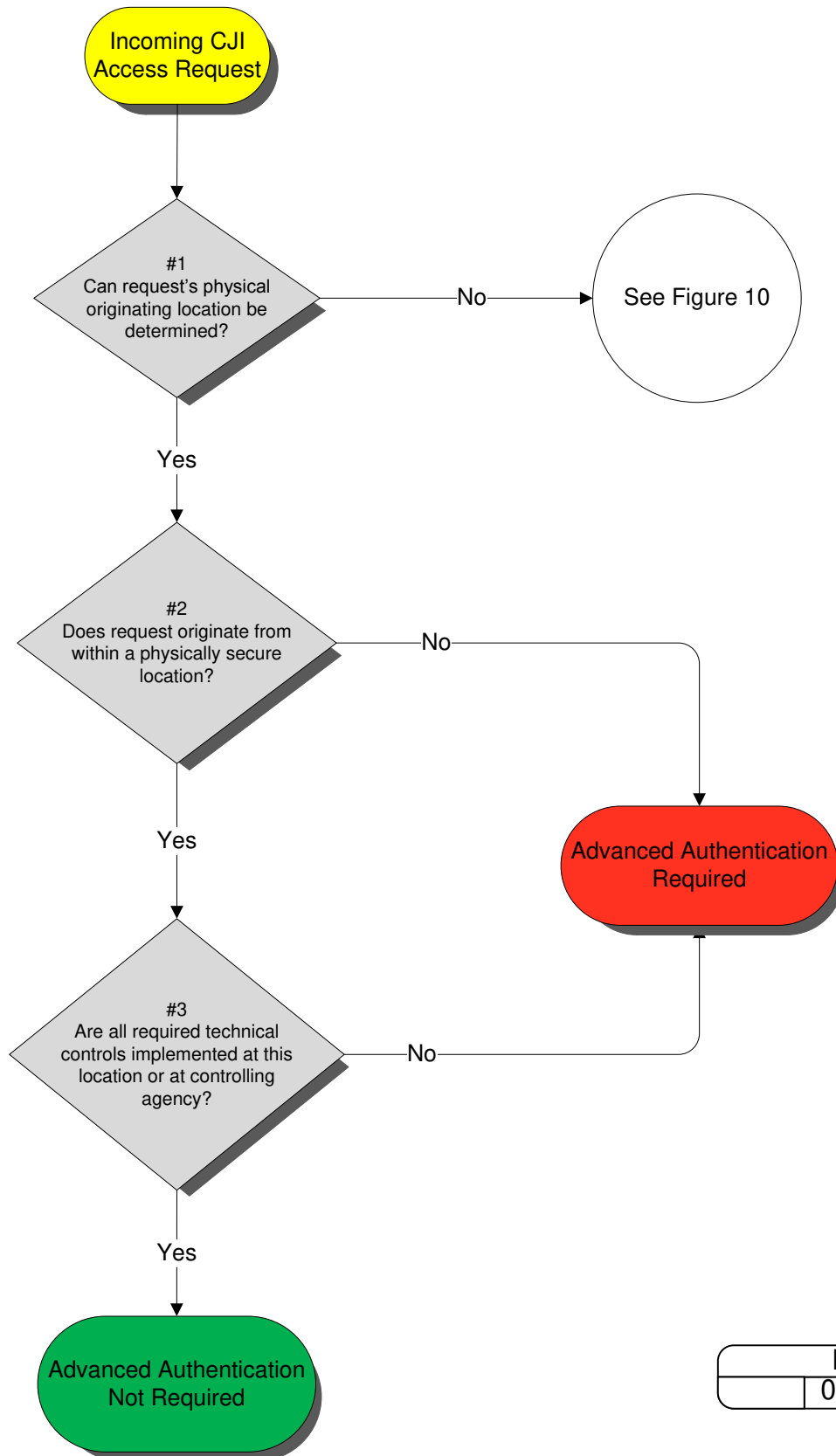
Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device
2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

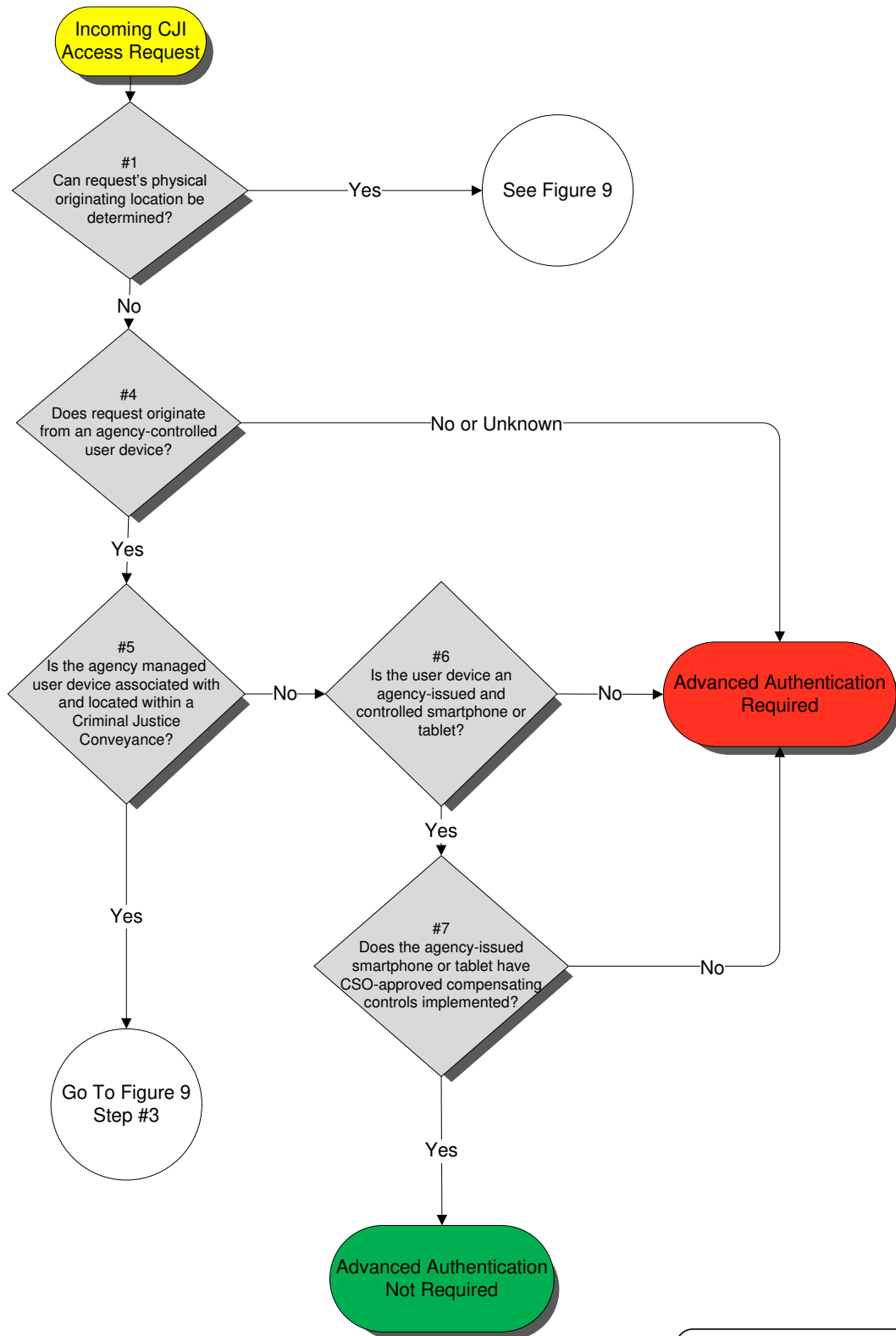
**Figure 9 – Authentication Decision for Known Location**



<b>Figure 9</b>		
	08/04/2014	



**Figure 10 – Authentication Decision for Unknown Location**



**Figure 10**

10/06/2015

## **5.7 Policy Area 7: Configuration Management**

### **5.7.1 Access Restrictions for Changes**

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

#### **5.7.1.1 Least Functionality**

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

#### **5.7.1.2 Network Diagram**

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

### **5.7.2 Security of Configuration Documentation**

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

### **5.7.3 References/Citations/Directives**

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

### **Figure 11 – A Local Police Department’s Configuration Management Controls**

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

## **5.8 Policy Area 8: Media Protection**

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

### **5.8.1 Media Storage and Access**

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

### **5.8.2 Media Transport**

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

#### **5.8.2.1 Digital Media during Transport**

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

#### **5.8.2.2 Physical Media in Transit**

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

### **5.8.3 Digital Media Sanitization and Disposal**

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

### **5.8.4 Disposal of Physical Media**

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

### 5.8.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

#### Figure 12 – A Local Police Department’s Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor’s vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentiality of the police department’s data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor’s vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

## **5.9 Policy Area 9: Physical Protection**

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

### **5.9.1 Physically Secure Location**

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

#### **5.9.1.1 Security Perimeter**

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

#### **5.9.1.2 Physical Access Authorizations**

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

#### **5.9.1.3 Physical Access Control**

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

#### **5.9.1.4 Access Control for Transmission Medium**

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

#### **5.9.1.5 Access Control for Display Medium**

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

#### **5.9.1.6 Monitoring Physical Access**

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

#### **5.9.1.7 Visitor Control**

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

#### **5.9.1.8 Delivery and Removal**

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

### **5.9.2 Controlled Area**

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

### **5.9.3 References/Citations/Directives**

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

#### **Figure 13 – A Local Police Department's Physical Protection Measures**

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state's CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by criminal justice professionals. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems' infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

## **5.10 Policy Area 10: System and Communications Protection and Information Integrity**

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

### **5.10.1 Information Flow Enforcement**

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

#### **5.10.1.1 Boundary Protection**

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open").



6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

#### **5.10.1.2 Encryption**

Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

1. Encryption shall be a minimum of 128 bit.
2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

##### **EXCEPTIONS:**

- a) See Sections 5.13.1.2.2 and 5.10.2.
- b) Encryption shall not be required if the transmission medium meets all of the following requirements:
  - i. The agency owns, operates, manages, or protects the medium.
  - ii. Medium terminates within physically secure locations at both ends with no interconnections between.
  - iii. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
  - iv. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
  - v. With prior approval of the CSO.

##### **Examples:**

- A campus is completely owned and controlled by a criminal justice agency (CJA) – If line-of-sight between buildings exists where a cable is buried, encryption is not required.
  - A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
  - A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.
3. When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).

- a) When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
    - i. Be at least 10 characters
    - ii. Not be a dictionary word.
    - iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
    - iv. Be changed when previously authorized personnel no longer require access.
  - b) Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.
4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation.

EXCEPTION: When encryption is used for CJI at rest, agencies may use encryption methods that are FIPS 197 certified, 256 bit as described on the National Security Agency (NSA) Suite B Cryptography list of approved algorithms.

5. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:
- a) Include authorization by a supervisor or a responsible official.
  - b) Be accomplished by a secure process that verifies the identity of the certificate holder.
  - c) Ensure the certificate is issued to the intended party.

### **5.10.1.3 Intrusion Detection Tools and Techniques**

The agency shall implement network-based and/or host-based intrusion detection tools.

The CSA/SIB shall, in addition:

- 1. Monitor inbound and outbound communications for unusual or unauthorized activities.
- 2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
- 3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

#### **5.10.1.4 Voice over Internet Protocol**

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

#### **5.10.1.5 Cloud Computing**

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

#### **5.10.2 Facsimile Transmission of CJI**

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

#### **5.10.3 Partitioning and Virtualization**

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

### **5.10.3.1 Partitioning**

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.
2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

### **5.10.3.2 Virtualization**

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

## **5.10.4 System and Information Integrity Policy and Procedures**

### **5.10.4.1 Patch Management**

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

### **5.10.4.2 Malicious Code Protection**

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

### **5.10.4.3 Spam and Spyware Protection**

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

#### **5.10.4.4 Security Alerts and Advisories**

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.
5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

#### **5.10.4.5 Information Input Restrictions**

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

#### **5.10.5 References/Citations/Directives**

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

### **Figure 14 – System and Communications Protection and Information Integrity Use Cases**

#### **A Local Police Department's Information Systems & Communications Protections**

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state's CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

#### Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

#### Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

## **5.11 Policy Area 11: Formal Audits**

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

### **5.11.1 Audits by the FBI CJIS Division**

#### **5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division**

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

#### **5.11.1.2 Triennial Security Audits by the FBI CJIS Division**

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

### **5.11.2 Audits by the CSA**

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.



### **5.11.3 Special Security Inquiries and Audits**

All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

### **5.11.4 References/Citations/Directives**

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

### **Figure 15 – The Audit of a Local Police Department**

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

## **5.12 Policy Area 12: Personnel Security**

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

### **5.12.1 Personnel Security Policy and Procedures**

#### **5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:**

1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
  - (i) 5 CFR 731.106; and/or
  - (ii) Office of Personnel Management policy, regulations, and guidance; and/or
  - (iii) agency policy, regulations, and guidance.

(See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.) Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.
2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
4. If a record of any other kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
5. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
6. If the person is employed by a NCJA, the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.
7. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant

hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.

8. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

#### **5.12.1.2 Personnel Screening for Contractors and Vendors**

In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:

1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.
2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer.
3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.
4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.
5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.

Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CSO to review a denial of access determination.

#### **5.12.2 Personnel Termination**

The agency, upon termination of individual employment, shall immediately terminate access to CJI.

### **5.12.3 Personnel Transfer**

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

### **5.12.4 Personnel Sanctions**

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

### **5.12.5 References/Citations/Directives**

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

### **Figure 16 – A Local Police Department's Personnel Security Controls**

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated policies. The police department re-evaluated each person's suitability for access to CJI every five years.

## **5.13 Policy Area 13: Mobile Devices**

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

### **5.13.1 Wireless Communications Technologies**

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

#### **5.13.1.1 802.11 Wireless Protocols**

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-80.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

### **5.13.1.2 Cellular Devices**

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

#### **5.13.1.2.1 Cellular Service Abroad**

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency’s policies prior to and after deployment outside of the U.S.

#### **5.13.1.2.2 Voice Transmissions Over Cellular Devices**

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

#### **5.13.1.3 Bluetooth**

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency’s operational and business processes.

#### **5.13.1.4 Mobile Hotspots**

Many mobile devices include the capability to function as a WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot’s default SSID
  - a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot’s port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

### **5.13.2 Mobile Device Management (MDM)**

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full featured operating systems may not function properly on devices with limited feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. Agencies shall implement the following controls when allowing CJI access from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the:
  - i. Remote locking of device
  - ii. Remote wiping of device
  - iii. Setting and locking device configuration
  - iv. Detection of “rooted” and “jailbroken” devices
  - v. Enforcement of folder or disk level encryption
  - vi. Application of mandatory policy settings on the device
  - vii. Detection of unauthorized configurations
  - viii. Detection of unauthorized software or applications
  - ix. Ability to determine the location of agency controlled devices
  - x. Prevention of unpatched devices from accessing CJI or CJI systems
  - xi. Automatic device wiping after a specified number of failed access attempts

### **5.13.3 Wireless Device Risk Mitigations**

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.
2. Are configured for local device authentication (see Section 5.13.7.1).
3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
4. Encrypt all CJI resident on the device.



5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

#### **5.13.4 System Integrity**

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM, application, or supporting service infrastructure.

##### **5.13.4.1 Patching/Updates**

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

##### **5.13.4.2 Malicious Code Protection**

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

##### **5.13.4.3 Personal Firewall**

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.
2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

### **5.13.5 Incident Response**

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
  - a. Device known to be locked, minimal duration of loss
  - b. Device lock state unknown, minimal duration of loss
  - c. Device lock state unknown, extended duration of loss
  - d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

### **5.13.6 Access Control**

Multiple user accounts are not generally supported on limited feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

### **5.13.7 Identification and Authentication**

Due to the technical methods used for identification and authentication on many limited feature mobile operating systems, achieving compliance may require many different components.

#### **5.13.7.1 Local Device Authentication**

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

#### **5.13.7.2 Advanced Authentication**

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user.

#### **5.13.7.2.1 Compensating Controls**

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The proposed compensating controls for AA are a combination of controls that provide acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

At least two of the following examples of AA compensating controls for agency-issued smartphones and tablets with limited feature operating systems shall be implemented to qualify for compensating control consideration:

- Possession of the agency issued smartphone or tablet as an indication it is the authorized user
- Implemented password protection on the Mobile Device Management application and/or secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after predetermined number of failed authentication attempts
- Remote device location (GPS) tracking
- Require CJIS Security Policy compliant password to access the device
- Use of device certificates as per Section 5.13.7.3 Device Certificates

#### **5.13.7.3 Device Certificates**

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

# APPENDICES

## APPENDIX A TERMS AND DEFINITIONS

---

**Access to Criminal Justice Information** — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

**Administration of Criminal Justice** — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

**Agency Controlled Mobile Device** — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

**Agency Coordinator (AC)** — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

**Agency Issued Mobile Device** — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).

**Agency Liaison (AL)** — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

**Authorized User/Personnel** — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

**Authorized Recipient** — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

**Availability** — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

**Biographic Data** — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

**Biometric Data** — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

**Case / Incident History** — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

**Certificate Authority (CA) Certificate** – Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

**Channeler** — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

**Cloud Client** – A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

**Cloud Computing** – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

**Cloud Provider** – An organization that provides cloud computing services.

**Cloud Subscriber** – A person or organization that is a customer of a cloud computing service provider.

**CJIS Advisory Policy Board (APB)** — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

**CJIS Audit Unit (CAU)** — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

**CJIS Security Policy** — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

**CJIS Systems Agency (CSA)** — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

**CJIS Systems Agency Information Security Officer (CSA ISO)** — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

**CJIS Systems Officer (CSO)** — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

**Compact Council** — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

**Compact Officers** — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

**Compensating Controls** — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

**Computer Security Incident Response Capability (CSIRC)** — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

**Confidentiality** — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

**Contractor** — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

**Contracting Government Agency (CGA)** — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

**Crime Reports Data** — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

**Criminal History Record Information (CHRI)** — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

**Criminal Justice Agency (CJA)** — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

**Criminal Justice Agency User Agreement** — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

**Criminal Justice Conveyance** — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

**Criminal Justice Information (CJI)** — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

**Criminal Justice Information Services Division (FBI CJIS or CJIS)** — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

**Data** — See Information and CJI.

**Degauss** — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

**Department of Justice (DoJ)** — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

**Digital Media** – Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

**Digital Signature** – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

**Direct Access** — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

**Dissemination** — The transmission/distribution of CJI to Authorized Recipients within an agency.

**Escort** – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

**Facsimile (Fax)** – Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

**Federal Bureau of Investigation (FBI)** — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

**FBI CJIS Information Security Officer (FBI CJIS ISO)** — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

**Federal Information Security Management Act (FISMA)** — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

**For Official Use Only (FOUO)** — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.



**Full-feature Operating System** — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g. Microsoft Windows, Apple OS X, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or “harden”, these devices from malicious network based technical attacks (e.g. malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

**Guest Operating System** — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

**Host Operating System** — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

**Hypervisor** — See Host Operating System.

**Identity History Data** — Textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

**In-Band** – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

**Indirect Access** – Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

**Information** — See data and CJI.

**Information Exchange Agreement** — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party’s information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

**Information Security Officer (ISO)** — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

**Information System** — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

**Integrated Automated Fingerprint Identification System (IAFIS)** — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

**Integrity** — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

**Interconnection Security Agreement (ISA)** — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

**Interface Agency** — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

**Internet Protocol (IP)** — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

**Interstate Identification Index (III)** — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

**Jailbreak (Jailbroken)** — The process of attaining privileged control (known as “root access”) of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

**Laptop Devices** – Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OS X, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited feature operating system (e.g. tablets).

**Law Enforcement Enterprise Portal (LEEP)** — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

**Limited-feature Operating System** — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows RT/Phone, Blackberry OS, etc.). These operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

**Logical Access** – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

**Logical Partitioning** – When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

**Local Agency Security Officer (LASO)** — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

**Management Control Agreement (MCA)** — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA's authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

**Mobile Device** — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

**Mobile Device Management (MDM)** — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

**Mobile (WiFi) Hotspot** — A mobile (WiFi) hotspot is a zone or area associated with a mobile device (e.g. smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

**National Crime Information Center (NCIC)** — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

**National Instant Criminal Background Check System (NICS)** — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

**National Institute of Standards and Technology (NIST)** — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

**Noncriminal Justice Agency (NCJA)** — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

**NCJA (Government)** — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

**NCJA (Private)** — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.

**NCJA (Public)** — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

**Noncriminal Justice Purpose** — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

**Office of Management and Budget (OMB)** — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

**Out-of-Band** — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

**Outsourcing** — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

**Outsourcing Standard** — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

**Partitioning** – Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

**Personal Firewall** — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

**Personally Identifiable Information (PII)** — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

**Physical Access** – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

**Physical Media** – Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

**Physical Partitioning** – When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

**Physically Secure Location** — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

**Pocket/Handheld Mobile Device** – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

**Property Data** — Information about vehicles and property associated with a crime.

**Rap Back** — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

**Receive-Only Terminal (ROT)** – A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

**Repository Manager, or Chief Administrator** — The designated manager of the agency having oversight responsibility for a CSA’s fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

**Root (Rooting, Rooted)** — The process of attaining privileged control (known as “root access”) of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

**Secondary Dissemination** — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

**Security Addendum (SA)** — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

**Sensitive But Unclassified (SBU)** — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others,

including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

**Server/Client Computer Certificate (device-based)** – Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

**Service** — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

**Shredder** — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

**Smartphone** – See pocket/handheld mobile devices.

**Social Engineering** — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

**Software Patch** — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

**State and Federal Agency User Agreement** — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

**State Compact Officer** — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

**State Identification Bureau (SIB)** — The state agency with the responsibility for the state's fingerprint identification services.

**State Identification Bureau (SIB) Chief** — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

**State of Residency** – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

**System** — Refer to connections to the FBI’s criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to applications and all interconnecting infrastructure required to use those applications that process CJI.

**Tablet Devices** – Tablet devices are mobile devices with a limited feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

**Terminal Agency Coordinator (TAC)** — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency’s compliance with CJIS systems policies.

**Wireless Access Point** – A wireless access point is a device that logically connects a wireless client device to an organization’s enterprise network which processes unencrypted CJI.

**Wireless (WiFi) Hotspot** – A wireless (WiFi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

**User Certificate (user-based)** – Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

**Virtual Escort** – Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

**Virtual Machine (VM)** – See Guest Operating System

**Virtualization** — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

**Voice over Internet Protocol (VoIP)** — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

## APPENDIX B ACRONYMS

---

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice



DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle
MOU	Memorandum of Understanding
NCIC	National Crime Information Center

NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau
SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
VLAN	Virtual Local Area Network

VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

## APPENDIX C NETWORK TOPOLOGY DIAGRAMS

---

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJJ, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

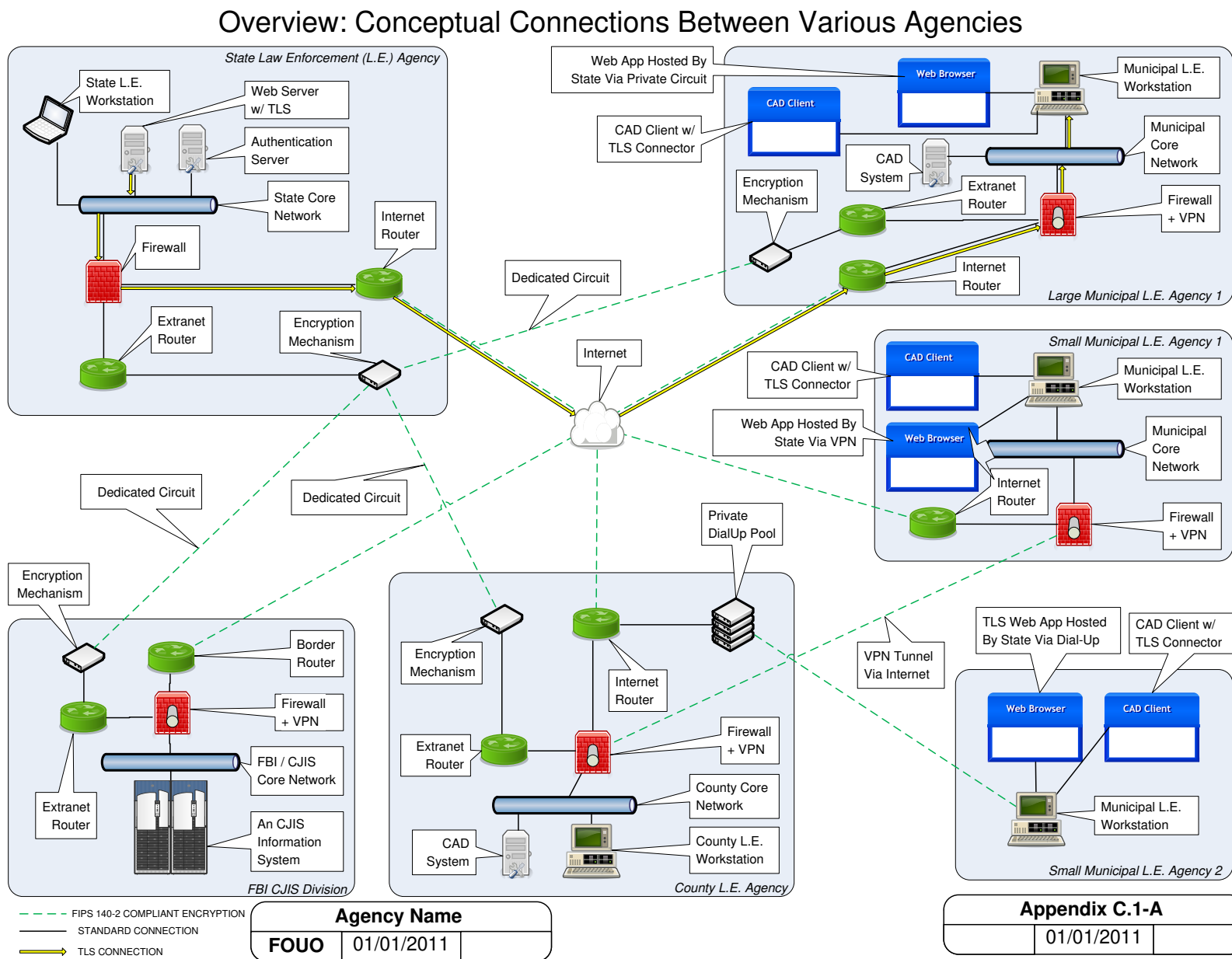
Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies



**Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency**

## Conceptual Topology Diagram For A State Law Enforcement Agency

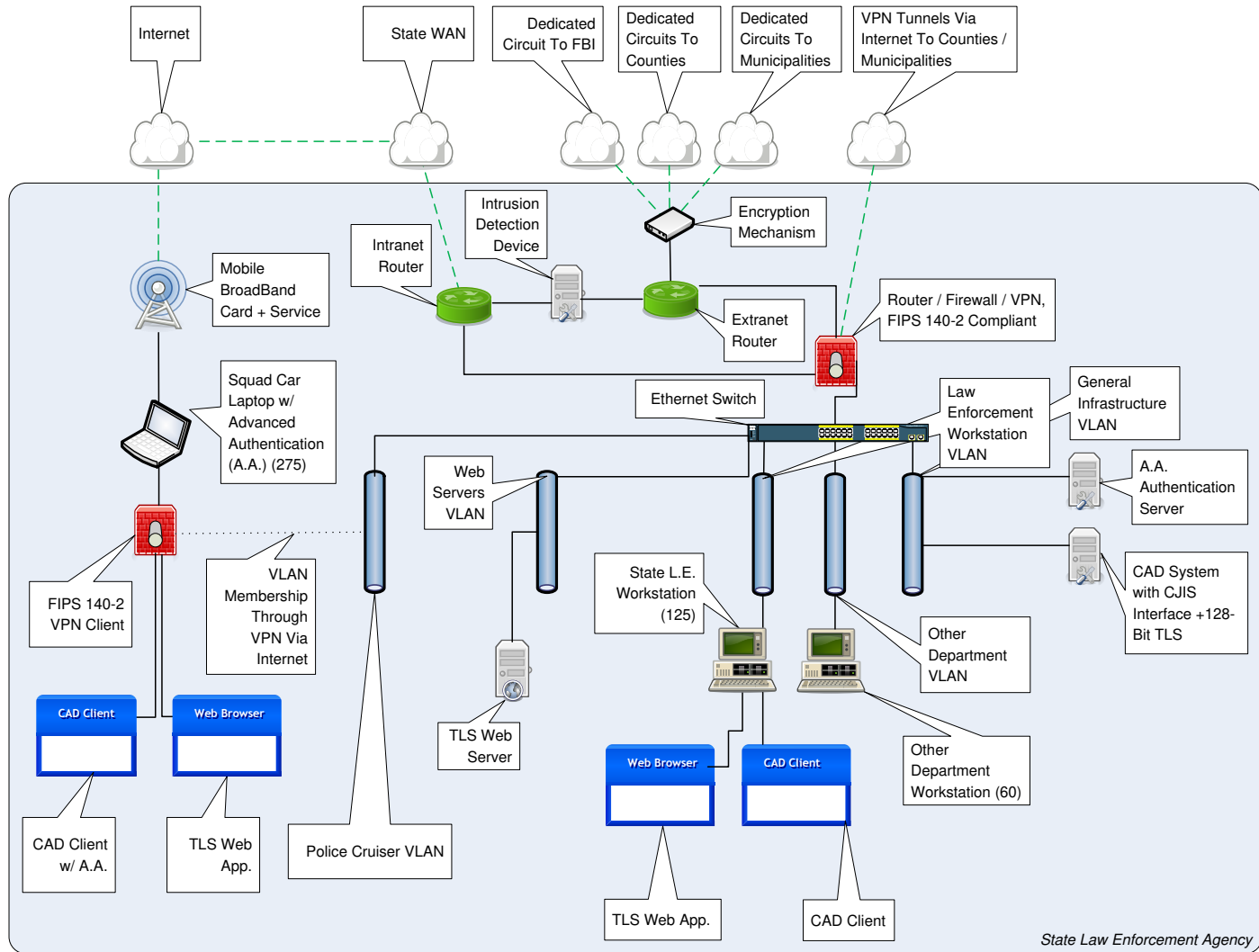
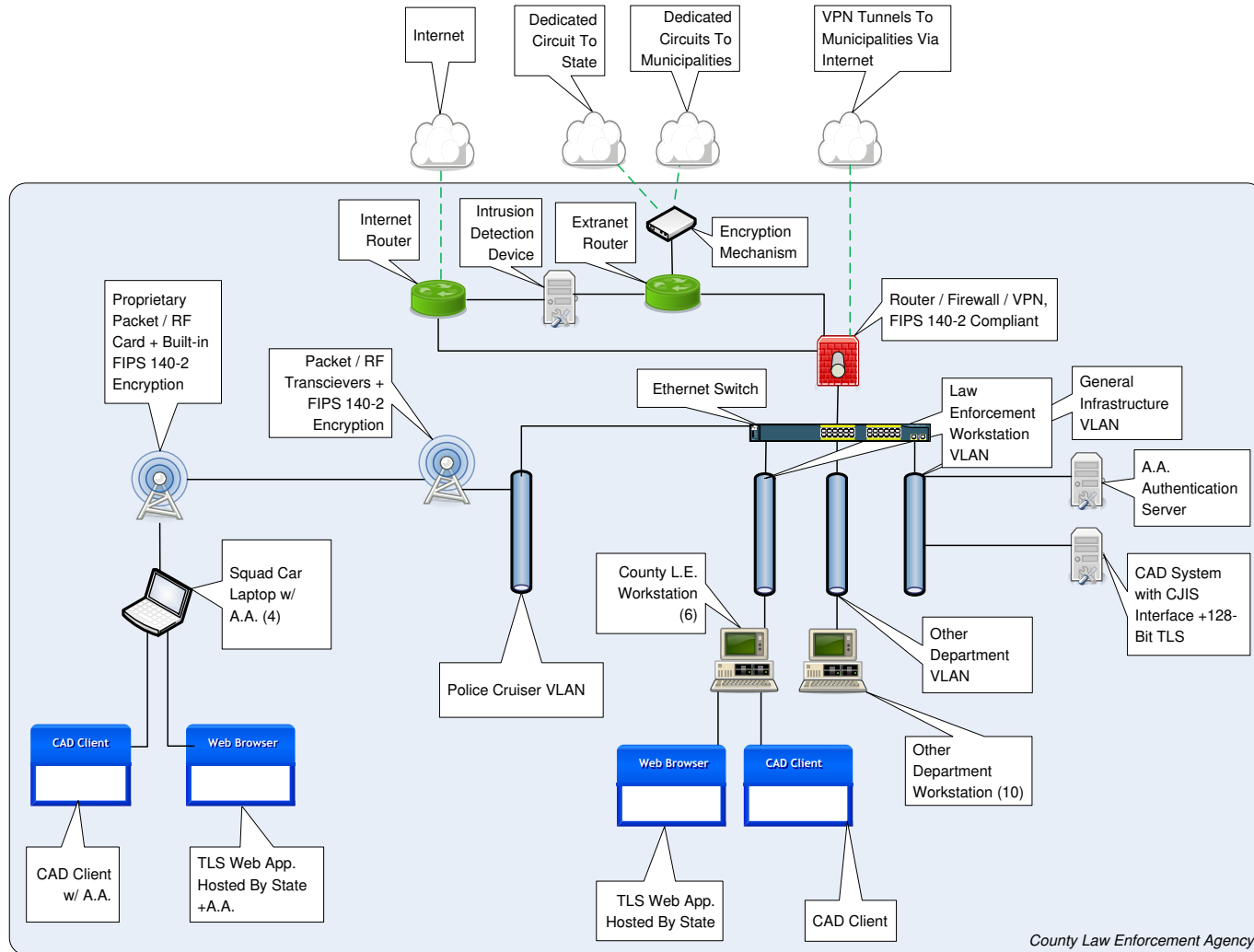


Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

## Conceptual Topology Diagram For A County Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION  
— STANDARD CONNECTION

### Sample County Agency

FOUO

01/01/2011

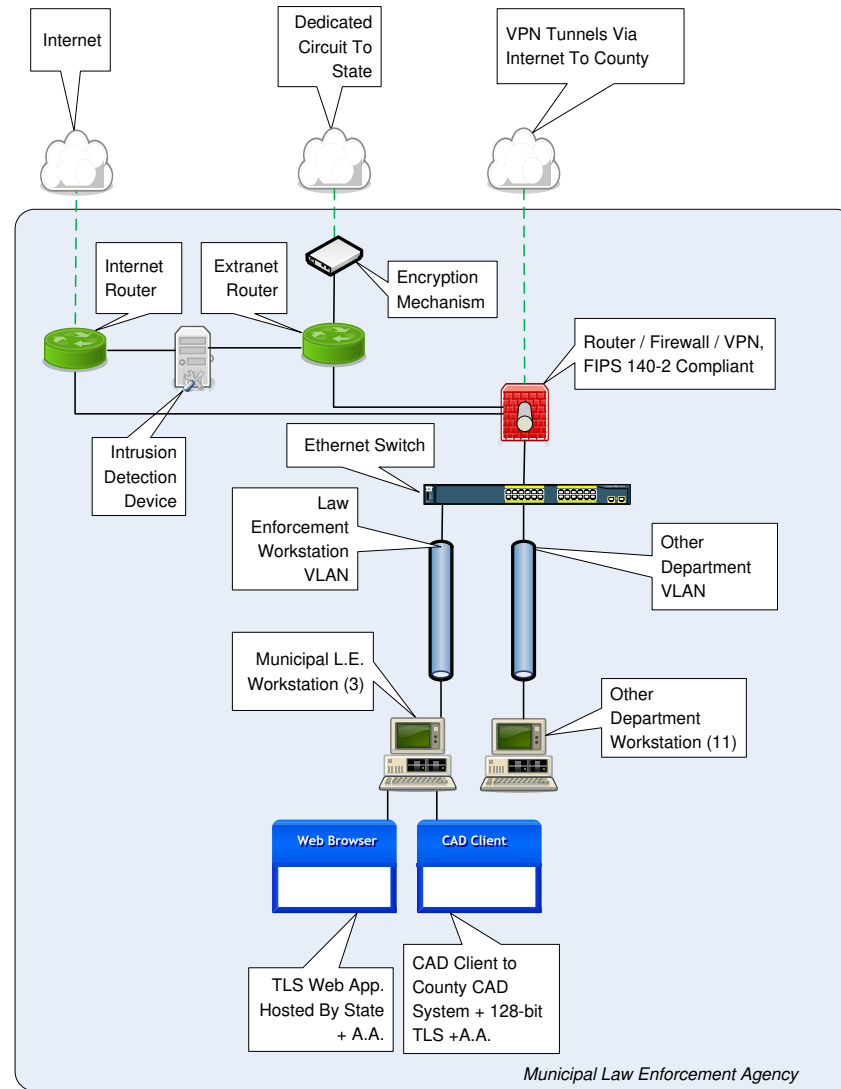
### Appendix C.1-C

01/01/2011



**Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency**

## Conceptual Topology Diagram For A Municipal Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION  
 ——— STANDARD CONNECTION

Sample Municipal Agency		
FOUO	01/01/2011	

Appendix C.1-D		
	01/01/2011	

# **APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS**

---

## **D.1 CJIS User Agreement**

### **CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT**

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Enterprise Portal; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance.

## **PART 1**

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.
2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.
3. Biannual file synchronization of information entered into the III by participating states.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history

records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.
7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJI. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.
2. CJIS Security Policy.
3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.
4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.
5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.
6. The National Fingerprint File Qualification Requirements.
7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.
8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.
10. Applicable federal, state, and tribal laws and regulations.

## **PART 2**

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.
2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.
3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.
4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.
2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.
3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.
4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

## **GENERAL PROVISIONS**

### **Funding:**

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

### **Termination:**

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.
2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.
3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:
  - a. The parties will continue participation, financial or otherwise, up to the effective date of termination.
  - b. Each party will pay the costs it incurs as a result of termination.
  - c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

## **ACKNOWLEDGMENT AND CERTIFICATION**

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity. Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

## SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

### PART 1

\_\_\_\_\_  
CJIS Systems Officer

Date: \_\_\_\_\_

\_\_\_\_\_  
Printed Name/Title

### CONCURRENCE OF CSA HEAD:

\_\_\_\_\_  
CSA Head

Date: \_\_\_\_\_

\_\_\_\_\_  
Printed Name/Title

### PART 2

\_\_\_\_\_  
CJIS WAN Official (or other CJIS Authorized Official)

Date: \_\_\_\_\_

\_\_\_\_\_  
Printed Name/Title

### CONCURRENCE OF CJIS WAN AGENCY HEAD:

\_\_\_\_\_  
CJIS WAN Agency Head

Date: \_\_\_\_\_

\_\_\_\_\_  
Printed Name/Title



**FBI CJIS DIVISION:**

\_\_\_\_\_

Date: \_\_\_\_\_

[Name]

Assistant Director

FBI CJIS Division

\* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

## D.2 Management Control Agreement

### Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

“...management control of the criminal justice function remains solely with the Criminal Justice Agency.” Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

\_\_\_\_\_  
John Smith, CIO  
Any State Department of Administration

\_\_\_\_\_  
Date

\_\_\_\_\_  
Joan Brown, CIO  
(Criminal Justice Agency)

\_\_\_\_\_  
Date

## D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

**(Insert Name of Requesting Organization)**

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF  
THIRD-PARTY CONNECTIVITY TO THE  
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. **PURPOSE:** This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. **BACKGROUND:** The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. **AUTHORITY:** The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. **SCOPE:**

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.

v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. **FUNDING:** There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. **SETTLEMENT OF DISPUTES:** Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

\_\_\_\_\_  
[Name]

\_\_\_\_\_  
Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

\_\_\_\_\_  
Date



## **D.4 Interagency Connection Agreement**

### **CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)**

#### **Wide Area Network (WAN) USER AGREEMENT**

#### **BY INTERIM REMOTE LATENT USERS**

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;
- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.
2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.
3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone

devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.
6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.
7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

## ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability*; and applicable federal or state laws and regulations applied to IAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

\*

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Print or Type

CJIS WAN Agency Official

Date

## CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE CJIS SYSTEMS OFFICER (CSO):

\*

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Print or Type

\*

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

State CSO

**FBI CJIS DIVISION:**

---

Signature – [Name]

Assistant Director

Title

Date

\* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

## APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

---

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC) <sup>2</sup>
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

## **APPENDIX F   SAMPLE FORMS**

---

This appendix contains sample forms.

## F.1 Security Incident Response Form

**FBI CJIS DIVISION  
INFORMATION SECURITY OFFICER (ISO)  
SECURITY INCIDENT REPORTING FORM**

---

NAME OF PERSON REPORTING THE INCIDENT: \_\_\_\_\_

DATE OF REPORT: \_\_\_\_\_ (mm/dd/yyyy)

DATE OF INCIDENT: \_\_\_\_\_ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): \_\_\_\_\_

LOCATION(S) OF INCIDENT: \_\_\_\_\_

INCIDENT DESCRIPTION: \_\_\_\_\_

SYSTEM(S) AFFECTED: \_\_\_\_\_

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): \_\_\_\_\_

METHOD OF DETECTION: \_\_\_\_\_

ACTIONS TAKEN/RESOLUTION: \_\_\_\_\_

**Copies To:**

**George White**

(FBI CJIS Division ISO)  
1000 Custer Hollow Road  
Clarksburg, WV 26306-0102  
(304) 625-5849  
iso@ic.fbi.gov

**John C. Weatherly**

(FBI CJIS CSIRC POC)  
1000 Custer Hollow Road/Module D-2  
Clarksburg, WV 26306-0102  
(304) 625-3660  
iso@ic.fbi.gov



## APPENDIX G BEST PRACTICES

---

### G.1 Virtualization

#### Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>:

*"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."*

From a trade publication, kernelthread.com

<http://www.kernelthread.com/publications/virtualization/>:

*"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."*

From an Open Source Software developer

<http://www.kallasoft.com/pc-hardware-virtualization-basics/>:

*"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:*

- *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
- *"Type-2 Hypervisor which requires a separate application to run within an operating system*

*“Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system.”*

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on [www.virtualization.com](http://www.virtualization.com) are examples of industry offerings.

*“Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Server 2008 Hyper-V, and is fully supported by both companies’ channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments.”*

*“Sun Microsystems today announced the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for Sun xVM Server software and contribute to the direction and development of the product.”*

*“NetEx, specialist in high-speed data transport over TCP, today announced Virtual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide-area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company’s award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network.”*

From several sources, particularly:

<http://www.windowsecurity.com/articles/security-virtualization.html>

<http://csrc.nist.gov/publications/drafts/6--64rev2/draft-sp800-64-Revision2.pdf>

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply “least privilege” technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

## G.2 Voice over Internet Protocol

### Voice over Internet Protocol (VoIP)

#### Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

#### Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

#### Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

- a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.
- b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

- a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.
- b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

### **VoIP Risks, Threats, and Vulnerabilities**

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic “CIA”). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

#### **Confidentiality and Privacy**

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker’s job easier

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

#### Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

**REMEDIATION:** If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

#### Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

**REMEDIATION:** A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

#### ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

**REMEDIATION:** Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

#### Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

#### IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

#### Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

#### Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

#### DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

#### TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious



information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

**REMEDIATION:** Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

### Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

#### **CPU Resource Consumption Attack without any account information.**

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

**REMEDIATION:** The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

#### **Default Password Vulnerability**

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

**REMEDIATION:** Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

### Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

**REMEDIATION:** These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

### Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

**REMEDIATION:** If remote access is not available, this problem can be solved with physical access control.

### **NIST Recommendations.**

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling.)
- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical securities measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone

systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

## G.3 Cloud Computing

### Cloud Computing

#### Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

#### Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

#### Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

#### Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

Ultimately, the move to cloud computing is a business decision in which the following relevant factors are giving proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

### **Achieving CJIS Security Policy Compliance:**

The question that is often asked is, “Can an Agency be compliant with the CSP and also cloud compute?”

Because the CSP is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CSP.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CSP requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the CSP requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.



Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. The following questions can help frame the process of determining compliance with the existing requirements of the CSP.

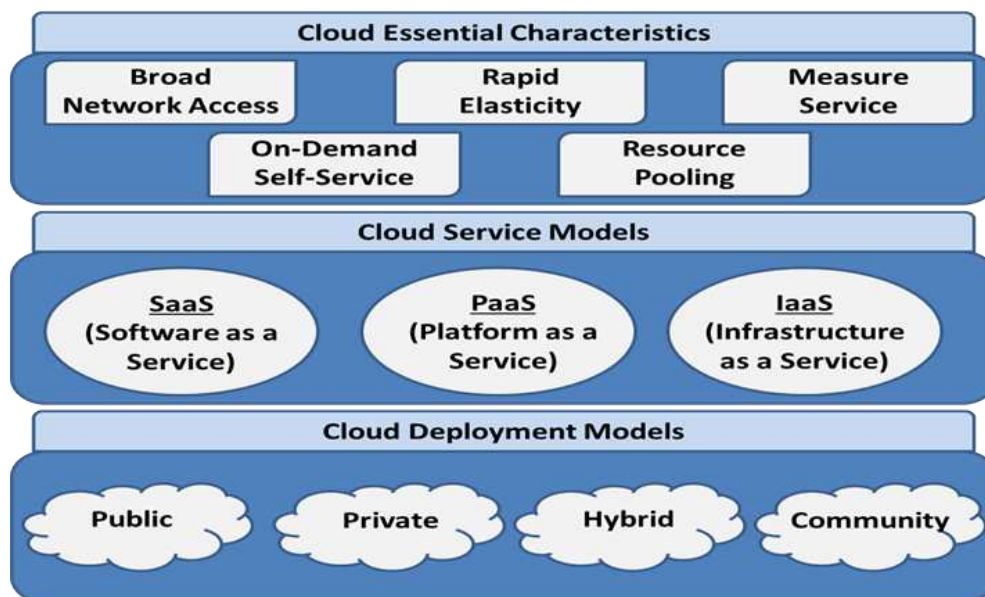
- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)
- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)
- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)
- Are the encryption requirements being met? (5.10.1.2 Encryption)
  - Who will be providing the encryption as required in the CJIS Security Policy? (client or cloud service provider)
  - Is the data encrypted while at rest and in transit?
- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
  - Will the cloud subscriber be notified of any incident?
  - If CJI is compromised, what are the notification and response procedures?
- Is the cloud service provider a private contractor/vendor?
  - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)
- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)
- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
  - Will the cloud service provider handle logging and provide that upon request?

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CSP, device and architecture independence can permit the use of cloud computing, but the security requirements do not change.

### **The Cloud Model Explained:**

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:



*Figure 1 - Visual Depiction of the NIST Cloud Computing Definition*

### Essential Characteristics:

#### *On-demand self-service*

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

### *Broad network access*

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

### *Resource pooling*

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

### *Rapid elasticity*

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

### *Measured service*

Cloud systems automatically control and optimize resource use by leveraging a metering capability\* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

*\* Typically this is done on a pay-per-use or charge-per-use basis.*

## Deployment Models:

### *Private cloud*

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

### *Community cloud*

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

### *Public cloud*

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

### *Hybrid cloud*

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

### Service Models:

#### *Software as a Service (SaaS)*

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure\*.

*\* A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as "Software deployed as a hosted service and accessed over the Internet."

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

#### *Platform as a Service (PaaS)*

This model provides the consumer the capability to deploy consumer-created or acquired applications\* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

*\* This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

#### *Infrastructure as a Service (IaaS)*

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

### **Key Security and Privacy Issues:**

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—at the extreme, *displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

### Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

## Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

### *Law and Regulations*

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

### *Data Location*

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

### *Electronic Discovery*

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

## Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

### *Insider Access*

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

### *Data Ownership*

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

### *Visibility*

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

### *Ancillary Data*

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

### *Risk Management*

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

### Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

### Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public



cloud and extending or changing the existing framework to support cloud services may prove difficult.

### Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

### Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

### *Value Concentration*

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

### *Data Isolation*

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

### *Data Sanitization*

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies

made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

### *Encryption*

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.
- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.
- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

### Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

### Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

#### *Data Availability*

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

#### *Incident Analysis and Resolution*

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

### **General Recommendations:**

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

**Table 1: Security and Privacy Issue Areas and Recommendations**

Areas	Recommendations
Governance	<ul style="list-style-type: none"> <li>Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.</li> <li>Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.</li> </ul>
Compliance	<ul style="list-style-type: none"> <li>Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements.</li> <li>Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements.</li> <li>Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.</li> </ul>
Trust	<ul style="list-style-type: none"> <li>Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time.</li> <li>Establish clear, exclusive ownership rights over data.</li> <li>Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system.</li> <li>Continuously monitor the security state of the information system to support on-going risk management decisions.</li> </ul>
Architecture	<ul style="list-style-type: none"> <li>Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.</li> </ul>
Identity and Access Management	<ul style="list-style-type: none"> <li>Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.</li> </ul>

Software Isolation	<ul style="list-style-type: none"> <li>• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.</li> </ul>
Data Protection	<ul style="list-style-type: none"> <li>• Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.</li> <li>• Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.</li> <li>• Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.</li> </ul>
Availability	<ul style="list-style-type: none"> <li>• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements.</li> <li>• Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.</li> </ul>
Incident Response	<ul style="list-style-type: none"> <li>• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.</li> <li>• Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.</li> <li>• Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.</li> </ul>

## **G.4 Mobile Appendix**

### **Mobile Appendix**

#### **Introduction**

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolution of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

#### **Mobile Device Risk Scenarios**

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce acquiring cost and enhance security.

## *Device Categories*

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

### *Laptop devices*

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a 'traditional', full featured operating system (e.g. Windows or a Linux variant). Also included in this category are 'tablet' type full featured computers running a traditional full featured operating system but without an attached keyboard. The main defining factor is the use of a full featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user's body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

### *Tablet devices*

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can

function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. 'always on cellular' vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

### *Pocket devices/Handheld devices*

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or 'holster' attached to the body. The bulk of this category will be cellular 'smartphones' with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

### *Device Connectivity*

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes 'on demand' cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either through the operating system or a third-party mobile device management (MDM) system may be



able to significantly control and define which particular connectivity risks may be associated with a particular device.

#### *Cellular Network Only (always on)*

Cellular network connectivity is characterized by ‘always on’ network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with ‘always on’ cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as ‘always on’ or ‘on demand’. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain ‘airplane’ mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other ‘eavesdropping’ devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a ‘personal firewall’ if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an ‘always on’ cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

#### *WiFi only (includes ‘on-demand’ cellular)*

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or ‘connected’ to the cellular network. They connect to the network or internet through WiFi ‘hotspots’ or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over ‘public’ WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with ‘on-demand’ cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking (‘bricking’) or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full featured laptops but may not be available for limited feature mobile operating systems.

#### *Cellular (always on) + WiFi Network*

This is a hybrid scenario that has become typical with most ‘smartphones’. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

### **Incident Handling (CJIS Security Policy Section 5.3)**

Additional or enhanced incident reporting and handling procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and

response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

### ***Loss of device Control***

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: “Is it reasonable to assume CJI could be accessed”) as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a ‘momentary’ loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while ‘minimal’ durations might include a few minutes of time and ‘extended’ periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

### ***Total Loss of device***

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out

of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

#### ***Potential device Compromise (software/application)***

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

#### **Audit and Accountability (CJIS Security Policy Section 5.4)**

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device will be necessary to ensure appropriate levels of auditing exist.

#### ***Auditable Events (reference 5.4.1)***

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and

consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

### ***Audit Event Collection***

Mobile devices without an ‘always-on’ cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in place for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

### **Access Control (CJIS Policy Section 5.5)**

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in ‘general’ purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

### ***Device Control levels and access.***

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) may bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

### ***Embedded passwords/login tied to device PIN.***

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and required a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

### ***Access requirement specification***

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

### ***Special Login attempt limit***

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

### *Login failure actions*

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

### ***System use Notification (CJIS Policy reference 5.5.4)***

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

### ***Session Lock (CJIS Policy reference 5.5.5)***

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

### ***Device WiFi Policy***

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

#### ***Hotspot capability***

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

#### ***Connection to public hotspots***

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

#### ***Cellular Service abroad***

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a 'trusted' entity by the device.



Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

### ***Bluetooth***

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

### ***Voice/Voice over IP (VoIP)***

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

### ***Chat/Text***

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

### *Administrative Access*

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from ‘general user’ access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of ‘routine’ device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

### *Rooting/Jailbreaking*

‘Rooting’ (Android OS) or ‘Jailbreaking’ (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of ‘traditional’ anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a ‘stock’ Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with ‘rooting’ and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate ‘secure’ versions of the Apple iOS and it is unlikely they will be developed.

## **Identity and Authentication**

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

### ***Utilizing Unique device Identification***

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

### *Certificate Use*

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to 'unlock' the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

### *Certificate Protections*

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

### ***Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)***

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

### **Configuration Management**

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

### ***Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)***

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

### ***Device Backups/Images***

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

### ***Bring Your Own device (BYOD) employment***

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

### ***Configurations and tests***

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

## **Media Protection**

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the 'internal' storage of the device, the Android OS does not provide secure separation of data stores on 'external' storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific 'external' media protection requirements which may actually include built-in media or storage.

### ***Protection of device connected media***

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

### ***Encryption for device media***

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

## **Physical Protection**

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

### ***Device Tracking/Recovery***

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via 'always-on' cellular data connections and the devices built-in GPS. Device tracking with WiFi only or 'on-demand' cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered

when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

### ***Devices utilizing unique device identification/certificates***

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

### **System Integrity (CJIS Policy Section 5.10)**

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

### ***Patching/Updates***

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without ‘always-on’ cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

### ***Malicious code protection/Restriction of installed applications and application permissions***

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing

other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

**TECHNOLOGY NOTE:** In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed by means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied



installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

**WARNING:** Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

### ***Firewall/IDS capability***

Traditional device or “personal” firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating sys long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

### ***Spam Protection***

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

### ***Periodic system integrity checks***

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

## **G.5 Administrator Accounts for Least Privilege and Separation of Duties**

### **Administrator Accounts for Least Privilege and Separation of Duties**

#### **PURPOSE:**

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

#### **ATTRIBUTION:**

- SANS, "The Critical Security Controls for Effective Cyber Defense", version 5.0
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", Revision 4 dated April 2013
- NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook" dated October 1995
- CNSSI-4009, "National Information Assurance (IA) Glossary", dated April 2010

#### **DEFINITIONS:**

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

#### **SUMMARY:**

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all

required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

## **USER ACCESS AND ACCOUNT MANAGEMENT:**

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user's role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account

management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

## **THREATS:**

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

### *Phishing Attacks*

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user's account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

### *Password Brute Force Guessing / Cracking*

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that

are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

## **MITIGATION:**

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g. firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

## **NIST CONSIDERATIONS FOR LEAST PRIVILEGE:**

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of

the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

## **AC-6 Least Privilege**

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

### Control Enhancements:

#### **(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS**

**The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].**

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

### Control Enhancements:

#### **(2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS**

**The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.**

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

### **(3) LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS**

**The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.**

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

### **(4) LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS**

**The information system provides separate processing domains to enable finer-grained allocation of user privileges.**

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

### **(5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS**

**The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].**



Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

**(6) LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS**

**The organization prohibits privileged access to the information system by non-organizational users.**

Supplemental Guidance: Related control: IA-8.

**(7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES**

**The organization:**

**(a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and**

**(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.**

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

**(8) LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION**

**The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.**

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such

applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

**(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS***

**The information system audits the execution of privileged functions.**

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

**(10) *LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS***

**The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.**

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	<b>LOW</b> Not Selected	<b>MOD</b> AC-6 (1) (2) (5) (9) (10)	<b>HIGH</b> AC-6 (1) (2) (3) (5) (9) (10)
----	-------------------------	--------------------------------------	-------------------------------------------

**SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS)  
CONSIDERATION FOR LEAST PRIVILEGE:**

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the “20 Critical Security Controls for Effective Cyber Defense”. This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled “Controlled Use of Administrative Privileges”. SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

## **Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges**

*The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

<b>ID #</b>	<b>Description</b>	<b>Category</b>
CSC 12--1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	<i>Quick win (One of the “First Five”)</i>
CSC 12--2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive	<i>Quick win</i>
CSC 12--3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	<i>Quick win</i>

CSC 12---4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration---level accounts.	<i>Quick win</i>
CSC 12---5	Ensure that all service accounts have long and difficult--- to---guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	<i>Quick win</i>
CSC 12---6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800---132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super---user privileges.	<i>Quick win</i>
CSC 12---7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e---mail, composing documents, or surfing the Internet. Web browsers and e---mail clients especially must be configured to never run as administrator.	<i>Quick win</i>
CSC 12---8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non---administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows “administrator” or UNIX “root” accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	<i>Quick win</i>
CSC 12---9	Configure operating systems so that passwords cannot be re---used within a timeframe of six months.	<i>Quick win</i>
CSC 12---10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators’ group, or when a new local administrator account is added on a system.	<i>Visibility/ Attribution</i>
CSC 12---11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	<i>Visibility/ Attribution</i>

CSC 12--12	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	<i>Configuration/ Hygiene</i>
CSC 12--13 (NEW)	When using certificates to enable multi-factor certificate-based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	<i>Configuration/ Hygiene</i>
CSC 12--14	Block access to a machine (either remotely or locally) for administrator-level accounts. Instead, administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	<i>Configuration/ Hygiene</i>

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

## **SEPARATION OF DUTIES:**

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection

against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

## **THREATS:**

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g. a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

## **MITIGATION:**

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.

Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

## **NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:**

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements but it is significant in protecting the integrity of an information system.

### **AC-5 Separation of Duties**

Control: The organization:

- a. Separates [*Assignment: organization-defined duties of individuals*];
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5
----	------------------	----------	-----------

## **APPENDIX H SECURITY ADDENDUM**

---

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).



**FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES  
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the  
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved

by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
  - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
  - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
  - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain

such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

**FEDERAL BUREAU OF INVESTIGATION**  
**CRIMINAL JUSTICE INFORMATION SERVICES**  
**SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

**1.00 Definitions**

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

**2.00 Responsibilities of the Contracting Government Agency.**

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

**3.00 Responsibilities of the Contractor.**

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

**4.00 Security Violations.**

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

#### 5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

#### 6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES  
SECURITY ADDENDUM**

**CERTIFICATION**

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

\_\_\_\_\_  
Printed Name/Signature of Contractor Employee

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed Name/Signature of Contractor Representative

\_\_\_\_\_  
Date

\_\_\_\_\_  
Organization and Title of Contractor Representative

## APPENDIX I REFERENCES

---

White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI)”, May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

- [NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44
- [NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2
- [NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46
- [NIST SP 800–48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800–48
- [NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52
- [NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2
- [NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A
- [NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58
- [NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT
- [NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT
- [NIST SP 800–64] NIST Special Publication 800–64
- [NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800–66
- [NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68
- [NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70
- [NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72
- [NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1
- [NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76
- [NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77
- [NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78
- [NIST SP 800–81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800–81



- [NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84
- [NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86
- [NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87
- [NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96
- [NIST SP 800–97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800–97
- [NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121
- [NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124
- [NIST SP 800-125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800-125
- [NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996
- [OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003
- [OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006
- [OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006
- [OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006
- [OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Memo 07–16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code,  
Title 44 - Public Printing and Documents; Chapter 35 - Coordination of  
Federal Information Policy; Subchapter I - Federal Information Policy, Section  
3506

## APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

---

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Noncriminal Justice Agencies (NCJA) with access to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau (SIB) and/or Channeling agency. Examples of the target audience for the Appendix J supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those NCJAs new to the CSP and Advisory Policy Board (APB) auditing process (all NCJAs will be periodically audited by the CJIS Systems Agency (CSA)/SIB and may be included in a sampling of triennial audits conducted by the FBI) it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every NCJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

### **General CJI Guidance**

The following information provides NCJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. **3.2.9 – Local Agency Security Officer (LASO)**

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local NCJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and

procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.6 – Agency User Agreements

When an NCJA (private or public) is permitted to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions as authorized pursuant to federal law or state statute approved by the U.S. Attorney General, the information received from the background check, such as criminal history record information (CHRI) or personally identifiable information (PII), must be protected as CJI. In order to receive access to CJI the NCJA must enter into a signed written agreement, i.e., an agency user agreement, with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the CJI access. An example of a NCJA (private) is a local bank. An example of a NCJA (public) is a county school board.

*Note 1: The CSA, SIB, or authorized agency providing the CJI access term should be part of the agency user agreement.*

*Note 2: Any NCJA that directly accesses FBI CJIS must allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.*

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2.1.1 – All Personnel (Security Awareness Training)

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

*Note: The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.*

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help NCJAs with:

- (i) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,

- (ii) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

*Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.*

*Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.*

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

*Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.*

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Electronic media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must

be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a criminal justice conveyance, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

*Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.*

*Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.*

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

*Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record information for the purposes of licensing or employment need to follow the guidance in Section 5.12 (referenced below).*

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring access to CJI - listed in CSP Section 5.12.1.1. In addition to the requirements listed in CSP Section 5.12.1.1 contractors and vendors must undergo additional screening requirements as listed in CSP Section 5.12.1.2.2.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

*Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law.*

**The following scenarios are intended to help the reader identify areas within the CSP that NCJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above General CJI Guidance section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.**

**Hard Copy CJI Storage and Accessibility**

When an NCJA receives CJI via a paper copy from a CJA and stores the paper within a locked file cabinet, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

**Electronic CJI Storage and Accessibility – Controlled Area**

When an NCJA creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:



a. 5.5.2.4 (3) – Access Control – Encryption

CSP Section 5.5.2.4 item 3 – Encryption describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

**Electronic CJI Storage and Accessibility – Physically Secure Location**

When an NCJA receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy sections:

a. 5.5 – Access Control

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. 5.6 – Identification and Authentication

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. 5.7 – Configuration Management

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

## Use Case Scenarios

### 1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that has indirect access to CJI and is located in a secure data center within the board of education offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to an employee's electronic record. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the record, the user is prompted to enter their unique username and password. Because the record resides on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required to access the record.

*NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.*

### 2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) encryption algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access an employee's record, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder.

*NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.*

## APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

---

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance is not intended for criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as “terminal agencies”.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to criminal justice information (CJI) maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those CJAs new to the CSP it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every CJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

### **General CJI Guidance**

The following information provides CJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

#### **a. 3.2.9 – Local Agency Security Officer (LASO)**

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local CJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI must enter into a signed agreement with the CSA providing the access. The agreement specifies the services and systems the agency will access. It must also specify all pertinent governance policies to which the agency must adhere.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2 – Security Awareness Training

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

CSP Section 5.2.1.2 describes the topics required to be discussed for personnel that have both physical and logical access to CJI. These topics are covered in addition to the ones addressed in basic security awareness training.

CSP Section 5.2.1.3 describes topics to be covered for those personnel assigned information technology roles. Topics covered in this section are in addition to the topics addressed in Sections 5.2.1.1 and 5.2.1.2.

*Note: The CSO may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.*

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help CJAs with:

- (iii) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (iv) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

*Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.*

*Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.*

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

*Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.*

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving

agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to digital and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Digital media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store digital and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy digital media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a police vehicle, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated

information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 explains the technical safeguards ranging from boundary and transmission protection to security an agency’s virtualized environment.

CSP Section 5.10.1.2 details the requirements for the encryption of CJI whether in transit or at rest. FIPS 140-2 certification is required when CJI is in transit outside a physically secure location. When at rest outside a physically secure location, encryption methods can use Advanced Encryption Standard (AES) at 256 bit strength or a FIPS 140-2 certified method.

CSP Section 5.10.3 explains the use of virtualization and partitioning when processing CJI in a virtual environment. A virtualized environment can be configured such that those parts of the system which process CJI are either physically or virtually separated from those that do not.

CSP Section 5.10.4 explains system and information integrity policy and procedures. This includes areas such as patch management, malicious code protection, and spam and spyware protection.

j. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

*Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.*

*Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.*

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

k. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring access to CJI - listed in CSP Section 5.12.1.1. In addition to the requirements listed in CSP Section 5.12.1.1 contractors and vendors must undergo additional screening requirements as listed in CSP Section 5.12.1.2.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

l. 5.13 – Mobile Devices

When access to CJI using mobile devices such as laptops, smartphones, and tablets is authorized, CSP Section 5.13 explains the controls required to manage those devices to ensure the information remains protected.

**The following scenarios are intended to help the reader identify areas within the CSP that CJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above “General CJI Guidance” section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.**

**Hard Copy CJI Storage and Accessibility**

When CJI is received in hard copy and the agency stores the paper within a locked file cabinet, the CJA should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

**Electronic CJI Storage and Accessibility – Controlled Area**

When an agency creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared



network drive in a controlled area for indirect access by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control Mechanisms – Encryption

CSP Section 5.5.2.4 item 3, Encryption – This describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

**Electronic CJI Storage and Accessibility – Physically Secure Location**

When an agency receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy sections:

a. 5.5 – Access Control

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. 5.6 – Identification and Authentication

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. 5.7 – Configuration Management

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency’s environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

## Use Case Scenarios

### 1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county court scans hard copy case documents containing CJI into an electronic format. The documents are placed on a network server which is located in a secure data center within the court offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to case documents. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the documents, the user is prompted to enter their unique username and password. Because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

*NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.*

### 2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county court scans hard copy case documents containing CJI in an electronic format. The documents are placed on a network server which is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access to the case documents, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder. Additionally, because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

*NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.*

## **Background Procedures 2025 nrt.pdf**

# Stanislaus County District Attorney

## Pre-employment Background Procedures

## **I. LEVELS OF THE BACKGROUND INVESTIGATION**

### **1. Definition of Levels of the Background**

Because of the expense and resources required to conduct background investigations, there will be four different levels of background investigations conducted on applicants for positions within the District Attorney's Office. All of the background investigations shall be conducted in a thorough manner, however, limited resources and different levels of responsibility for different positions within the office, dictate the necessity to conduct a more thorough inquiry into some positions than others.

The level of background completed shall be determined by the position being applied for. A level four investigation shall be the most thorough and a level one investigation the least. The levels shall be determined as follows:

**Level One:** Volunteer, Student Intern, other non-paid positions, Contract Employees.

**Level Two:** Legal Clerk, Administrative Clerk, Account Clerk, Victim Advocate, Social Worker, other clerical positions, GSA custodian and maintenance positions.

**Level Three:** Deputy District Attorney, Family Support Officer, Confidential Assistant, Paralegal, Manager, Account Technician, Personnel Manager, Personnel Assistant, Administrative Secretary, Clerical Supervisor, System Analyst and IT Positions, other management or supervisory positions.

**Level Four:** All Criminal Investigators or any position which requires peace officer powers.

Based on the proposed assignment of an applicant, a supervisor may request a more thorough background be conducted on a person whose classification calls for a lower level. For example, a level three investigation, instead of a level two, may be conducted on a Legal Clerk or Administrative Clerk who is going to be assigned to the Investigations Division.

The procedures for conducting the background investigation listed in this manual will state which level of background the procedure will apply to. If no level is stated, then the procedure will apply to all levels.

## **II. CONDUCTING THE BACKGROUND INVESTIGATION**

### **1. Local Computer Database Checks (All Levels)**

Once the Personal History Statement has been checked by the Human Resources Manager it shall be turned over to the Investigations Division clerical staff for file preparation. The clerical staff shall prepare the investigative file and assign a background number to it.

The clerical staff will then be responsible for conducting the below listed checks on **all levels** of backgrounds:

A. Run a DMV check on the applicant. Attach the printout to the file.

(1) Check to see if the driver's license is suspended or revoked, note any restrictions on the license, and note the number of citations and accidents on the license record. Record this information on your report.

B. Run a warrant check on the applicant and on each person that the applicant lists as residing in their home. Print out all of the response screens and attach those to the file.

(2) This check should reveal if the applicant has any arrest warrants or restraining orders against him or her, is on parole, or is a registered sex or drug offender. If any of this information is located this information should be printed and attached to the file.

C. Check in DA ICJIS for any open or closed cases prosecuted by this office on the applicant, any person the applicant lists as residing with them, the immediate family members of the applicant, and any current or former spouses of the applicant. If any cases are located print out the information and attach them to the file.

D. Check the computerized probation records for any contacts with the applicant, any person the applicant lists as residing with them, and the immediate family of the applicant. If any contacts are located print out the screens and attach to the file.

E. Obtain a credit report for all Level II, III, and IV backgrounds. Credit reports are not required for a Level I background.

*(Note: The investigator must check the credit report to ensure that the information provided on the credit report matches the information provided by the applicant in the personal history statement. The credit report may list former addresses and former employers of the applicant. These should be compared with the information provided by the applicant. An applicant who was fired from a job or evicted from a residence may try to conceal this information by not including it on their personal history statement.)*

F. Check social media pages such as Facebook, Instagram, and Twitter. If located, print the home page identifying the applicant. Look for any posts that are criminal in nature or that may reflect negatively on the office. A paragraph on these findings or lack thereof must be documented in the investigator's report.

## **2. Criminal Offender History Information (CORI) (All Levels)**

*(Note: State regulations prohibit the running of an automated rap sheet on the applicant or on*

*anybody else for any purpose associated with a pre-employment background investigation. The only exception is if criminal activity is suspected and then only if a criminal investigation is initiated.)*

A very important step in the background process for all levels of backgrounds is looking for Criminal History Offender Information (CORI). CORI can be located in a number of different locations. The easiest location is in the automated RAP sheet through the Department of Justice. CORI information maintained by the Department of Justice is called State Summary Criminal Offender Record Information. State regulations prevent us from using the automated RAP sheets for the purposes of the background investigation.

Part of the background investigation process involves fingerprinting the applicant and submitting the fingerprints to DOJ where they will search the State Summary CORI. The problem with relying solely on the fingerprint check is DOJ will only return information which would disqualify an applicant from employment with the District Attorney's office. They won't return information on arrests of the applicant where there was no conviction, or arrests for some misdemeanors. In some cases, a person may have been convicted of a crime and their automated RAP sheet was never updated with the conviction information. If this happens the fingerprint check will come back clear. For this reason we must make every effort to look for CORI from other sources during the background investigation. The clerical staff is responsible for looking for CORI on **all levels** of background investigations.

The following checks shall be made by the clerical staff looking for CORI:

- A. Check DA ICJIS if not already done.
- B. Check the Superior Court and Stanislaus County Jail databases if not already done.
- C. Check with each police agency having jurisdiction over the applicant's residences for the last ten years for Level I, II, and III backgrounds and the last fifteen years for a Level IV background. We are looking for any contacts the police agency may have had with the applicant.
  - (1) Police Agency checks will require either an automated message through CLETS or a faxed request with a copy of a waiver (Attachment \*\*\*) signed by the applicant.
  - (2) To avoid delays, the police agency should be contacted within 48 hours if they have not responded to our request for information.
  - (3) If a police agency fails to respond, or refuses to respond, to our request for information the investigator assigned to handle the background should be notified or the background Lieutenant should be notified of the problem.

*(Note: In the event a police agency refuses to provide information, section 13300 of the California Penal Code should be reviewed by the investigator. Sections 6262 through 6264,*

*6254 (f)(1), and 6254 (f)(2) should also be reviewed. Certain information regarding arrests and criminal complaints are public record. Section 13300 of the Penal Code deals directly with CORI and requires release of CORI information to a District Attorney, (“when needed in the course of their duties.” )*

*(Note: Section 432.7 of the California Labor Code governs the use of arrest information, that has not resulted in a conviction, during the pre-employment screening process. However, subsection (e) of section 432.7 exempts agencies defined under section 13101 of the Penal Code from these same restrictions. A District Attorney’s Office is an agency defined by section 13101 of the Penal Code.)*

### **3. Education and State Bar Checks. (All Levels Where Applicable)**

If an applicant lists a college degree on their application or personal history statement, this information shall be confirmed whether the degree is required for the position or not. The education checks, with the exception of the on-line State bar check, should be done by the investigator. However, a properly trained legal or admin clerk can be allowed to conduct these checks.

A. If the degree is not required for the position telephone confirmation with the college or university is sufficient.

B. If the degree is required for the position, the applicant shall provide a copy of the diploma along with copies of all the applicable transcripts. Telephone confirmation with the college or university shall be made to confirm the veracity of the documents provided.

C. For applicants for attorney positions confirmation will be made with the State Bar to ensure membership. This can be done on the State Bar’s web site.

D. For applicants attorney positions the investigator shall check with the law school the applicant attended and check for records of suspension or discipline.

E. The credit report shall be checked to confirm that all student loans are being paid promptly and are not in default.

### **4. Interviewing the Applicant (Level II, III and IV)**

For Level II and III investigations the investigator should schedule an interview with the applicant prior to starting the rest of the investigation. For Level IV investigations the investigator shall schedule an interview with the applicant. This interview should be done in person at the applicant’s home whenever possible. The interview can be scheduled to coincide with the neighborhood checks discussed later in this manual. This isn’t required for Level I investigations but is not prohibited if the investigator feels it’s necessary.



There are several reasons for conducting these interviews at the applicant's home. It gives you a chance to see where the applicant lives. You should look for things that may suggest gang involvement, involvement with drugs, or anything that may suggest criminal behavior on the part of the applicant or anybody residing with the applicant. You should also look for things that may suggest the applicant is unorganized or sloppy, both traits which may affect his or her job performance.

During this interview the investigator will go over the Personal History Statement and make sure the applicant has provided all of the required information. If the applicant has not provided all of the required documents such as diplomas, transcripts, DD214, etc., those documents should be obtained now.

Care should be taken to determine if the applicant has listed all of their previous employers and has listed all of the information required to complete the background investigation. If adequate phone numbers and contact information have not been listed for references and previous employers that information should be obtained now. You should obtain any information that will help you in making the required contacts on the background investigation. For example, directions to previous employers, names of personnel managers, is the previous employer still in business, who was the applicant's direct supervisor at the place of employment, etc.

## **5. Previous Employer Checks (Levels II, III, and IV)**

Previous employers shall be checked for information about the applicant. This is not required on Level I backgrounds. Previous employer checks should be done by a criminal investigator. In the case of a Level IV background the previous employer checks must be done by a Criminal Investigator.

Previous employer contacts for Level III and Level IV backgrounds shall be done in person whenever possible.

When deciding whether to do previous employer checks in person on Level III and Level IV backgrounds, the cost of travel to the location versus the information expected to be obtained should be weighed and discussed with the background Lieutenant. For example, if an applicant for a Deputy District Attorney position worked for a law firm in Arizona ten years previously, the expense of traveling to Arizona probably won't be worth the information that would be obtained. However, travel may be required to contact previous or current employers of applicants for Level III and IV investigations. In the event applicants have recent employers in other areas of the Country, management approval must be sought before traveling to those locations for the purpose of background investigations.

On Level IV (Peace Officer) backgrounds, section 1031.1 of the California Government Code requires previous employers to provide certain information about applicants for peace officer positions. In the event you find a previous employer who is unwilling to provide information, section 1031.1 should be reviewed and appropriate action taken.

Whenever possible the investigator should try and examine an applicant's personnel file. On Level IV investigations this is mandatory and is mandatory for any level of investigation where the applicant lists Stanislaus County as the previous employer. Contact the County personnel department (located at the CEO's Office) for access to County personnel files.

The personnel file should be thoroughly examined. This should not be a problem for previous government agency employers (except for the Federal Government), but many private companies will probably not allow you access to the personnel files. Many employers may allow you access to the file but may not allow you to make copies of documents. Take notes if this is the case. Look for any records of discipline. Review performance appraisals and note good and bad behavior trends. Look for the applicant's job application to that employer. Make sure the information provided on that job application matches the information provided by the applicant on the personal history statement. Look to see if the previous employer conducted a background investigation and if so review that background investigation.

In some cases, you will find that an applicant has made an agreement with a previous employer not to reveal any information about the reason the applicant separated from employment with the employer. This should send up a red flag and needs to be investigated thoroughly. The applicant must be willing to sign a special waiver allowing us access to the information in their personnel file at the previous employer. Failure or refusal to sign a waiver to grant this access could result in the applicant not being considered for employment. When circumstances such as this arises, this shall be brought to the attention of the background Lieutenant.

Remember when asking questions of a former employer, you must avoid areas that are prohibited to inquire into by the Americans with Disabilities Act (ADA). For example, you cannot ask about excessive sick leave usage, but you may ask if the employee was ever disciplined for abusing sick leave. You can ask about extended absences from work but caution the employer not to respond if the absences related to a medical condition.

Do not promise a previous employer that the information they provide will never be revealed to the applicant. You can tell them the information is confidential, and we will never voluntarily release it to the applicant absent a court order. Avoid giving legal advice to a former employer or supervisor. Many times, they may ask if they can be sued for giving you information. Do not tell them they can't be sued. You can tell them the applicant has signed a waiver agreeing to release them from liability for providing truthful and accurate information. Do not go any further into this matter than this. The facts are a former employer can be successfully sued if they intentionally provide false or misleading information about previous employee's job performance.

Below is a list of some questions you may ask of a previous employer or supervisor. This list is just a guide. If areas of concern arise, they should be questioned more thoroughly:

A. What were the dates the applicant was employed with your company?

*(Note: The answer to this question must be compared with the information provided by the applicant on the personal history statement. Applicants who have been fired from previous jobs may try and cover this up by lying about employment dates with other employers so as to not show a gap in employment.)*

- B. Was the applicant punctual and dependable?
  - C. How did the applicant get along with other employees?
  - D. How did the applicant confront problems?
  - E. Did the applicant ever display a hostile or violent temper?
  - F. Was the applicant honest and truthful?
  - G. Do you have any record of salary garnishment or other financial problems of the applicant?
- (Note: The IRS or Franchise Tax Board, along with many other government agencies may garnish and applicant's wages. This information should also be listed on the credit report.)*
- H. Did the applicant have any extended work absences for other than medical reasons?
  - I. Would you re-employ the applicant?
  - J. Can you think of any reason the applicant may not be suited to work in a criminal justice agency such as the District Attorney's Office?

If an employer seems like they are giving too favorable of a recommendation for a current employee this may send up a red flag. Sometimes employers or supervisors will give glowing recommendations for current employees if they have a reason to want to get rid of that employee. This happens more often than we may think. If it seems like this is happening the investigator should make efforts to contact more co-workers. Co-workers are more likely to be truthful with you.

## **6. Neighborhood Checks (Levels II, III and IV only)**

The investigator shall check with neighbors on levels II, III, and IV backgrounds. If the applicant has lived at his or her current residence longer than two years you only need to check at the current residence. If the applicant has lived at the current residence less than two years you should check with neighbors at the previous residence. For GSA employees, a neighborhood check will be conducted at the discretion of the background investigator.

For level IV backgrounds follow the guidelines in the POST manual for the neighbor checks. For level III backgrounds you should inquire about the following; How well the applicant got

along with his or her neighbors, were there any neighborhood problems related to the applicant, is the neighbor aware of any time of criminal activity on the part of the applicant, etc.

## **7. Relatives, Spouses, Ex-Spouses (Levels II, III and IV only)**

For level IV backgrounds follow the guidelines in the POST manual for checking with relatives, spouses and ex-spouses. For level III backgrounds the investigator should contact several of the relatives listed by the applicant. Inquire about the applicant's character, reliability, and trustworthiness.

The investigator should contact the current spouse and any former spouses. Keep in mind that former spouses may not think too kindly of the applicant and may not be completely honest in their evaluation of the applicant. Inquire about the applicant's character, reliability, and trustworthiness. Spouses should also be asked about domestic violence issues.

When contacting relatives and spouses the investigator may also want to confirm information provided by the applicant on the personal history statement. Ask the relative or spouse where the applicant has worked for the past ten years and ask if they are familiar with any contacts the applicant has had with the police. Compare this information to the information the applicant has provide you on the personal history statement.

## **8. Personal References (Levels II, III, and IV only)**

For level IV backgrounds follow the guidelines in the POST manual for checking with personal references. For level III backgrounds the investigator should contact several of the personal references listed by the applicant. Inquire about the applicant's character, reliability, and trustworthiness.

# **III. RECOMMENDATIONS**

## **1. Pass or Fail**

Every background investigation will contain the recommendations of the Investigator conducting the background. If the Investigator is going to recommend that the applicant not be hired because of information in the background, the Investigator must first consult the background Lieutenant.

## **2. Failure Prior to Completion of the Investigation**

In the event information is located during the background that would disqualify the applicant from employment, do not continue the background investigation. This information shall be brought to the attention of the background Lieutenant who can direct the background be discontinued. If it's not clear whether the information will disqualify the applicant, the background Lieutenant can consult the Chief Investigator and allow them to make this

determination. If more information is needed, the Investigator may be directed to investigate the matter further and then bring the findings back for a determination.

### **3. Things to Consider Before Making Recommendations**

A. Title 11, Chapter 5, Section 525, of the United States Code prohibits a government employer from denying employment to an applicant based solely on the applicants filing for bankruptcy.

(1) The simple fact that an applicant has filed for bankruptcy is not to be used to deny employment. However, the circumstances surrounding the bankruptcy can be used to determine suitability for employment.

(2) Bankruptcies can happen for many reasons not the fault of the applicant. Deaths in the family, spouses who don't pay child support, unforeseen medical bills, downturns in the real estate market, are all reasons for bankruptcies that shouldn't necessarily be counted against the applicant.

(3) Bankruptcies based on the applicant living a lifestyle they can't afford should be considered during the background process. Buying expensive cars and running up department store credit cards are signs that the applicant is displaying irresponsible behavior. It is reasonable to assume that if an applicant can't be responsible with his or her own finances, they are likely not to be a responsible employee.

B. In the event the applicant has been arrested and the arrest did not result in a conviction, this information shall not be used against the applicant without a thorough review of all the circumstances of the arrest and any subsequent court proceedings.

C. Criminal Activity of family members of the applicant, or of people living with the applicant, should be considered on a case-by-case basis but does not automatically disqualify an applicant. The investigator should try and determine the applicant's knowledge of criminal behavior and should consider the severity of the criminal behavior.

(1) In the event a family member of the applicant or a person the applicant is living with, is currently being prosecuted by our office, this needs to be brought to the attention of the background Lieutenant who will notify the Chief Investigator. In the event the applicant is offered employment by the District Attorney's Office, a conflict of interest could arise that would result in the Attorney General's Office taking over the prosecution of the case.

D. If an applicant is a victim of or a witness to a crime that is currently being prosecuted by this office, that information should be noted in the background report and brought to the attention of the background Lieutenant who will notify the Chief Investigator. Being a victim of a crime shall not be used to deny employment to an applicant.

### **IV. THE BACKGROUND INVESTIGATION REPORT**

The background investigation report format shall be the same for all levels of background investigations. Only the particular headings that are relevant to the level of the background being conducted shall be included on the final report.

As of the writing of this manual the report format listed herein will comply with the POST requirements for Peace Officers. In the event POST requires a different format than is listed in this manual, then the POST requirements will prevail.

The background investigation report shall be completed on the authorized District Attorney's Office memorandum form. The original report will have one-inch margins on both sides and the top and bottom. Copies shall not be made of the original without the approval of the background Lieutenant. The investigator shall retain a copy of their own background reports on their computers until such time as the reports have been reviewed by the Assistant District Attorney and/or the District Attorney. If no additions or changes to the reports are required or requested the computerized copies of the reports can be deleted.

The file format and background investigator report format shall be consistent with the following:

### **1. The Report File Tab Sections**

The background report shall be comprised of the following tabs/headings. Don't include the tabs/ headings if they don't apply to the level of investigation:

- A. Personal History Statement
- B. Education/Certificates
- C. Financial
- D. DMV
- E. LiveScan
- F. POST
- G. Agency Checks
- H. Previous Background

### **2. The Investigative Report Format**

The Investigative report shall contain the following headings in the order listed as this order matches the order on the personal history statement. Don't include headings if they don't apply to the level of investigation:

- A. Personal Information
- B. Relatives and References
- C. Education
- D. Residence History
- E. Experience and Employment History

- F. Military Experience
- G. Financial History
- H. Legal
- I. Motor Vehicle Information
- J. Recommendation

## **V. U.S. DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAMS**

The Office of Justice Programs (OJP) awards federal grants to agencies that supplement salaries, equipment, and training. OJP grants have award conditions that determine suitability, in advance, for Stanislaus County employees who may interact with participating minors. Members of the Victims Services Unit are funded by an OJP grant and must meet the following award conditions every 5 years. (OJP website: <https://www.ojp.gov/funding/explore/interact-minors>, February 13, 2024)

### **Determination of suitability required, in advance, for certain individuals who may interact with participating minors**

#### **1. Advance determination regarding suitability.**

The recipient (and any subrecipient at any tier) may not permit any covered individual to interact with any participating minor in the course of activities under the award, unless the recipient or subrecipient first has made a written determination of the suitability of that individual to interact with participating minors, based on current and appropriate information as described in paragraph 3.E., and taking into account the factors and considerations described in paragraph 4.

#### **2. Updates and reexaminations**

A. The recipient (or subrecipient) must, at least every five years, update the searches described in paragraph 3.E.1. and 2., reexamine the covered individual's suitability determination in light of those search results, and, if appropriate, modify or withdraw that determination.

B. The recipient also must reexamine a covered individual's suitability determination upon learning of information that reasonably may suggest unsuitability and, if appropriate, modify or withdraw that determination.

#### **3. Definitions**

A. "Covered individual" means any individual (other than a participating minor, as defined in this condition, or a client of the recipient (or subrecipient)) who is expected, or reasonably likely, to interact with any participating minor (other than the individual's own minor children). A covered individual need not have any particular employment status or legal relationship with the recipient (or subrecipient). Such an individual might be an employee of a recipient (or subrecipient), but also might be (for example) a consultant, contractor, employee of a contractor, trainee, volunteer, or teacher.

B. "Participating minor." All individuals under 18 years of age within the set of individuals described in the scope section of this condition as it appears on the award document are participating minors.

C. "Interaction" includes physical contact, oral and written communication, and the transmission of images and sound, and may be in person or by electronic (or similar) means. But "interaction" does not include—

- (1) brief contact that is both unexpected by the recipient (or subrecipient) and unintentional on the part of the covered individual -- such as might occur when a postal carrier delivers mail to an administrative office.

- (2) personally-accompanied contact -- that is, infrequent or occasional contact (for example, by someone who comes to make a presentation) in the presence of an accompanying adult, pursuant to written policies and procedures of the recipient (or subrecipient) that are designed to ensure that -- throughout the contact -- an appropriate adult who has been determined to be suitable pursuant to this condition will closely and personally accompany, and remain continuously within view and earshot of, the covered individual.

D. "Activities under the award." Whether paid for with federal funds from the award, "matching" funds included in the OJP-approved budget for the award, or "program income" for the award as defined by the (DOJ) Part 200 Uniform Requirements), activities under the award include both—

- (1) activities carried out under the award by the recipient (or subrecipient); and

- (2) actions taken by an entity or individual pursuant to a procurement contract under the award or to a procurement contract under a subaward at any tier.

E. "Current and appropriate information"

In addition to information resulting from checks or screening required by applicable federal, state, tribal, or local law, and/or by the recipient's (or subrecipient's) written policies and procedures, current and appropriate information includes the results of all required searches listed below, each of which must be completed no earlier than six months before the determination regarding suitability.

- (1) Public sex offender and child abuse websites/registries

A search (by current name, and, if applicable, by previous name(s) or aliases), of the pertinent and reasonably- accessible federal, state, and (if applicable) local and tribal sex offender and child abuse websites/public registries, including—



(a) the Dru Sjodin National Sex Offender Public Website ([www.nsopw.gov](http://www.nsopw.gov));

(b) the website/public registry for each state (and/or tribe, if applicable) in which the individual lives, works, or goes to school, or has lived, worked, or gone to school at any time during the past five years; and

(c) the website/public registry for each state (and/or tribe, if applicable) in which the individual is expected to, or reasonably likely to, interact with a participating minor in the course of activities under the award.

(2) Criminal history registries and similar repositories of criminal history records  
For each individual at least 18 years of age who is a covered individual under this award, a fingerprint search (or, if the recipient or subrecipient documents that a fingerprint search is not legally available, a name-based search, using current and, if applicable, previous names and aliases) -- encompassing at least the time period beginning five calendar years preceding the date of the search request -- of pertinent state (and, if applicable, local and tribal) criminal history registries or similar repositories, including—

(a) the criminal history registry for each state in which the individual lives, works, or goes to school, or has lived, worked, or gone to school at any time during the past five years; and

(b) the criminal history registry for each state in which he or she is expected to, or reasonably likely to, interact with a participating minor in the course of activities under the award.

#### **4. Factors and considerations in determinations regarding suitability**

In addition to the factors and considerations that must or may be considered under applicable federal, state, tribal, or local law, and under the recipient's (or subrecipient's) written policies and procedures, in making a determination regarding suitability, the recipient (or subrecipient) must consider the current and appropriate information described in paragraph 3.E.

In particular (unless applicable law precludes it), with respect to either an initial determination of suitability or a subsequent reexamination, the recipient (or subrecipient) may not determine that a covered individual is suitable to interact with participating minors in the course of activities under the award if the covered individual—

A. Withholds consent to a criminal history search required by this condition;

B. Knowingly makes (or made) a false statement that affects, or is intended to affect, any search required by this condition;

C. Is listed as a registered sex offender on the Dru Sjodin National Sex Offender Public Website;

D. To the knowledge of the recipient (or subrecipient), has been convicted -- whether as a felony or misdemeanor -- under federal, state, tribal, or local law of any of the following crimes (or any substantially equivalent criminal offense, regardless of the specific words by which it may be identified in law):

- (1) sexual or physical abuse, neglect, or endangerment of an individual under the age of 18 at the time of the offense;
- (2) rape/sexual assault, including conspiracy to commit rape/sexual assault;
- (3) sexual exploitation, such as through child pornography or sex trafficking;
- (4) kidnapping;
- (5) voyeurism; or

E. Is determined by a federal, state, tribal, or local government agency not to be suitable.

## **5. Administration; rule of construction**

A. The requirements of this condition are among those that must be included in any subaward (at any tier), and must be monitored. They apply as of the date of acceptance of this award, and throughout the remainder of the period of performance.

B. The recipient is to contact the DOJ awarding agency with any questions regarding the requirements of this condition and must not allow a covered individual to interact with a participating minor until such questions are answered.

C. Award funds may be obligated for the reasonable, necessary, and allocable costs (if any) of actions designed to ensure compliance with this condition, provided that such funds would not supplant non-federal funds that would otherwise be available for such costs.

D. Nothing in this condition shall be understood to authorize or require any recipient, any subrecipient at any tier, or any person or other entity, to violate any federal, state, tribal, or local law, including any applicable civil rights or nondiscrimination law.

## **6. OJP Suitability Process**

A. Members assigned to work under a OJP grant who may interact with participating minors shall undergo a suitability review conducted by the District Attorney's Bureau of Investigation (BI). Members will complete a suitability form that requires all addresses the member has resided in the past 5 years.

B. An assigned BI Background Investigator will complete all the required checks listed in under VIII., E.

C. Members will be required to complete a LiveScan process at the Sheriff's Office.

D. At the completion of the suitability check, the assigned Background Investigator will provide the completed suitability form, and the LiveScan report to the Admin Lieutenant who will in turn notify the members supervisor/manager of the results.

E. If the member is determined not to be suitable, as outlined in VIII., 4., that member will be removed from participating in the OJP grant program.

F. The suitability form, livescan report, and additional needed documents will be maintained in the members original background file and updated every 5 years.

Last updated: Feb 2025 NRT

## **DA Office Op Plan Template.pdf**

## **DA Office Op Plan Template.pdf**

## Operational Plan

Case Number	L/E Agency Case Number (if applicable)	Case Agent
-------------	----------------------------------------	------------

Briefing Date and Time	Operation Date and Time	Staging Area Date and Time	Staging Area Location
------------------------	-------------------------	----------------------------	-----------------------

### Type of Operation

Vehicle Stop ☐ Arrest Warrant ☐ CI Operation ☐  
U/C Operation ☐ Search Warrant ☐ Other ☐ \_\_\_\_\_

### Target Location/Assessment

Address	Telephone Number
---------	------------------

Description and GPS Coordinates (If applicable)

Physical Fortifications	<input type="checkbox"/>	Countersurveillance	<input type="checkbox"/>	Animals	<input type="checkbox"/>
Explosives	<input type="checkbox"/>	High Crime Area	<input type="checkbox"/>	Close Proximity to Schools	<input type="checkbox"/>
Children Present	<input type="checkbox"/>	Approach Difficulties	<input type="checkbox"/>	Vehicular Traffic Difficulties	<input type="checkbox"/>
High Level of Foot Traffic	<input type="checkbox"/>	Location Frequented By Public	<input type="checkbox"/>	Chemical/Bio Hazards	<input type="checkbox"/>
				Firearms Present at Target Location	<input type="checkbox"/>
Type of Door: _____				Opens: Right or Left	<input type="checkbox"/>
Occupants					

Occupants

## Operation Objectives

---

Case Background

---

Narrative:

**Suspect Information** *(Complete one for each suspect-additional Suspect Information forms are located at the end of this document)*

Suspect's Name	Date of Birth	Race	Sex
----------------	---------------	------	-----

Aliases

Description/Characteristics *(Height, Weight, Scars, Marks, Tattoos, Language proficiency, etc.)*

Ht:  
Wt:  
Eyes:  
Hair:

Home Address and Telephone Number	Work Address and Telephone Number
-----------------------------------	-----------------------------------

Other Addresses Used

Suspect(s) Known To Be Armed Yes <input type="checkbox"/> No <input type="checkbox"/>	Photograph Attached Yes <input type="checkbox"/> No <input type="checkbox"/>
------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------

Criminal History *(Arrests and Convictions)*  
Felony Arrests ☐ Felony Convictions ☐ History of Violence ☐ FBI Number \_\_\_\_\_

Describe:

**Additional Information**

Mental Illness _____	Substance Abuse _____	Specialized Training _____
Gang Affiliation _____	Anti-government _____	Other _____

**Suspect Vehicles**

Year	Make	Model	Color	License <i>(State)</i>	Other

**Undercover/Informant Information**

Name	Electronic Equipment	Radio Frequency	Vehicle Description	Description/Clothing

**Bust Signals**

Primary <i>(Audible)</i>	Secondary <i>(Visual)</i>	Trouble/Rip Off <i>(Audible)</i>	Trouble/Rip Off <i>(Visual)</i>



---

Tactical Plan (*Synopsis*)

---

This plan is a guide - This plan can be modified based on updated intelligence and on scene contingencies.

WSIN notified

Personnel and Assignments

Name	Radio Frequency	Pager or Cell Phone	Vehicle Call Sign	Assignment <i>(Primary/Secondary)</i>	Specialized Equipment
Name of Onscene Commander					
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					
21.					
22.					
23.					
24.					
25.					
26.					
27.					

**ABORT:** At any time during the operation, the On-Scene COMMANDER (OSC), lead investigator or any investigator may abort the operation for the safety of everyone involved.

**COMPROMISE:** If it is determined that the CTI has been compromised during the operation, the CTI will depart the area and travel to the staging area to meet with the cover team. If necessary, the cover team will extract the CTI using force.

**UNANTICIPATED MULTIPLE SUBJECTS:** In the event that multiple suspects (other than those anticipated) are present during the install, the OSC will evaluate the situation and determine if the operation is to be aborted or continued.

**HOSTAGE SITUATION:** In the event of a hostage situation, whether a civilian or law enforcement officer is taken hostage, the OSC will establish a perimeter. Once a perimeter has been established, the OSC will begin hostage negotiations and the local tactical team will be contacted. If the opportunity to rescue the hostage arises, the cover team will confront the threat(s) using force as necessary to extract the hostage.

**DOWNED INVESTIGATOR:** If during the operation any investigator/officer is injured, the injured person will be extracted in the most expeditious way possible while investigators/officers confront the threats using force as necessary.

**DOGS/ VICIOUS ANIMALS:** If during the enforcement operation a dog and/or other vicious animal is encountered and acts aggressively toward investigators/LEOs, OC will be used on the animal as a deterrent. If possible, lethal force against the animal will be used as a last option when all other attempts to control the animal have failed, and only if the investigators/LEOs fear that the animal poses danger to the safety of the investigators/LEOs and/or others. Note: Animal Control will be notified if further assistance is required.

**CHOKEHOLDS/CAROTID RESTRAINTS:** Chokeholds and carotid restraints are prohibited unless deadly force is authorized.

**DUTY TO INTERCEDE:** An Investigator must intercede when observing another investigator/law enforcement officer using force that is clearly beyond that which is objectively reasonable under the circumstances, when in a position to do so. Investigators should recognize that other investigators/ law enforcement officers may have additional information and different perspectives of the ongoing situation, and investigators must consider these possibilities when deciding whether to intercede. If they cannot act for whatever reason, they must immediately notify their supervisor.

**HOSTILE FIRE/ACTION:** If, during the installation, the team receives hostile fire, or is met with other hostile action, the team will immediately address the threat using force as necessary. The team will hold their position and ascertain the status of all team members. Investigators/Officers involved will report to/discuss all options with the on scene commander as soon as safely possible.

THIS OPERATIONAL PLAN IS A GUIDELINE THAT WILL BE FOLLOWED UNLESS CIRCUMSTANCES AND/OR SUSPECT(S) OR SUBJECT(S) DICTATE THAT THE TEAM ALTER THE PLAN IN A SAFER MANNER. THIS DECISION WILL BE MADE DURING THE OPERATION AND WILL BE BASED ON THE INFORMATION AVAILABLE AT THE TIME. USE ATTACHMENTS AS NECESSARY.

**Telephone Numbers**

Police Department Local Number	Chief Investigator (Cellular phone)	Case Agent
--------------------------------	-------------------------------------	------------

**Emergency Information**

Nearest Hospital/Trauma Center	Address	Emergency Room Telephone Number(s)
		Life Flight Telephone Number(s)

**Command Post**

Location	Telephone Number	Radio Frequency	Coordinator

Area Map/Diagram of Location Attached ☐

Firearms/Use of Force Policy Attached ☐

Intel Group Contacted ☐

Pursuit Policy Attached ☐

Plan Prepared By	Date
Plan Approved By	Date
Chief Investigator Approval	Date

## **Use of Deadly Force Policy**

### **General Principles**

1. The use of deadly force is only justified when the investigator reasonably believes it is necessary in the following circumstances (Penal Code section 835a):
  - a. An investigator may use deadly force to protect themselves or others from what the investigator reasonably believes is an imminent threat of death or serious bodily injury to the investigator or another person.
  - b. An investigator may use deadly force to apprehend a fleeing person for any felony that threatened or resulted in death or serious bodily injury, if the investigator reasonably believes that the person will cause death or serious bodily injury to another unless immediately apprehended.
  - c. An investigator should only discharge a firearm at a moving vehicle or its occupants when the investigator reasonably believes there are no other reasonable means available to avert the imminent threat of the vehicle, or if deadly force other than the vehicle is directed at the investigator or others (Government Code § 7286(b)).
  - d. Investigators should not shoot at any part of a vehicle in an attempt to disable the vehicle.
  - e. Where feasible, the investigator shall, prior to the use of deadly force, make reasonable efforts to identify themselves as a peace officer and to warn that deadly force may be used, unless the investigator has objectively reasonable grounds to believe the person is aware of those facts (Penal Code § 835a).
  - f. Warning shots shall not be used.
  - g. Officers will be trained in alternative methods and tactics for handling resisting subjects which must be used when the use of deadly force is not authorized by policy.

### **Emergency Driving and Pursuit Driving Policy**

Circumstances that may necessitate a high-speed pursuit or emergency response may include, but are not limited to, the threat of serious bodily injury or death to an agent or other party.

The following factors should be considered before driving at high speed or engaging in maneuvers that place anyone at risk of death or injury.

1. Severity of the offense or emergency
2. Probability of apprehending the violator (*s*) at a later time.
3. Weather and road conditions.
4. Availability of emergency equipment.

If the potential risk outweighs the benefits, the pursuit or response will not be initiated or will be terminated.

The use of roadblocks or ramming to stop a vehicle is a seizure under the fourth amendment, and must also be considered the potential use of deadly force, and therefore, should only be attempted when the use of such force is justified.

In any type of driving, investigators must have the utmost regard and respect for the safety of others.

### **Authorization of Otherwise Illegal Activity (OIA) by an Confidential Informant (CI)**

If this operation calls for a CI to be used to engage in any activity that would constitute a misdemeanor or felony under federal, state, or local law without authorization, such planned activity must be noted in the "Type of Operation" section of this form and the corresponding Chief Investigator name must be documented as the approving official.

Upon the Lieutenant's approval of the operational plan and subsequently the Chief approval, the CI is only then authorized to engage in the authorized activity.

Before commencing the operation, the CI's handler and another law enforcement witness are required to instruct the CI that he or she is only authorized to engage in the specific conduct and within the specific timeframes described in this operational plan.

Authorization reflects a finding by the Chief or Lieutenant that the operational planning process has reasonably included the safety of all persons involved, including the general public, and a finding that this activity is necessary either to:

- A. Obtain information or evidence essential for the success of an investigation that is not reasonably available without such authorization; or
- B. Prevent death, serious bodily injury, or significant damage to property; and
- C. That in the case of either A or B, the benefits to be obtained from the CI's participation outweigh the risks. Specific factors that should be considered in making this finding include the following: the risk of the CI exceeding the scope of the authorization, the risk of violence or financial loss, the extent of the CI's participation in the OIA, and the ability of the special agent to closely supervise the CI during the operation and to ensure that the CI does not profit from the OIA

## Operational Plan

Case Number		L/E Agency Case Number (if applicable)		Case Agent	
Briefing Date and Time		Operation Date and Time		Staging Area Date and Time	
Staging Area Location					
Type of Operation					
Vehicle Stop <input type="checkbox"/>		Arrest Warrant <input type="checkbox"/>		CI Operation <input type="checkbox"/>	
U/C Operation <input type="checkbox"/>		Search Warrant <input type="checkbox"/>		Other <input type="checkbox"/> _____	
Target Location/Assessment					
Address					Telephone Number
Description and GPS Coordinates ( <i>If applicable</i> )					
Physical Fortifications <input type="checkbox"/>					
Countersurveillance <input type="checkbox"/>		Animals <input type="checkbox"/>			
Explosives <input type="checkbox"/>		High Crime Area <input type="checkbox"/>		Close Proximity to Schools <input type="checkbox"/>	
Children Present <input type="checkbox"/>		Approach Difficulties <input type="checkbox"/>		Vehicular Traffic Difficulties <input type="checkbox"/>	
High Level of Foot Traffic <input type="checkbox"/>		Location Frequented By Public <input type="checkbox"/>		Chemical/Bio Hazards <input type="checkbox"/>	
				Firearms Present at Target Location <input type="checkbox"/>	
Type of Door: _____				Opens: Right or Left <input type="checkbox"/>	
Occupants					
Operation Objectives					

---

Case Background

---

Narrative:

**Suspect Information** *(Complete one for each suspect-additional Suspect Information forms are located at the end of this document)*

Suspect's Name	Date of Birth	Race	Sex
----------------	---------------	------	-----

Aliases

Description/Characteristics *(Height, Weight, Scars, Marks, Tattoos, Language proficiency, etc.)*

Ht:  
Wt:  
Eyes:  
Hair:

Home Address and Telephone Number	Work Address and Telephone Number
-----------------------------------	-----------------------------------

Other Addresses Used

Suspect(s) Known To Be Armed Yes <input type="checkbox"/> No <input type="checkbox"/>	Photograph Attached Yes <input type="checkbox"/> No <input type="checkbox"/>
------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------

Criminal History *(Arrests and Convictions)*  
Felony Arrests ☐ Felony Convictions ☐ History of Violence ☐ FBI Number \_\_\_\_\_

Describe:

**Additional Information**

Mental Illness \_\_\_\_\_ Substance Abuse \_\_\_\_\_ Specialized Training \_\_\_\_\_

Gang Affiliation \_\_\_\_\_ Anti-government \_\_\_\_\_ Other \_\_\_\_\_

**Suspect Vehicles**

Year	Make	Model	Color	License <i>(State)</i>	Other

**Undercover/Informant Information**

Name	Electronic Equipment	Radio Frequency	Vehicle Description	Description/Clothing

**Bust Signals**

Primary <i>(Audible)</i>	Secondary <i>(Visual)</i>	Trouble/Rip Off <i>(Audible)</i>	Trouble/Rip Off <i>(Visual)</i>

---

## Tactical Plan (*Synopsis*)

---

This plan is a guide - This plan can be modified based on updated intelligence and on scene contingencies.

WSIN notified



Personnel and Assignments

Name	Radio Frequency	Pager or Cell Phone	Vehicle Call Sign	Assignment (Primary/Secondary)	Specialized Equipment
Name of Onscene Commander					
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					
21.					
22.					
23.					
24.					
25.					
26.					
27.					

**ABORT:** At any time during the operation, the On-Scene COMMANDER (OSC), lead investigator or any investigator may abort the operation for the safety of everyone involved.

**COMPROMISE:** If it is determined that the CTI has been compromised during the operation, the CTI will depart the area and travel to the staging area to meet with the cover team. If necessary, the cover team will extract the CTI using force.

**UNANTICIPATED MULTIPLE SUBJECTS:** In the event that multiple suspects (other than those anticipated) are present during the install, the OSC will evaluate the situation and determine if the operation is to be aborted or continued.

**HOSTAGE SITUATION:** In the event of a hostage situation, whether a civilian or law enforcement officer is taken hostage, the OSC will establish a perimeter. Once a perimeter has been established, the OSC will begin hostage negotiations and the local tactical team will be contacted. If the opportunity to rescue the hostage arises, the cover team will confront the threat(s) using force as necessary to extract the hostage.

**DOWNED INVESTIGATOR:** If during the operation any investigator/officer is injured, the injured person will be extracted in the most expeditious way possible while investigators/officers confront the threats using force as necessary.

**DOGS/ VICIOUS ANIMALS:** If during the enforcement operation a dog and/or other vicious animal is encountered and acts aggressively toward investigators/LEOs, OC will be used on the animal as a deterrent. If possible, lethal force against the animal will be used as a last option when all other attempts to control the animal have failed, and only if the investigators/LEOs fear that the animal poses danger to the safety of the investigators/LEOs and/or others. Note: Animal Control will be notified if further assistance is required.

**CHOKEHOLDS/CAROTID RESTRAINTS:** Chokeholds and carotid restraints are prohibited unless deadly force is authorized.

**DUTY TO INTERCEDE:** An Investigator must intercede when observing another investigator/law enforcement officer using force that is clearly beyond that which is objectively reasonable under the circumstances, when in a position to do so. Investigators should recognize that other investigators/ law enforcement officers may have additional information and different perspectives of the ongoing situation, and investigators must consider these possibilities when deciding whether to intercede. If they cannot act for whatever reason, they must immediately notify their supervisor.

**HOSTILE FIRE/ACTION:** If, during the installation, the team receives hostile fire, or is met with other hostile action, the team will immediately address the threat using force as necessary. The team will hold their position and ascertain the status of all team members. Investigators/Officers involved will report to/discuss all options with the on scene commander as soon as safely possible.

THIS OPERATIONAL PLAN IS A GUIDELINE THAT WILL BE FOLLOWED UNLESS CIRCUMSTANCES AND/OR SUSPECT(S) OR SUBJECT(S) DICTATE THAT THE TEAM ALTER THE PLAN IN A SAFER MANNER. THIS DECISION WILL BE MADE DURING THE OPERATION AND WILL BE BASED ON THE INFORMATION AVAILABLE AT THE TIME. USE ATTACHMENTS AS NECESSARY.

#### Telephone Numbers

Police Department Local Number	Chief Investigator (Cellular phone)	Case Agent
--------------------------------	-------------------------------------	------------

#### Emergency Information

Nearest Hospital/Trauma Center	Address	Emergency Room Telephone Number(s)
		Life Flight Telephone Number(s)

#### Command Post

Location	Telephone Number	Radio Frequency	Coordinator

Area Map/Diagram of Location Attached ☐

Firearms/Use of Force Policy Attached ☐

Intel Group Contacted ☐

Pursuit Policy Attached ☐

Plan Prepared By	Date
Plan Approved By	Date
Chief Investigator Approval	Date

## **Use of Deadly Force Policy**

### **General Principles**

1. The use of deadly force is only justified when the investigator reasonably believes it is necessary in the following circumstances (Penal Code section 835a):
  - a. An investigator may use deadly force to protect themselves or others from what the investigator reasonably believes is an imminent threat of death or serious bodily injury to the investigator or another person.
  - b. An investigator may use deadly force to apprehend a fleeing person for any felony that threatened or resulted in death or serious bodily injury, if the investigator reasonably believes that the person will cause death or serious bodily injury to another unless immediately apprehended.
  - c. An investigator should only discharge a firearm at a moving vehicle or its occupants when the investigator reasonably believes there are no other reasonable means available to avert the imminent threat of the vehicle, or if deadly force other than the vehicle is directed at the investigator or others (Government Code § 7286(b)).
  - d. Investigators should not shoot at any part of a vehicle in an attempt to disable the vehicle.
  - e. Where feasible, the investigator shall, prior to the use of deadly force, make reasonable efforts to identify themselves as a peace officer and to warn that deadly force may be used, unless the investigator has objectively reasonable grounds to believe the person is aware of those facts (Penal Code § 835a).
  - f. Warning shots shall not be used.
  - g. Officers will be trained in alternative methods and tactics for handling resisting subjects which must be used when the use of deadly force is not authorized by policy.

### **Emergency Driving and Pursuit Driving Policy**

Circumstances that may necessitate a high-speed pursuit or emergency response may include, but are not limited to, the threat of serious bodily injury or death to an agent or other party.

The following factors should be considered before driving at high speed or engaging in maneuvers that place anyone at risk of death or injury.

1. Severity of the offense or emergency
2. Probability of apprehending the violator (s) at a later time.
3. Weather and road conditions.
4. Availability of emergency equipment.

If the potential risk outweighs the benefits, the pursuit or response will not be initiated or will be terminated.

The use of roadblocks or ramming to stop a vehicle is a seizure under the fourth amendment, and must also be considered the potential use of deadly force, and therefore, should only be attempted when the use of such force is justified.

In any type of driving, investigators must have the utmost regard and respect for the safety of others.

### **Authorization of Otherwise Illegal Activity (OIA) by an Confidential Informant (CI)**

If this operation calls for a CI to be used to engage in any activity that would constitute a misdemeanor or felony under federal, state, or local law without authorization, such planned activity must be noted in the "Type of Operation" section of this form and the corresponding Chief Investigator name must be documented as the approving official.

Upon the Lieutenant's approval of the operational plan and subsequently the Chief approval, the CI is only then authorized to engage in the authorized activity.

Before commencing the operation, the CI's handler and another law enforcement witness are required to instruct the CI that he or she is only authorized to engage in the specific conduct and within the specific timeframes described in this operational plan.

Authorization reflects a finding by the Chief or Lieutenant that the operational planning process has reasonably included the safety of all persons involved, including the general public, and a finding that this activity is necessary either to:

- A. Obtain information or evidence essential for the success of an investigation that is not reasonably available without such authorization; or
- B. Prevent death, serious bodily injury, or significant damage to property; and
- C. That in the case of either A or B, the benefits to be obtained from the CI's participation outweigh the risks. Specific factors that should be considered in making this finding include the following: the risk of the CI exceeding the scope of the authorization, the risk of violence or financial loss, the extent of the CI's participation in the OIA, and the ability of the special agent to closely supervise the CI during the operation and to ensure that the CI does not profit from the OIA

**Bail increase affidavit and  
order 2023B Template-Final.pdf**



## **Bail increase affidavit and order 2023B Template.pdf**



## **Driver Authorization and Performance Policy Employee Training Standards.pdf**



**Driver Authorization and Performance Policy  
Employee Training Standards**

Who Must Attend	Frequency of Training	Duration	Training Resource
All Full-Time, Extra-Help, Personal Services Contractors & Volunteers who drive on official County business.	<p>Defensive driver training must occur:</p> <ul style="list-style-type: none"> <li>Initial training completed no later than the first 12 months of employment or authorization to drive.</li> <li>Follow-up training at least once every four years.</li> <li>Additional training within 90-days of any “at fault” vehicle accident while on County business. In the event the employee is on a leave of absence, time may be extended. This training may also act as the employee’s follow-up training required every four years. Failure to comply may result in driving privileges being suspended.</li> </ul> <p>Departments may enforce stricter training policies based on the individual driving and training needs of the department. Failure to comply may result in driving privileges being suspended.</p>	Can range from one to four hours	<p>Classroom training (Risk Management)</p> <p>Law Enforcement - EVOC</p> <p>Online training (Target Solutions)</p>

**Training Content**

- Basic driver risk management; driving distance, correct hand position, vehicle safety inspection, handling a skidding vehicle, correct tire inflation, etc.
- Effective visual awareness
- Sharing the road
- Using speed and space effectively
- Distractions, drowsiness and emotions
- Driving in adverse conditions and driving emergencies
- The impact drugs and alcohol can have on a driver

\* Authorized Drivers that complete a POST certified defensive driving course are considered to be in compliance with the County’s training requirements.

## **Stanislaus County Motor Vehicle Accident Report.pdf**



**STANISLAUS COUNTY MOTOR VEHICLE ACCIDENT REPORT**  
CEO-RISK MANAGEMENT DIVISION FAX NUMBER 525-5779  
**PRIVILEGED AND CONFIDENTIAL ATTORNEY/CLIENT COMMUNICATION**

Place of Accident \_\_\_\_\_ Date of Accident \_\_\_\_\_ Time of Accident \_\_\_\_\_  
Accident Investigated by Police \_\_\_\_\_ CHP \_\_\_\_\_ Sheriff \_\_\_\_\_ Investigating Officer's Name \_\_\_\_\_ Report Number \_\_\_\_\_

**Vehicle Number One--County Driver (or Person Reporting)** NOTE: IT IS THE DRIVERS RESPONSIBILITY TO REPORT ACCIDENTS WITH DAMAGE OVER  
\$ 750.00 TO DMV ON FORM SR-1

Name \_\_\_\_\_ Home Address \_\_\_\_\_  
Home Phone \_\_\_\_\_ Work Phone \_\_\_\_\_ DOB \_\_\_\_\_ California Driver's License # \_\_\_\_\_  
Employee ID # \_\_\_\_\_ Dept. \_\_\_\_\_ Job Title \_\_\_\_\_  
Car Make \_\_\_\_\_ Type \_\_\_\_\_ Year \_\_\_\_\_ County Car # \_\_\_\_\_ Car License Plate \_\_\_\_\_  
Number of passengers \_\_\_\_\_ Name of Passenger \_\_\_\_\_ Name of Passenger \_\_\_\_\_  
Describe damages \_\_\_\_\_

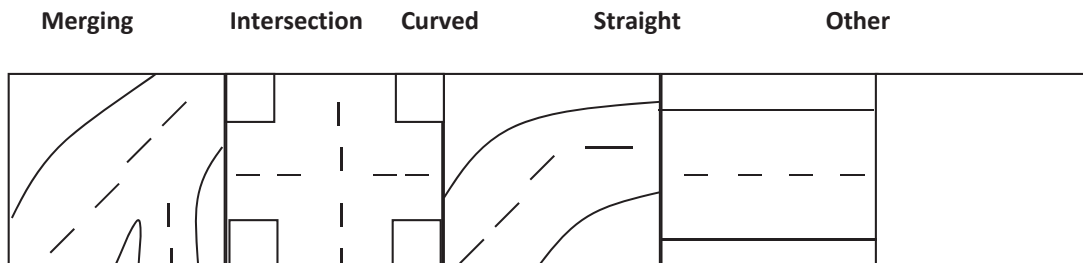
**Vehicle Number Two—Other Party** NOTE: REQUIRED INFORMATION INSURANCE CO. & POLICY # \_\_\_\_\_

Name \_\_\_\_\_ Home Address \_\_\_\_\_  
Home Phone \_\_\_\_\_ Work Phone \_\_\_\_\_ DOB \_\_\_\_\_ California Driver's License # \_\_\_\_\_  
Car Make \_\_\_\_\_ Type \_\_\_\_\_ Year \_\_\_\_\_ County Car # \_\_\_\_\_ Car License Plate \_\_\_\_\_  
Number of passengers \_\_\_\_\_ Name of Passenger \_\_\_\_\_ Name of Passenger \_\_\_\_\_  
Describe damages \_\_\_\_\_

Witness \_\_\_\_\_ Address \_\_\_\_\_ Phone \_\_\_\_\_  
Injured \_\_\_\_\_ Address \_\_\_\_\_ Phone \_\_\_\_\_  
Injured \_\_\_\_\_ Address \_\_\_\_\_ Phone \_\_\_\_\_

**Describe how the accident happened** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Diagram of Accident:** Choose the appropriate diagram below. Number the County Vehicle as 1 and the other vehicle as 2. Show the direction of travel by arrows. Use a solid line to show the path of the vehicles before the accident and a broken line for after the accident. Show a pedestrian with a circle, railroads with tracks, give names and numbers of streets and highways, indicate which way is north, and show traffic signs and signals.



I certify this report is complete and true to the best of my knowledge.

\_\_\_\_\_  
Driver's Signature Date

Supervisor: Check to make sure the report is complete. Review the diagram.

\_\_\_\_\_  
Supervisor's Signature Date

## **Application for Authorization to Drive on Official County Business Form.pdf**



## APPLICATION FOR AUTHORIZATION TO DRIVE ON OFFICIAL COUNTY BUSINESS

Date of Application: \_\_\_\_\_  
Add: ☐ Cancel: ☐ Change: ☐

Employee ID#				
Name (Last)	(First)	(Middle)	AKA (Last Name)	DOB
California Driver's License	License Class	License Expiration Date	Home Address (Street)	(City) (Zip Code)
Dept and Div	Job Classification	Restrictions to License (If none, write none)		
Frequency of Driving (to be completed by department)				
<input type="checkbox"/> Occasional (Employee drives less than once per month on average with a Class "C" license.)				
<input type="checkbox"/> Frequent (Employee drives once per month or more on average with a class "C" license <b>or</b> employees who are required to maintain a class "A", "B", <b>or</b> "C" license with a Hazardous Materials endorsement.)				
<input type="checkbox"/> Insurance Verified <input type="checkbox"/> Commercial Driver's License Required for Vehicle Operation		I hereby declare that I will: (a) Report immediately to my supervisor or department head all vehicle accidents on the job whenever I am the driver on forms provided by Risk Management. (b) Inform my supervisor or department head immediately in the event my driver's license is expired, suspended or revoked.  I understand that failure to do (a) and/or (b) above may result in disciplinary action up to and including termination.  Signature: _____		
Class A or B Medical Expiration Date: _____				

### APPOINTING AUTHORITY AUTHORIZATION

I hereby authorize the above named individual applicant to drive County or private vehicles in the performance of County business that is included in the driver's license class for which the individual is licensed. This authorization is automatically canceled in the event the above named individual's driver's license is expired, suspended or revoked.

\_\_\_\_\_  
(Type Name and Title)

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

### APPOINTING AUTHORITY CANCELLATION

I hereby cancel this authorization as of this date. (Signature) \_\_\_\_\_ (Title) \_\_\_\_\_ (Date) \_\_\_\_\_

**NOTE: UPON CANCELLATION, FORWARD TO CEO-RISK MGT DIV**

Copy – ☐ Department ☐ Original - CEO-Risk Management Division \_\_\_\_\_

### DRIVER'S PERMIT ID CARD

Name of Authorized Driver
Driver's Department and Division:
Name and Title of Appointing Authority:
Signature of Appointing Authority:

### INSTRUCTIONS

1. Appointing authority must sign and date application and ID Card.
2. Appointing authority provides copy to Risk Management and maintains a copy for Departments Records.
3. Appointing authority provides original signed copy to driver.
4. Upon cancellation, forward department's copy to Risk Management.

## **Photo Lineup Advisement.pdf**



# Office of the District Attorney Stanislaus County

**Birgit Fladager**  
**District Attorney**

**Assistant District Attorney**  
David P. Harris

**Chief Deputies**  
Annette Rees  
Marlisa Ferreira  
Stephen R. Robinson  
Jeffrey M. Laugero  
Jeff Mangar

**Bureau of Investigation**  
Chief Terry L. Seese

Case # \_\_\_\_\_

## **PHOTO LINEUP ADVISEMENT** **PC 859.7**

You will be asked to view a series of photos to determine if you can identify anyone as being involved in the offense you witnessed. The perpetrator may or may not be shown. The fact these photos are shown to you should not influence your judgement. You should not feel compelled to make an identification; it is just as important to free innocent persons from suspicion as to identify the perpetrator. An identification or failure to make an identification will not end the investigation. Keep in mind that hair styles, beards, and moustaches may be easily changed. Also, photos may not depict the true complexion of a person (their complexion may be lighter or darker than shown in the photo). Pay no attention to any markings or numbers that may appear on the pages with the photos or any other differences in the type, style, or background of the photos. After you have looked at all of the photos, tell me if you see the person involved in the offense. Please do not discuss the case with other witnesses or indicate in any way that you have or have not identified anyone.

Witness Name: \_\_\_\_\_ Signature: \_\_\_\_\_

Viewing Date: \_\_\_\_\_ Time: \_\_\_\_\_ Location: \_\_\_\_\_

Recording: ☐ Audio ☐ Video ☐ None (explain): \_\_\_\_\_

ID Confidence: ☐ Positive ☐ Possible ☐ None Person Identified: \_\_\_\_\_

Verbatim Witness Identification Statement: \_\_\_\_\_

Notes: \_\_\_\_\_

Investigator Name: \_\_\_\_\_ Signature: \_\_\_\_\_

Office: 832 12th Street, Suite 300 Modesto, CA 95354 Mailing: PO BOX 442 Modesto, CA 95353  
Telephone: (209) 525-5550 Fax: (209) 558-4027 www.stanislaus-da.org



<https://www.facebook.com/StanislausDistrictAttorney/>

## **SCDA Risk Assessment Matrix.pdf**



## SCDA Bureau of Investigation (BI) Risk Assessment

When preparing an operation plan, this assessment form shall be incorporated and used to evaluate the need for assistance from a Special Weapons and Tactics (S.W.A.T.) team. Any number of circumstances may demonstrate the need to use a S.W.A.T. team to protect and preserve the safety of all concerned. BI supervisors are encouraged to contact S.W.A.T. team leaders within the appropriate jurisdiction whenever questions arise concerning the evaluation of the listed criteria.

Type of Operation:	Location of Operation:
Prepared by / Date:	Case Number:

<b>Items 1-5 (Mark "YES" to 1 or more of the criteria listed below, S.W.A.T. should be consulted.)</b>	<b>YES</b>	<b>NO</b>	<b>If Yes, EXPLAIN / Provide Documentation if Possible</b>
1. Is the location fortified with reinforced security measures (i.e. "man traps", internal fortifications, multiple gates, steel doors, etc.)?			
2. Automatic weapons, explosives, body armor or military ordinance on the premises?			
3. Do the Suspect(s) have a history of assault on Peace Officers involving weapons?			
4. Based upon specific articulable facts, is there a likelihood of violent or armed confrontation?			
5. Related to a 664/187 or a 187 case and the suspect is believed to be present at the time of service.			

<b>Items 6-19 (Mark "Yes" to 3 or more of the criteria listed below, S.W.A.T. should be consulted.) Items 11-19 should only be answered "YES" if the suspect is expected to be or may be present at the time of service.</b>	<b>YES</b>	<b>NO</b>	<b>If Yes, EXPLAIN / Provide Documentation if Possible</b>
6. Large property with multiple out buildings.			
7. Vicious or guard dogs are expected to be present at the time of service.			
8. Known gang or drug house where multiple gang members/drug users may be present at the time of service.			
9. Sophisticated counter surveillance (i.e. Spotters, intrusion devices, etc.)?			
10. Related to a violent crime (not a 664/187 or a 187).			
11. Is there specific information that the suspect(s) have access to firearms or other deadly weapons?			
12. Is the suspect a 3 strikes candidate?			
13. The suspect has priors for using a firearm during the commission of a crime.			
14. Does the suspect have a propensity for violence?			
15. Does the suspect have a mental illness?			
16. Is the suspect unidentified?			

17. The suspect has a history of resisting arrest/evading?			
18. Suspect is a member of a gang, criminal organization or militant group.			
19. Suspect is prior law enforcement or Military			

Information and consideration only. No point value	YES	NO	If Yes, EXPLAIN / Provide Documentation if Possible
Children expected to be present. School district checked <a href="mailto:boutsikakis.j@monet.k12.ca.us">boutsikakis.j@monet.k12.ca.us</a> <a href="mailto:ramirez.ma@monet.k12.ca.us">ramirez.ma@monet.k12.ca.us</a> 209-550-3301 Ext.5557			
Suspect is on probation or Parole. Offense?			

<b>ORDER</b>	<b>TACTICS / DEPLOYMENT STRATEGIES</b>
	<b>Surveillance:</b> Observe the location for the suspect(s) to leave the premises, follow away and take into custody away from the location. At least the surveillance phase should be used in most cases. This provides good intelligence on what to expect at the location. Can be used in conjunction with other strategies. <b>Comments:</b>
	<b>Standard Service:</b> A perimeter is set, proper knock and notice is given and sufficient time is allowed for subjects to answer (if conditions permit, consider phoning into the location to seek compliance). Forced entry may be used if there is no response and no unusual circumstances are present, or if exigent circumstances develop. A deliberate, controlled and systematic clearing method is used. <b>Comments:</b>
	<b>Ruse:</b> Law Enforcement presence or intention is not initially revealed. Deception is used to trick suspect(s) into answering the door or coming outside so a safe entry can be made. Can be used in conjunction with other strategies. <b>Comments:</b>
	<b>Surround and Call-Out:</b> A surreptitious or visible perimeter is set on the location. A phone call, bullhorn or PA announcement is used to contact the suspect(s) inside. Suspect(s) are told the circumstances, ordered to surrender and ordered out of the location. Safest method, but evidence may be lost. If a standoff occurs, specialized units may be called into assist. May be used as a fallback strategy if other strategies are met with resistance. <b>Comments:</b>
	<b>Breach-and-Hold:</b> Breach outer most opening, so officers can see inside and order suspects to exit the location. Do not enter and search until the suspect(s) comply and the location is believed to be empty. Most likely to be used if entry under another strategy is compromised or safety concerns develop during an entry. <b>Comments:</b>
	<b>Dynamic Entry:</b> This strategy is rarely used (generally a SWAT tactic). This is different than a forced entry. A dynamic entry is a hard, fast entry with fluid clearing throughout the location. Most appropriate for a hostage/officer down rescue operation or active shooter situation where speed and violence of action are necessary to save lives or critically important evidence. <b>Comments:</b>

**\*\*Attach supporting documents (i.e. Reports, Warrants, RAPs, Probation / Parole Status, Photos, etc.)**

#### APPROVALS:

BI Lieutenant \_\_\_\_\_ CNT Commander \_\_\_\_\_

CRU Commander \_\_\_\_\_

SWAT Commander \_\_\_\_\_

## **Live Line Up and In Field Show Up Advisement Form.pdf**



# Office of the District Attorney Stanislaus County

**Birgit Fladager**  
**District Attorney**

**Assistant District Attorney**  
David P. Harris

**Chief Deputies**  
Annette Rees  
Marlisa Ferreira  
Stephen R. Robinson  
Jeffrey M. Laugero  
Jeff Mangar

**Bureau of Investigation**  
Chief Terry L. Seese

Case # \_\_\_\_\_

## **LIVE LINEUP / IN FIELD SHOW-UP ADVISEMENT** **PC 859.7**

You will be asked to view a person or persons to determine if you can identify anyone as being involved in the offense you witnessed. The perpetrator may or may not be shown. The fact these subjects are shown to you should not influence your judgement. You should not feel compelled to make an identification; it is just as important to free innocent persons from suspicion as to identify the perpetrator. An identification or failure to make an identification will not end the investigation. The fact these subjects may be in custody or handcuffed should not influence your judgement. After you have looked at all of the subjects, tell me if you see the person involved in the offense. Please do not discuss the case with other witnesses or indicate in any way that you have or have not identified anyone.

Witness Name: \_\_\_\_\_ Signature: \_\_\_\_\_

Viewing Date: \_\_\_\_\_ Time: \_\_\_\_\_ Location: \_\_\_\_\_

Recording: ☐ Audio ☐ Video ☐ None (explain): \_\_\_\_\_

ID Confidence: ☐ Positive ☐ Possible ☐ None Person Identified: \_\_\_\_\_

Verbatim Witness Identification Statement: \_\_\_\_\_

\_\_\_\_\_

Notes: \_\_\_\_\_

Investigator Name: \_\_\_\_\_ Signature: \_\_\_\_\_

Office: 832 12th Street, Suite 300 Modesto, CA 95354 Mailing: PO BOX 442 Modesto, CA 95353  
Telephone: (209) 525-5550 Fax: (209) 558-4027 [www.stanislaus-da.org](http://www.stanislaus-da.org)



<https://www.facebook.com/StanislausDistrictAttorney/>

## **UOF Review Blank Example.pdf**



# Office of the District Attorney Stanislaus County

**Birgit Fladager**  
District Attorney

**Assistant District Attorney**  
David P. Harris

**Chief Deputies**  
Annette Rees  
Marlisa Ferreira  
Stephen R. Robinson  
Jeffrey M. Laugero  
Jeff Mangar

**Bureau of Investigation**  
Chief Terry L. Seese

---

## MEMORANDUM

**To: Chief Investigator**

**From: Lieutenant**

**Date:**

**Subject: UOF Review**

---

**Case Number:**

**Date/Time of Incident:**

**Involved DAI and Officers:**

**Summary of Incident:**

**Disposition (arrest, citation), Including Arrestee Information:**

**Injuries/Property Damage:**

**Medical Treatment:**

**Name of Supervisor Over Incident:**

**Conclusion:**

**Training Issues Identified:**

**Recommendation:**

Office: 832 12th Street, Suite 300 Modesto, CA 95354 Mailing: PO BOX 442 Modesto, CA 95353  
Telephone: (209) 525-5550 Fax: (209) 558-4027 [www.stanislaus-da.org](http://www.stanislaus-da.org)



<https://www.facebook.com/StanislausDistrictAttorney/>

\_\_\_\_\_  
Lieutenant

Date: \_\_\_\_\_

\_\_\_\_\_  
Criminal Investigator

Date: \_\_\_\_\_

Office: 832 12th Street, Suite 300 Modesto, CA 95354 Mailing: PO BOX 442 Modesto, CA 95353  
Telephone: (209) 525-5550 Fax: (209) 558-4027 www.stanislaus-da.org



<https://www.facebook.com/StanislausDistrictAttorney/>

## **Hate Crime Checklist.pdf**



# HATE CRIME CHECKLIST

Page \_\_\_\_\_ of \_\_\_\_\_

<b>VICTIM</b>	<p style="text-align: center;"><b><u>Victim Type:</u></b></p> <p><input type="checkbox"/> <b>Individual</b> Legal name (Last, First): _____ Other Names used (AKA): _____</p> <p><input type="checkbox"/> <b>School, business or organization</b> Name: _____ Type: _____ <small>(e.g., non-profit, private, public school)</small> Address: _____</p> <p><input type="checkbox"/> <b>Faith-based organization</b> Name: _____ Faith: _____ Address: _____</p>	<p style="text-align: center;"><b><u>Target of Crime (Check all that apply):</u></b></p> <p><input type="checkbox"/> Person    <input type="checkbox"/> Private property    <input type="checkbox"/> Public property</p> <p><input type="checkbox"/> Other _____</p> <p style="text-align: center;"><b><u>Nature of Crime (Check all that apply):</u></b></p> <p><input type="checkbox"/> Bodily injury                      <input type="checkbox"/> Threat of violence</p> <p><input type="checkbox"/> Property damage</p> <p><input type="checkbox"/> Other crime: _____</p> <p>Property damage - estimated value _____</p>
<b>BIAS</b>	<p style="text-align: center;"><b><u>Type of Bias</u></b> <b><u>(Check all characteristics that apply):</u></b></p> <p><input type="checkbox"/> Disability</p> <p><input type="checkbox"/> Gender</p> <p><input type="checkbox"/> Gender identity/expression</p> <p><input type="checkbox"/> Sexual orientation</p> <p><input type="checkbox"/> Race</p> <p><input type="checkbox"/> Ethnicity</p> <p><input type="checkbox"/> Nationality</p> <p><input type="checkbox"/> Religion</p> <p><input type="checkbox"/> Significant day of offense <small>(e.g., 9/11, holy days)</small></p> <p><input type="checkbox"/> Other: _____</p> <p>Specify disability (be specific): _____ _____</p>	<p style="text-align: center;"><b><u>Actual or Perceived Bias – Victim’s Statement:</u></b></p> <p><input type="checkbox"/> Actual bias [Victim actually has the indicated characteristic(s)].</p> <p><input type="checkbox"/> Perceived bias [Suspect believed victim had the indicated characteristic(s)]. <i>If perceived, explain the circumstances in narrative portion of Report.</i></p> <hr/> <p style="text-align: center;"><b><u>Reason for Bias:</u></b></p> <p><b>Do you feel you were targeted based on one of these characteristics?</b> <input type="checkbox"/> Yes    <input type="checkbox"/> No    <i>Explain in narrative portion of Report.</i></p> <p><b>Do you know what motivated the suspect to commit this crime?</b> <input type="checkbox"/> Yes    <input type="checkbox"/> No    <i>Explain in narrative portion of Report.</i></p> <p><b>Do you feel you were targeted because you associated yourself with an individual or a group?</b> <input type="checkbox"/> Yes    <input type="checkbox"/> No    <i>Explain in narrative portion of Report.</i></p> <p><b>Are there indicators the suspect is affiliated with a Hate Group (i.e., literature/tattoos)?</b> <input type="checkbox"/> Yes    <input type="checkbox"/> No    <i>Describe in narrative portion of Report.</i></p> <p><b>Are there Indicators the suspect is affiliated with a criminal street gang?</b> <input type="checkbox"/> Yes    <input type="checkbox"/> No    <i>Describe in narrative portion of Report.</i></p>
	<p style="text-align: center;"><b><u>Bias Indicators (Check all that apply):</u></b></p> <p><input type="checkbox"/> Hate speech                      <input type="checkbox"/> Acts/gestures                      <input type="checkbox"/> Property damage                      <input type="checkbox"/> Symbol used</p> <p><input type="checkbox"/> Written/electronic communication                      <input type="checkbox"/> Graffiti/spray paint                      <input type="checkbox"/> Other: _____</p> <p><i>Describe with exact detail in narrative portion of Report.</i></p>	
<b>HISTORY</b>	<p style="text-align: center;"><b><u>Relationship Between Suspect &amp; Victim:</u></b></p> <p>Suspect known to victim?    <input type="checkbox"/> Yes    <input type="checkbox"/> No</p> <p>Nature of relationship: _____</p> <p>Length of relationship: _____</p> <p><i>If Yes, describe in narrative portion of Report</i></p>	<p><input type="checkbox"/> Prior reported incidents with suspect? Total # _____</p> <p><input type="checkbox"/> Prior unreported incidents with suspect? Total # _____</p> <p>Restraining orders?    <input type="checkbox"/> Yes    <input type="checkbox"/> No</p> <p><i>If Yes, describe in narrative portion of Report</i></p> <p>Type of order: _____    Order/Case# _____</p>
<b>WEAPONS</b>	<p>Weapon(s) used during incident?    <input type="checkbox"/> Yes    <input type="checkbox"/> No    Type: _____</p> <p>Weapon(s) booked as evidence?    <input type="checkbox"/> Yes    <input type="checkbox"/> No</p> <p>Automated Firearms System (AFS) Inquiry attached to Report?    <input type="checkbox"/> Yes    <input type="checkbox"/> No</p>	

# HATE CRIME CHECKLIST

Page \_\_\_\_\_ of \_\_\_\_\_

<b>EVIDENCE</b>	Witnesses present during incident? <input type="checkbox"/> Yes <input type="checkbox"/> No		Statements taken? <input type="checkbox"/> Yes <input type="checkbox"/> No	
	Evidence collected? <input type="checkbox"/> Yes <input type="checkbox"/> No Photos taken? <input type="checkbox"/> Yes <input type="checkbox"/> No Total # of photos: _____ D#: _____ Taken by: _____ Serial #: _____		Recordings: <input type="checkbox"/> Video <input type="checkbox"/> Audio <input type="checkbox"/> Booked Suspect identified: <input type="checkbox"/> Field ID <input type="checkbox"/> By photo <input type="checkbox"/> Known to victim	

<b>OBSERVATIONS</b>	<u><b>VICTIM</b></u>	<u><b>SUSPECT</b></u>
	<input type="checkbox"/> Tattoos <input type="checkbox"/> Shaking <input type="checkbox"/> Unresponsive <input type="checkbox"/> Crying <input type="checkbox"/> Scared <input type="checkbox"/> Angry <input type="checkbox"/> Fearful <input type="checkbox"/> Calm <input type="checkbox"/> Agitated <input type="checkbox"/> Nervous <input type="checkbox"/> Threatening <input type="checkbox"/> Apologetic <input type="checkbox"/> Other observations: _____	<input type="checkbox"/> Tattoos <input type="checkbox"/> Shaking <input type="checkbox"/> Unresponsive <input type="checkbox"/> Crying <input type="checkbox"/> Scared <input type="checkbox"/> Angry <input type="checkbox"/> Fearful <input type="checkbox"/> Calm <input type="checkbox"/> Agitated <input type="checkbox"/> Nervous <input type="checkbox"/> Threatening <input type="checkbox"/> Apologetic <input type="checkbox"/> Other observations: _____
	<u><b>ADDITIONAL QUESTIONS (Explain all boxes marked "Yes" in narrative portion of report):</b></u>	
	Has suspect ever threatened you? <input type="checkbox"/> Yes <input type="checkbox"/> No Has suspect ever harmed you? <input type="checkbox"/> Yes <input type="checkbox"/> No Does suspect possess or have access to a firearm? <input type="checkbox"/> Yes <input type="checkbox"/> No Are you afraid for your safety? <input type="checkbox"/> Yes <input type="checkbox"/> No Do you have any other information that may be helpful? <input type="checkbox"/> Yes <input type="checkbox"/> No	
<u><b>Resources offered at scene:</b></u> <input type="checkbox"/> Yes <input type="checkbox"/> No Type: _____		

<b>MEDICAL</b>	<table style="width: 100%;"> <tr> <th style="text-align: left;"><u>Victim</u></th> <th style="text-align: left;"><u>Suspect</u></th> <th></th> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td>Declined medical treatment</td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td>Will seek own medical treatment</td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td>Received medical treatment</td> </tr> </table> Authorization to Release Medical Information, Form 05.03.00, signed? <input type="checkbox"/> Yes <input type="checkbox"/> No	<u>Victim</u>	<u>Suspect</u>		<input type="checkbox"/>	<input type="checkbox"/>	Declined medical treatment	<input type="checkbox"/>	<input type="checkbox"/>	Will seek own medical treatment	<input type="checkbox"/>	<input type="checkbox"/>	Received medical treatment	<b>Paramedics at scene?</b> <input type="checkbox"/> Yes <input type="checkbox"/> No Unit # _____ Name(s)/ID #: _____ Hospital: _____ Jail Dispensary: _____ Physician/Doctor: _____ Patient #: _____
	<u>Victim</u>	<u>Suspect</u>												
<input type="checkbox"/>	<input type="checkbox"/>	Declined medical treatment												
<input type="checkbox"/>	<input type="checkbox"/>	Will seek own medical treatment												
<input type="checkbox"/>	<input type="checkbox"/>	Received medical treatment												

Officer (Name/Rank)	Date
Officer (Name/Rank)	Date
Supervisor Approving (Name/Rank)	Date

## **SCDA Ops Plan.pdf**

## **Military Equipment Attachment.pdf**

**Questionnaire from LA Cty  
CertificateRehabandPardonPacket.pdf**

**DISTRICT ATTORNEY  
BUREAU OF INVESTIGATIONS**

**REHABILITATION AND PARDON INFORMATION SHEET**

In order that the investigation requested by the petition seeking a Rehabilitation and Pardon be completed in a timely fashion your assistance in providing the following information is requested.

1. Case number or numbers petitioner is seeking rehabilitation for:

---

---

---

2. What was the petitioner charged with?

---

---

---

3. Conviction date for each case applying for:

---

---

---

4. Date petitioner placed on parole or probation for each case:

---

---

---

5. C.I.I. number for petitioner: \_\_\_\_\_

6. What is petitioner's 1203.4 P.C. date? \_\_\_\_\_

**PLEASE NOTIFY THIS OFFICE BY MAIL OF ANY ADDRESS CHANGES:**

STANISLAUS COUNTY DISTRICT ATTORNEY  
ATTN: BUREAU OF INVESTIGATIONS  
832 12TH STREET  
MODESTO, CA 95351

**NOTE:** The attached Rehabilitation and Pardon form must be completely filled out in detail when submitted or the questionnaire will be returned to you for completion. This will delay your court date.

I acknowledge receipt of this rehabilitation and pardon information package.

X \_\_\_\_\_  
Petitioner's Signature

Legal Name \_\_\_\_\_  
Last First Middle

What other names have you used \_\_\_\_\_

If married, maiden name \_\_\_\_\_

Residence Address \_\_\_\_\_  
Number Street  
City County Zip Code

How long have you lived at this address \_\_\_\_\_

Nearest large intersection \_\_\_\_\_

Res. phone \_\_\_\_\_ Bus. phone \_\_\_\_\_

U.S. Citizen Yes \_\_\_\_\_ No \_\_\_\_\_

Are you a legal resident of the United States: Yes \_\_\_\_\_ No \_\_\_\_\_

If alien resident of the United States, what is your Alien Registration Number

\_\_\_\_\_

Birthplace \_\_\_\_\_ Birth date \_\_\_\_\_ Sex \_\_\_\_\_  
City State

Height \_\_\_\_\_ Weight \_\_\_\_\_ Hair \_\_\_\_\_ Eyes \_\_\_\_\_ Decent \_\_\_\_\_ Race \_\_\_\_\_

Driver's License Number \_\_\_\_\_

Social Security Number \_\_\_\_\_

Present Marital Status ☐ Single ☐ Married ☐ Divorced ☐ Widow(er)

Date Marriage Performed \_\_\_\_\_  
Month / Date/ Year City State

Living with Spouse: Yes \_\_\_\_\_ No \_\_\_\_\_

Spouse's Name \_\_\_\_\_ Birthdate \_\_\_\_\_  
Month / Date/ Year

Height \_\_\_\_\_ Weight \_\_\_\_\_ Hair \_\_\_\_\_ Eyes \_\_\_\_\_ Decent \_\_\_\_\_ Race \_\_\_\_\_

Circle Last Grade Completed

**Grammar School** 5 6 7 8 **High School** 9 10 11 12 **College** 1 2 3 4 5 6



Employment: List employments since your release.

(Last or Present)

Date (From – To)		Name of Employer		Phone	
Number	Street	City	State	Zip Code	
Department		Job Title	Annual Salary	Immediate Supervisor	
Reason for Leaving					

(Previous)

Date (From – To)		Name of Employer		Phone	
Number	Street	City	State	Zip Code	
Department		Job Title	Annual Salary	Immediate Supervisor	
Reason for Leaving					

(Previous)

Date (From – To)		Name of Employer		Phone	
Number	Street	City	State	Zip Code	
Department		Job Title	Annual Salary	Immediate Supervisor	
Reason for Leaving					

## **2022-10-03 Military Equipment Attachment.pdf**

**INVENTORY ATTACHMENT**  
**POLICY 706 MILITARY EQUIPMENT**

The following is a list of military equipment as defined by Government Code §7070 held/maintained by the Stanislaus County District Attorney's Office Bureau of Investigation

## **A. MILITARY EQUIPMENT**

**1. Unmanned Aircraft System (UAS)**- An unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV) and all supporting or attached systems designed for gathering information through imaging, recording or any other means.

### a. Description, quantity, capabilities, and purchase cost

#### **i. DJI Phantom IV cost: \$2000 quantity: 1**

Drone assigned to the Regional Fire Investigation Unit. Drone is equipped with camera and has a flight time of 30 minutes. Purchased through Less Than County Wide Tax.

#### **ii. DJI Mavic II cost: \$3500 quantity: 4**

Drone assigned to the Regional Fire Investigation Unit. Drone is equipped with infrared camera and has a flight time of 30 minutes. Purchased through Less than County Wide Tax.

### b. Purpose

i. To be deployed when its view would assist with the following situations including but not limited to

1. Search for missing persons
2. Major Collision investigations
3. Natural Disaster Management
4. Crime Scene Photography
5. Tactical or other public safety and life preservation missions
6. Response to specific requests from local, state, or federal authorities for fire response, investigation, and or prevention.

### c. Authorized Use

Only assigned operators who have completed the required training shall be permitted to operate drones during approved missions.

### d. Expected Life Span

All UAS equipment, approximately 5-7 years

### e. Fiscal Impact

Annual maintenance is approximately \$2,500

f. Training

All UAS operators are licensed by the Federal Aviation Administration (FAA) for UAS operation.

g. Legal and Procedural Rules

Use is established by the Stanislaus County District Attorney Bureau of Investigation Lexipol Policy 606 (Drone Policy) and FAA Regulation 14 CFR Part 107

**2. Rifles and Ammunition-** Shoulder mounted firearms allowing greater precision and accuracy at long distances. These may be department owned or privately owned weapons authorized for agency use

a. Description, quantity, capabilities, and purchase cost

**i. Colt M4 Rifle, Cost: \$1,200 per rifle: Quantity: 9**

Semi-automatic rifle that fires .223/5.56mm cartridge. Equipped with red-dot sights, weapon mounted lights and suppressors.

**ii. Colt LE6933 Rifle, Cost: \$1,200: Quantity: 3**

Semi-automatic rifle that fires .223/5.56mm cartridge. Equipped with red-dot sights, weapon mounted lights and suppressors.

**iii. Colt AR15 Rifle, Cost: \$1,200 Quantity: 1**

Semi-automatic rifle that fires .223/5.56mm cartridge.

**iv. Bushmaster XM15 Rifle, Cost: \$800, Quantity: 1**

Semi-automatic rifle that fires .223/5.56mm cartridge.

**v. PWA AR15 Rifle, Cost: \$2,000, Quantity: 1**

Semi-automatic rifle that fires .223/5.56mm cartridge.

**vi. Federal FMJ 55 grain .223 ammunition, Cost: \$.40 per round, Quantity: 5,800**

Rifle ammunition, used for training and qualification.

**vii. Hornady FMJ 55 grain .223 ammunition, Cost: \$.40 per round, Quantity: 1,900**

Rifle ammunition, used for training and qualification.

**vii. Hornady TAP 60 grain .223 ammunition, Cost: \$.60 per round Quantity: 140**

Rifle ammunition, used for duty.

**ix. Speer GDSP 62 grain .223 ammunition, Cost: \$.60 per round Quantity: 240**

Rifle ammunition used for duty.

b. Purpose

Rifles and rifle ammunition are used to address a threat with more precision and accuracy than a handgun

c. Authorized Use

Only sworn personnel that are POST-certified are authorized to deploy rifles

d. Expected Life Span

Rifles-25 years

Ammunition-10 years

e. Fiscal Impact

Annual maintenance is approximately \$20 for each rifle

f. Training

Prior to deploying a rifle, sworn personnel must be certified by POST instructors in the operation of the rifle. All members that operate any rifle are required to pass a range qualification twice a year

g. Legal and Procedural Rules

Use is established by the Stanislaus County District Attorney Bureau of Investigation Lexipol Policy 300 (Use of Force) and 306 (Firearms).

**3. Less Lethal Shotgun-** Used to deploy a less lethal 12-gauge drag stabilized beanbag round.

a. Description, quantity, capabilities, and purchase cost

**i. Remington 870 Less lethal shotgun, Cost: \$800 quantity: 1**

Remington 870 12-gauge shotgun with orange buttstock and fore end.

**ii. Mossberg 500 Less lethal shotgun, Cost: \$600 quantity: 1**

Mossberg 500 12-gauge shotgun with orange buttstock and fore end.

**iii. CTS 12 Gauge Super-Sock Bean Bag Impact Round, Cost \$7.10 per round quantity: 150.** Drag stabilized beanbag round for use in designated beanbag shotgun.

b. Purpose

To limit the escalation of conflict where use of lethal force is prohibited or undesirable.

c. Authorized Use

- Situations for use of the less lethal weapon systems may include, but are not limited to
- Self-destructive, dangerous and or combative individuals.
- Riots and incidences of violent criminal behavior
- Circumstances where a tactical advantage can be obtained.
- Vicious Animals

d. Expected Life Span

Less lethal shotgun- 20 years  
Beanbag round- 5 years

e. Fiscal impact

Annual maintenance is approximately \$20 per shotgun.

f. Training

All sworn personnel are trained in the 12-gauge less lethal shotgun by in service training

g. Legal Procedures

Use is established by the Stanislaus County District Attorney Bureau of Investigation  
Lexipol Policy 300 (Use of Force) and 306(Firearms).

**INVENTORY ATTACHMENT**  
**POLICY 706 MILITARY EQUIPMENT**



The following is a list of military equipment as defined by Government Code §7070 held/maintained by the Stanislaus County District Attorney's Office Bureau of Investigation

## **A. MILITARY EQUIPMENT**

**1. Unmanned Aircraft System (UAS)**- An unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV) and all supporting or attached systems designed for gathering information through imaging, recording or any other means.

a. Description, quantity, capabilities, and purchase cost

**i. DJI Phantom IV cost: \$2,000 quantity: 1**

Drone assigned to the Regional Fire Investigation Unit. Drone is equipped with camera and has a flight time of 30 minutes. Purchased through Less Than County Wide Tax.

**ii. DJI Mavic II cost: \$3,500 quantity: 4**

Drone assigned to the Regional Fire Investigation Unit. Drone is equipped with infrared camera and has a flight time of 30 minutes. Purchased through Less than County Wide Tax.

b. Purpose

i. To be deployed when its view would assist with the following situations including but not limited to

1. Search for missing persons
2. Major Collision investigations
3. Natural Disaster Management
4. Crime Scene Photography
5. Tactical or other public safety and life preservation missions
6. Response to specific requests from local, state, or federal authorities for fire response, investigation, and or prevention.

c. Authorized Use

Only assigned operators who have completed the required training shall be permitted to operate drones during approved missions.

d. Expected Life Span

All UAS equipment, approximately 5-7 years

e. Fiscal Impact

Annual maintenance is approximately \$2,500

f. Training

All UAS operators are licensed by the Federal Aviation Administration (FAA) for UAS operation.

g. Legal and Procedural Rules

Use is established by the Stanislaus County District Attorney Bureau of Investigation Lexipol Policy 606 (Drone Policy) and FAA Regulation 14 CFR Part 107

**2. Less Lethal Shotgun-** Used to deploy a less lethal 12-gauge drag stabilized beanbag round.

a. Description, quantity, capabilities, and purchase cost

**i. Mossberg 590 Less lethal shotgun, Cost: \$600 quantity: 2**

Mossberg 500 12-gauge shotgun with orange buttstock and fore end.

**ii. CTS 12 Gauge Super-Sock Bean Bag Impact Round, Cost \$7.10 per round quantity: 150.** Drag stabilized beanbag round for use in designated beanbag shotgun.

b. Purpose

To limit the escalation of conflict where use of lethal force is prohibited or undesirable.

c. Authorized Use

- Situations for use of the less lethal weapon systems may include, but are not limited to
- Self-destructive, dangerous and or combative individuals.
- Riots and incidences of violent criminal behavior
- Circumstances where a tactical advantage can be obtained.
- Vicious Animals

d. Expected Life Span

Less lethal shotgun- 20 years  
Beanbag round- 5 years

e. Fiscal impact

Annual maintenance is approximately \$20 per shotgun.

f. Training

All sworn personnel are trained in the 12-gauge less lethal shotgun by in service training

g. Legal Procedures

Use is established by the Stanislaus County District Attorney Bureau of Investigation Lexipol Policy 300 (Use of Force) and 306(Firearms).

## **2020-05-11 SCDA Ops Plan.pdf**



# Office of the District Attorney Stanislaus County

Birgit Fladager  
District Attorney

Assistant District Attorney  
Dave Harris

Chief Deputies  
Annette Rees  
Marlisa Ferreira  
Stephen R. Robinson  
Jeffrey M. Laugero  
Jeff Mangar

Chief Investigator  
Terry L. Seese

## TACTICAL OPERATIONS PLAN

DATE/TIME: CASE# CASE AGENT:

SWAT Consultation: Yes ☐ No ☐

Risk Assessment Matrix shall be attached to this operations plan

### TYPE OF OPERATION:

- |                                              |                                         |                                           |                                        |
|----------------------------------------------|-----------------------------------------|-------------------------------------------|----------------------------------------|
| <input type="checkbox"/> Surveillance        | <input type="checkbox"/> Search Warrant | <input type="checkbox"/> U/C Op           | <input type="checkbox"/> C/I buy       |
| <input type="checkbox"/> Knock and talk      | <input type="checkbox"/> Arrest         | <input type="checkbox"/> Probation Search | <input type="checkbox"/> Parole Search |
| <input type="checkbox"/> Enforcement Op      | <input type="checkbox"/> Flash          | <input type="checkbox"/> Reverse          |                                        |
| <input type="checkbox"/> Controlled Delivery | <input type="checkbox"/> Buy/Bust       |                                           |                                        |

### CASE BACKGROUND:

Write a brief narrative of the type of case and what the operation is: Search warrant, surveillance (for what), arrest warrant- take down etc...

### OPERATIONAL OBJECTIVE(s):

A SAFE SUCCESSFUL OPERATION FOR ALL INVOLVED IS OUR PRIMARY OBJECTIVE.

- 1.
- 2.
- 3.
- 4.

All MPD and Stanislaus County DA personnel will follow their respective policies.

### LOCATION(s):

List address and provide a photo

### SUBJECT(s):

- 1.
- 2.
- 3.

**OUTSIDE AGENCY OPERATIONS PERSONNEL:**

Personnel	Agency	Call Sign	Cell Phone	Vehicle	Assignment
					Supervisor
					Entry
					Entry

**STANISLAUS D.A. PERSONNEL:**

Personnel	Agency	Call Sign	Cell Phone	Vehicle	Assignment

**AGENCY PHONE NUMBERS:**

<b>Stan. Co S/O</b>	<b>209-525-7914</b>	<b>Modesto PD</b>	<b>209-572-9595</b>	<b>Ceres PD</b>	<b>209-538-5713</b>
Turlock PD	209-668-1200	Oakdale PD	209-847-2231	Merced PD	209-385-6907
Merced S/O	209-385-7445	Hughson PD	209-883-4052	Riverbank PD	209-869-2572
Manteca PD	209-239-8042	Waterford PD	209-874-2349	Patterson PD	209-575-9780
SDEA	209-558-6300	StanCATT	209-545-7316	Stanislaus DA	209-525-5550

**Operational Codes / UC Information:**

None.

**Communications:**Primary Radio Channel: **Comm with MPD Channel 1**Secondary/Emergency Radio Channel: **MPD Channel 2****Caution Statement:**

- 1. Weapons ☐
- 2. Violent History ☐
- 3. Fortifications ☐
- 4. Guard dogs/Animals ☐
- 5. Surveillance Equipment ☐
- 6. Children/Elderly ☐

**Additional:**

- 1. Rap sheets ☐
- 2. Photos attached ☐
- 3. Premise History ☐
- 4. Maps/Diagrams attached ☐
- 5. Risk Assessment Matrix ☐
- 6. Undercover Ops Risk Analysis ☐

7. Mental Conditions ☐

7. Animal Mitigation Plan ☐

**Notifications:**

1. WSIN	916-263-1166	Notified By:	
2. LA CLEAR	877-550-2532	Notified By:	Date/Time:
3. Comm Center	209-572-9595	Notified By:	Date/Time:
4. Watch Cmdr.	209-572-9584	Notified By:	Date/Time:

**Individual Equipment**

<input type="checkbox"/> BDUs	<input type="checkbox"/> Ballistic Vests	<input type="checkbox"/> Helmet	<input type="checkbox"/> Raid Vest	<input type="checkbox"/> Eye Protection
<input type="checkbox"/> OC Spray	<input type="checkbox"/> Portable Radio	<input type="checkbox"/> Flashlight	<input type="checkbox"/> Handcuffs	<input type="checkbox"/> Baton
<input type="checkbox"/> Handgun	<input type="checkbox"/> Rifle	<input type="checkbox"/> Gloves	<input type="checkbox"/> Lab Gear	<input type="checkbox"/> Mirror
<input type="checkbox"/> Other				

**Specialized Equipment**

<input type="checkbox"/> Shield	<input type="checkbox"/> Cutters	<input type="checkbox"/> Hooligan	<input type="checkbox"/> Pry Bar	<input type="checkbox"/> Ram
<input type="checkbox"/> 35mm Camera	<input type="checkbox"/> Digital Camera	<input type="checkbox"/> Video Camera	<input type="checkbox"/> Evidence Kit	<input type="checkbox"/> Sledge
<input type="checkbox"/> Aircraft	<input type="checkbox"/> Night Vision	<input type="checkbox"/> Flir	<input type="checkbox"/> Other	

**Hospitals:**

**Doctor's Medical Center**  
1441 Florida Avenue  
Modesto, CA  
(209) 578-1211

**Memorial Hospital**  
1700 Coffee Road  
Modesto, CA  
(209) 526-4500

**SUPERVISOR'S AUTHORIZATION TO PROCEED:**

\_\_\_\_\_  
LIEUTENANT SIGNATURE

\_\_\_\_\_  
DATE

\_\_\_\_\_  
TIME

**Contingency Plans**

**Shots Fired Prior To Entry:**

1. React to threat
2. Establish perimeter or move to rally point
3. Account for personnel
4. Establish Command Post with responding agency

**Shots Fired After Entry or Barricaded Suspect:**

1. React to threat
2. Hold existing positions or move to Rally Point
3. If necessary, withdraw and establish exterior perimeter
4. Account for personnel
5. Establish Command Post with responding agency

**Agent Down-Interior or Exterior:**

1. React to threat
2. Evacuate injured personnel

3. Hold existing positions or move to Rally Point
4. If necessary, withdraw and establish exterior perimeter
5. Account for personnel
6. Establish Command Post with responding agency

**Tactical Entry:**

1. React to threat
2. Work in pairs
3. Announce cleared rooms
4. Do not enter or exit through rear doors unless previously planned and announced

**Hostage Situation:**

1. React to threat
2. Contain/secure immediate area
3. Commence negotiations
4. If hostage is in vehicle, agent should attempt to disable vehicle by throwing out keys

**Hostage Rescue:**

1. Hostage will give, "Hostage Signal"
2. Rescue team leader will give the same signal back to hostage advising the rescue team is ready
3. When hostage is ready, hostage will drop/fall to ground allowing a clear target

**Jump out:**

1. If the suspect walks away from the location, officers will jump out on him to gain a tactical advantage.
2. If the suspect leaves in a car, officers will follow the suspect away and jump out on him at a safe location of our choosing.

**Jam:**

1. If the suspect leaves in a car and does not appear to be going to any particular location, officers may Jam the vehicle if the opportunity presents itself, at a location of our choosing.
2. Whether we use the Jump out or the Jam will depend on the suspect's actions. These options will be used to eliminate vehicle pursuits, reduce foot pursuits, reduce the likelihood of a violent reaction, avoid evidence destruction, and stop a phone call back to the house where the search warrant will be served. These tactics will help officers gain a significant tactical advantage over the suspect.



# Office of the District Attorney Stanislaus County

Birgit Fladager  
District Attorney

Assistant District Attorney  
Dave Harris

Chief Deputies  
Annette Rees  
Marlisa Ferreira  
Stephen R. Robinson  
Jeffrey M. Laugero  
Jeff Mangar

Chief Investigator  
Terry L. Seese

## TACTICAL OPERATIONS PLAN

DATE/TIME: CASE# CASE AGENT:

SWAT Consultation: Yes ☐ No ☐

Risk Assessment Matrix shall be attached to this operations plan

### TYPE OF OPERATION:

- |                                              |                                         |                                           |                                        |
|----------------------------------------------|-----------------------------------------|-------------------------------------------|----------------------------------------|
| <input type="checkbox"/> Surveillance        | <input type="checkbox"/> Search Warrant | <input type="checkbox"/> U/C Op           | <input type="checkbox"/> C/I buy       |
| <input type="checkbox"/> Knock and talk      | <input type="checkbox"/> Arrest         | <input type="checkbox"/> Probation Search | <input type="checkbox"/> Parole Search |
| <input type="checkbox"/> Enforcement Op      | <input type="checkbox"/> Flash          | <input type="checkbox"/> Reverse          |                                        |
| <input type="checkbox"/> Controlled Delivery | <input type="checkbox"/> Buy/Bust       |                                           |                                        |

### CASE BACKGROUND:

Write a brief narrative of the type of case and what the operation is: Search warrant, surveillance (for what), arrest warrant- take down etc...

### OPERATIONAL OBJECTIVE(s):

A SAFE SUCCESSFUL OPERATION FOR ALL INVOLVED IS OUR PRIMARY OBJECTIVE.

- 1.
- 2.
- 3.
- 4.

All MPD and Stanislaus County DA personnel will follow their respective policies.

### LOCATION(s):

List address and provide a photo

### SUBJECT(s):

- 1.
- 2.
- 3.



**OUTSIDE AGENCY OPERATIONS PERSONNEL:**

Personnel	Agency	Call Sign	Cell Phone	Vehicle	Assignment
					Supervisor
					Entry
					Entry

**STANISLAUS D.A. PERSONNEL:**

Personnel	Agency	Call Sign	Cell Phone	Vehicle	Assignment

**AGENCY PHONE NUMBERS:**

<b>Stan. Co S/O</b>	<b>209-525-7914</b>	<b>Modesto PD</b>	<b>209-572-9595</b>	<b>Ceres PD</b>	<b>209-538-5713</b>
Turlock PD	209-668-1200	Oakdale PD	209-847-2231	Merced PD	209-385-6907
Merced S/O	209-385-7445	Hughson PD	209-883-4052	Riverbank PD	209-869-2572
Manteca PD	209-239-8042	Waterford PD	209-874-2349	Patterson PD	209-575-9780
SDEA	209-558-6300	StanCATT	209-545-7316	Stanislaus DA	209-525-5550

**Operational Codes / UC Information:**

None.

**Communications:**Primary Radio Channel: **Comm with MPD Channel 1**Secondary/Emergency Radio Channel: **MPD Channel 2****Caution Statement:**

- 1. Weapons ☐
- 2. Violent History ☐
- 3. Fortifications ☐
- 4. Guard dogs/Animals ☐
- 5. Surveillance Equipment ☐
- 6. Children/Elderly ☐

**Additional:**

- 1. Rap sheets ☐
- 2. Photos attached ☐
- 3. Premise History ☐
- 4. Maps/Diagrams attached ☐
- 5. Risk Assessment Matrix ☐
- 6. Undercover Ops Risk Analysis ☐

7. Mental Conditions ☐

7. Animal Mitigation Plan ☐

**Notifications:**

1. WSIN	916-263-1166	Notified By:	
2. LA CLEAR	877-550-2532	Notified By:	Date/Time:
3. Comm Center	209-572-9595	Notified By:	Date/Time:
4. Watch Cmdr.	209-572-9584	Notified By:	Date/Time:

**Individual Equipment**

<input type="checkbox"/> BDUs	<input type="checkbox"/> Ballistic Vests	<input type="checkbox"/> Helmet	<input type="checkbox"/> Raid Vest	<input type="checkbox"/> Eye Protection
<input type="checkbox"/> OC Spray	<input type="checkbox"/> Portable Radio	<input type="checkbox"/> Flashlight	<input type="checkbox"/> Handcuffs	<input type="checkbox"/> Baton
<input type="checkbox"/> Handgun	<input type="checkbox"/> Rifle	<input type="checkbox"/> Gloves	<input type="checkbox"/> Lab Gear	<input type="checkbox"/> Mirror
<input type="checkbox"/> Other				

**Specialized Equipment**

<input type="checkbox"/> Shield	<input type="checkbox"/> Cutters	<input type="checkbox"/> Hooligan	<input type="checkbox"/> Pry Bar	<input type="checkbox"/> Ram
<input type="checkbox"/> 35mm Camera	<input type="checkbox"/> Digital Camera	<input type="checkbox"/> Video Camera	<input type="checkbox"/> Evidence Kit	<input type="checkbox"/> Sledge
<input type="checkbox"/> Aircraft	<input type="checkbox"/> Night Vision	<input type="checkbox"/> Flir	<input type="checkbox"/> Other	

**Hospitals:**

**Doctor's Medical Center**  
1441 Florida Avenue  
Modesto, CA  
(209) 578-1211

**Memorial Hospital**  
1700 Coffee Road  
Modesto, CA  
(209) 526-4500

**SUPERVISOR'S AUTHORIZATION TO PROCEED:**

\_\_\_\_\_  
LIEUTENANT SIGNATURE

\_\_\_\_\_  
DATE

\_\_\_\_\_  
TIME

**Contingency Plans**

**Shots Fired Prior To Entry:**

1. React to threat
2. Establish perimeter or move to rally point
3. Account for personnel
4. Establish Command Post with responding agency

**Shots Fired After Entry or Barricaded Suspect:**

1. React to threat
2. Hold existing positions or move to Rally Point
3. If necessary, withdraw and establish exterior perimeter
4. Account for personnel
5. Establish Command Post with responding agency

**Agent Down-Interior or Exterior:**

1. React to threat
2. Evacuate injured personnel

3. Hold existing positions or move to Rally Point
4. If necessary, withdraw and establish exterior perimeter
5. Account for personnel
6. Establish Command Post with responding agency

**Tactical Entry:**

1. React to threat
2. Work in pairs
3. Announce cleared rooms
4. Do not enter or exit through rear doors unless previously planned and announced

**Hostage Situation:**

1. React to threat
2. Contain/secure immediate area
3. Commence negotiations
4. If hostage is in vehicle, agent should attempt to disable vehicle by throwing out keys

**Hostage Rescue:**

1. Hostage will give, "Hostage Signal"
2. Rescue team leader will give the same signal back to hostage advising the rescue team is ready
3. When hostage is ready, hostage will drop/fall to ground allowing a clear target

**Jump out:**

1. If the suspect walks away from the location, officers will jump out on him to gain a tactical advantage.
2. If the suspect leaves in a car, officers will follow the suspect away and jump out on him at a safe location of our choosing.

**Jam:**

1. If the suspect leaves in a car and does not appear to be going to any particular location, officers may Jam the vehicle if the opportunity presents itself, at a location of our choosing.
2. Whether we use the Jump out or the Jam will depend on the suspect's actions. These options will be used to eliminate vehicle pursuits, reduce foot pursuits, reduce the likelihood of a violent reaction, avoid evidence destruction, and stop a phone call back to the house where the search warrant will be served. These tactics will help officers gain a significant tactical advantage over the suspect.

## **2022-01-06 UOF Review blank.pdf**



# Office of the District Attorney Stanislaus County

**Birgit Fladager**  
District Attorney

**Assistant District Attorney**  
Jeffrey M. Laugero

**Chief Deputies**  
Marlisa Ferreira  
Wendell Emerson  
Michael D. Houston  
Mark Zahner

**Bureau of Investigation**  
Chief Terry L. Seese

---

## MEMORANDUM

**To:** Chief Investigator  
**From:** Lieutenant  
**Date:**  
**Subject:** Use of Force Review

---

**Case Number:**

**Date/Time of Incident:**

**Involved DAI and Officers:**

**Summary of Incident:**

**Disposition (arrest, citation), Including Arrestee Information:**

**Injuries/Property Damage:**

**Medical Treatment:**

**Name of Supervisor Over Incident:**

**Conclusion:**

**Training Issues Identified:**

**Recommendation:**

Office: 832 12th Street, Suite 300 Modesto, CA 95354 Mailing: PO BOX 442 Modesto, CA 95353

Telephone: (209) 525-5550 Fax: (209) 558-4027 [www.stanislaus-da.org](http://www.stanislaus-da.org)



<https://www.facebook.com/StanislausDistrictAttorney/>

\_\_\_\_\_  
Lieutenant

Date: \_\_\_\_\_

\_\_\_\_\_  
Criminal Investigator

Date: \_\_\_\_\_

Office: 832 12th Street, Suite 300 Modesto, CA 95354 Mailing: PO BOX 442 Modesto, CA 95353

Telephone: (209) 525-5550 Fax: (209) 558-4027 [www.stanislaus-da.org](http://www.stanislaus-da.org)



<https://www.facebook.com/StanislausDistrictAttorney/>

## **2022-01-06 Pursuit Review blank.pdf**



# Office of the District Attorney Stanislaus County

**Birgit Fladager**  
District Attorney

**Assistant District Attorney**  
Jeffrey M. Laugero

**Chief Deputies**  
Marlisa Ferreira  
Wendell Emerson  
Michael D. Houston  
Mark Zahner

**Bureau of Investigation**  
Chief Terry L. Seese

---

## MEMORANDUM

**To:** Chief Investigator

**From:** Lieutenant

**Date:**

**Subject:** Pursuit Review

---

**Case Number:**

**Date/Time of Pursuit:**

**Length of pursuit:**

**Starting and Termination Point:**

**Start:**

**Termination:**

**Involved Units and DAI's:**

**Initial Reason for Pursuit:**

**Summary of Incident:**

**Disposition (arrest, citation), Including Arrestee Information:**

**Injuries/Property Damage:**

**Medical Treatment:**

**Name of Supervisor Over Incident:**

**Conclusion:**

Office: 832 12th Street, Suite 300 Modesto, CA 95354 Mailing: PO BOX 442 Modesto, CA 95353

Telephone: (209) 525-5550 Fax: (209) 558-4027 [www.stanislaus-da.org](http://www.stanislaus-da.org)



<https://www.facebook.com/StanislausDistrictAttorney/>



**Training Issues Identified:**

**Recommendation:**

\_\_\_\_\_  
Lieutenant

Date: \_\_\_\_\_

\_\_\_\_\_  
Criminal Investigator

Date: \_\_\_\_\_

Office: 832 12th Street, Suite 300 Modesto, CA 95354 Mailing: PO BOX 442 Modesto, CA 95353

Telephone: (209) 525-5550 Fax: (209) 558-4027 [www.stanislaus-da.org](http://www.stanislaus-da.org)



<https://www.facebook.com/StanislausDistrictAttorney/>

## **Supplemental Hate Crime Report-Agency.pdf**

# SUPPLEMENTAL HATE CRIME REPORT

Page 1 of 2

☐ Hate incident (No Crime Committed)

☐ Hate Crime (422.6 PC, 51.7 CC, 52.1 CC)

## VICTIM

### VICTIM TYPE

☐ Individual

Legal name (Last, First): \_\_\_\_\_

Date of Birth

Age

Sex

Race

☐ School, business or organization

Name: \_\_\_\_\_

Type: \_\_\_\_\_  
(e.g., non-profit, private, public school)

☐ Faith-based organization

Name: \_\_\_\_\_

Faith: \_\_\_\_\_

☐ Other

Name: \_\_\_\_\_

Type: \_\_\_\_\_

Address: \_\_\_\_\_

Date and time of incident: \_\_\_\_\_

Location of incident: \_\_\_\_\_

Date and time of report: \_\_\_\_\_

Location of report: \_\_\_\_\_

Agency Case #: \_\_\_\_\_

### NATURE OF CALL FOR SERVICE (check all that apply)

☐ Crime against persons

☐ Crime against property

☐ Gang activity

☐ Other \_\_\_\_\_

## BIAS

### TYPE OF BIAS

(Check all characteristics that apply)

☐ Disability

☐ Gender

☐ Gender identity/expression

☐ Sexual orientation

☐ Race

☐ Ethnicity

☐ Nationality

☐ Religion

☐ Significant day of offense  
(e.g., 9/11, holy days)

☐ Association with a person or group with  
one or more of these characteristics  
(actual or perceived)

☐ Other: \_\_\_\_\_

### ACTUAL OR PERCEIVED BIAS – VICTIM'S STATEMENT

☐ Actual bias [Victim has the indicated characteristic(s)].

☐ Perceived bias [Suspect believed victim had the indicated  
characteristic(s)].

### REASON FOR BIAS:

Do you feel you were targeted based on one of these characteristics?

☐ Yes ☐ No

Do you know what motivated the suspect to commit this crime?

☐ Yes ☐ No

Do you feel you were targeted because you associated yourself with an  
individual or a group?

☐ Yes ☐ No

Are there indicators the suspect is affiliated with a Hate Group  
(i.e., literature/tattoos)?

☐ Yes ☐ No

Are there Indicators the suspect is affiliated with a criminal street gang?

☐ Yes ☐ No

### BIAS INDICATORS (CHECK ALL THAT APPLY):

☐ Hate speech

☐ Acts/gestures

☐ Property damage

☐ Symbol used

☐ Written/electronic communication

☐ Graffiti/spray paint

☐ Other: \_\_\_\_\_

## SUPPLEMENTAL HATE CRIME REPORT

Page 2 of 2

### HISTORY

SUSPECT INFORMATION				RELATIONSHIP BETWEEN SUSPECT & VICTIM	
Legal name (Last, First): _____				Suspect known to victim: <input type="checkbox"/> Yes <input type="checkbox"/> No	
Other Names used (AKA): _____				Nature of relationship: _____	
Date of Birth	Age	Sex	Race	Length of relationship: _____	
				<input type="checkbox"/> Prior reported incidents with suspect: <i>Total #</i> _____	
Relationship to Victim: _____				Prior unreported incidents with suspect: <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown	

### WEAPONS/FORCE

Weapon(s) used during incident?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	Type: _____
Force used during incident?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	Type: _____

### EVIDENCE

Witnesses present during incident?		<input type="checkbox"/> Yes	<input type="checkbox"/> No	Statements taken?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Evidence collected?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	Recordings:	<input type="checkbox"/> Video	<input type="checkbox"/> Audio	<input type="checkbox"/> Booked	
Photos taken?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	Suspect identified:	<input type="checkbox"/> Field ID	<input type="checkbox"/> By photo/video	<input type="checkbox"/> Known	

### RESOURCES

Resources offered at scene: <input type="checkbox"/> Yes <input type="checkbox"/> No		
<input type="checkbox"/> Marsy's Law Handout	<input type="checkbox"/> Hate Crimes Brochure	<input type="checkbox"/> Other: _____

### MEDICAL

Victim	Suspect	
<input type="checkbox"/>	<input type="checkbox"/>	Declined medical treatment
<input type="checkbox"/>	<input type="checkbox"/>	Will seek own medical treatment
<input type="checkbox"/>	<input type="checkbox"/>	Received medical treatment
<input type="checkbox"/>	<input type="checkbox"/>	Injuries observed

Completed by	Date
Name/Title/ID number	

Stanislaus County District  
Attorney's Office Policy Manual  
Policy Manual

---

## INDEX / TOPICS

### A

#### ACKNOWLEDGEMENTS

Policy manual. . . . .	16
Policy revisions. . . . .	16

#### ADMINISTRATIVE INVESTIGATIONS

Vehicle damage. . . . .	331
-------------------------	-----

#### ALCOHOL. . . . . 399

##### ALCOHOL

Vehicle use. . . . .	330
----------------------	-----

#### ALCOHOL, INTOXICANTS. . . . . 377

#### ALCOHOL USE. . . . . 399

#### AMMUNITION

Gun violence restraining order surrenders. . . . .	236
----------------------------------------------------	-----

#### APPOINTMENTS

Operations director. . . . .	168
------------------------------	-----

#### ARRESTS

First amendment assemblies. . . . .	117, 119
-------------------------------------	----------

#### AUDIO/VIDEO RECORDING

Custodial interrogation. . . . .	160
----------------------------------	-----

#### AUTHORITY

Policy manual. . . . .	14
------------------------	----

#### AUTHORITY, ETHICS. . . . . 373

### B

#### BADGE. . . . . 450

#### BATON. . . . . 45

#### BODY ARMOR. . . . . 421

#### BOMBS. . . . . 101

#### BRADY MATERIAL. . . . . 303

#### BREATH TEST. . . . . 478

### C

#### CANINES

Pursuits. . . . .	58
-------------------	----

#### CHIEF EXECUTIVE. . . . . 12

#### CHILD ABUSE. . . . . 255

#### CHILDREN

Transporting. . . . .	419
-----------------------	-----

#### CIVILIAN/NON-SWORN. . . . . 14

#### CODE-3. . . . . 63

#### COMMAND STAFF

Policy review. . . . .	16
------------------------	----

#### COMMUNICABLE DISEASE

Health orders. . . . .	225
------------------------	-----

#### COMMUNICATIONS CENTER

Foot pursuits. . . . .	61
------------------------	----

#### COMPUTERS

Digital evidence. . . . .	162
---------------------------	-----

#### CONDUCT. . . . . 371

Standards of conduct. . . . .	375
-------------------------------	-----

#### CONTACTS AND TEMPORARY DETENTIONS

Warrant service. . . . .	171
--------------------------	-----

#### CONTROL DEVICES. . . . . 45

#### CONTROL DEVICES. . . . . 45

#### CONTROL DEVICES, CUSTODY

FIREARMS, Custody. . . . .	359
----------------------------	-----

#### COURT ORDERS

Gun violence restraining order surrenders. . . . .	236
----------------------------------------------------	-----

#### CRIME SCENE AND DISASTER INTEGRITY 224

#### CUSTODIAL INTERROGATIONS. . . . . 160

### D

#### DEBRIEFING

Warrant service. . . . .	171
--------------------------	-----

#### DECONFLICTION. . . . . 179

#### DEFINITIONS. . . . . 14

#### DEPARTMENTAL DIRECTIVES. . . . . 20

#### DEPARTMENT OWNED PROPERTY. . . . . 323

#### DEPARTMENT PROPERTY

Loss Or Damage. . . . .	324
-------------------------	-----

#### DISCIPLINE. . . . . 372

#### DISCLAIMER. . . . . 14

#### DRIVING, SAFETY SAFETY, CONDUCT

#### FIREARMS, CONDUCT. . . . . 376

#### DRUG USE. . . . . 399

#### DUI ENFORCEMENT. . . . . 476

### E

#### ELECTRONIC MAIL. . . . . 23

#### EVIDENCE

Digital. . . . .	162
------------------	-----

Seizing recordings. . . . .	277
-----------------------------	-----

#### EVIDENCE, BOMBS. . . . . 105

#### EXPLOSIONS. . . . . 104

### F

#### FIELD SOBRIETY TESTS. . . . . 476

#### FIREARMS

Retiree. . . . .	24
------------------	----

# Stanislaus County District Attorney's Office

## Policy Manual

### Stanislaus County District Attorney's Office Policy Manual

---

FOREIGN DIPLOMATIC AND CONSULAR  
REPRESENTATIVES. . . . . 245

## G

GRIEVANCE PROCEDURE. . . . . 391  
GRIEVANCES  
    Supervisor authority. . . . . 14  
GROOMING STANDARDS. . . . . 440

## I

INFORMATION TECHNOLOGY USE  
TECHNOLOGY USE. . . . . 66  
INVESTIGATION AND PROSECUTION. . 159

## L

LIMITED ENGLISH PROFICIENCY. . . . 74  
LIMITED ENGLISH PROFICIENCY  
    Eyewitness identification. . . . . 299

## M

MEDICAL  
    Releases. . . . . 125  
MODIFIED-DUTY ASSIGNMENTS. . . . 452  
MUTUAL AID  
    First amendment assemblies. . . . . 118  
    Warrant service. . . . . 171

## N

NOTIFICATIONS  
    Impaired driving. . . . . 477  
    Sick leave. . . . . 402

## O

OATH OF OFFICE. . . . . 13  
OFFICER SAFETY  
    Crime scene and disaster integrity. . . . 224  
    Foot pursuits. . . . . 58  
    LEOSA. . . . . 24  
    Seat belts. . . . . 419  
    Warrant service. . . . . 168

OPERATIONS PLANNING AND  
DECONFLICTION. . . . . 177  
ORGANIZATIONAL STRUCTURE. . . . 18  
OUTSIDE AGENCY ASSISTANCE. . . . 157  
OUTSIDE EMPLOYMENT. . . . . 435  
    Change in Status. . . . . 438  
    Obtaining Approval. . . . . 435  
    Prohibited Outside Employment. . . . . 436  
    Security Employment. . . . . 436  
OVERTIME PAYMENT. . . . . 433

## P

PERFORMANCE EVALUATIONS  
    Sick leave. . . . . 403  
PERSONAL APPEARANCE. . . . . 440  
PERSONAL PROPERTY. . . . . 323  
    Loss Or Damage. . . . . 324  
POLICY MANUAL. . . . . 14  
POLITICAL ACTIVITY. . . . . 458  
POLITICAL ENDORSEMENTS. . . . . 458  
PRIVATE PERSONS ARRESTS. . . . . 72  
PUBLIC RECORDING OF LAW  
ENFORCEMENT ACTIVITY. . . . . 276  
PURSUITS  
    Foot. . . . . 58

## R

RECORDS BUREAU  
    Administrative hearings. . . . . 481  
    Impaired driving. . . . . 481  
    Suspicious activity reports. . . . . 210  
RECORDS RETENTION  
    Oath of office. . . . . 13  
RELIGION, ACCOMMODATIONS IN  
CUSTODY. . . . . 359  
RESPONSE TO CALLS. . . . . 63  
REVIEWS  
    Policy manual. . . . . 16  
RISK ASSESSMENT. . . . . 177

## S

SAFETY  
    Canine. . . . . 329  
    First responder. . . . . 224  
    Temporary custody of adults. . . . . 356  
SAFETY EQUIPMENT

# Stanislaus County District Attorney's Office

## Policy Manual

### *Stanislaus County District Attorney's Office Policy Manual*

---

First amendment assemblies. . . . .	117
Seat belts. . . . .	419
SCHOOL EMPLOYEE REPORTING. . . . .	79
SEARCH & SEIZURE. . . . .	166
SEARCHES	
Crime scene. . . . .	224
Gun violence restraining orders. . . . .	235
SEARCH WARRANTS. . . . .	168
SECURITY EMPLOYMENT. . . . .	436
SOCIAL NETWORKING. . . . .	456
STANDARDS OF CONDUCT. . . . .	371
SUSPICIOUS ACTIVITY REPORTING. . . . .	209

## T

TOLL ROADS. . . . .	331
TRAINING	
Impaired driving. . . . .	481
Operation planning and deconfliction. . . . .	181
Warrant service. . . . .	172
TRAINING PLAN. . . . .	21
TRAINING POLICY. . . . .	21

## U

UNMANNED AERIAL SYSTEM. . . . .	312
---------------------------------	-----

## W

WARRANT SERVICE. . . . .	168
--------------------------	-----