U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Information Technology Security Audit (ITSA) Report

California

March 2014

Table of Contents

Table of Contents

Executive Summary

Overview

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years at a minimum, to assess agency compliance with the *CJIS Security Policy*. The essential premise of the *CJIS Security Policy* is to provide appropriate controls to protect the full lifecycle of criminal justice information (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. Policies and procedures governing the security of CJI are examined during the audits. Although compliance with all CJIS security policies was not assessed, adherence to all CJIS security policies and procedures is required for FBI CJIS systems access.

Audit Recommendations

Based on the ITSA conducted during March 2014, the FBI's CJIS Division makes the following recommendation(s) to the CSA as listed below.

1. **Ensure the local agencies implement appropriate agreements with their respective noncriminal justice agencies. (This was a recommendation during the previous audit cycle.)**
2. **Ensure the CSA and the local agencies implement the CJIS Security Addendum with their servicing private contractor personnel. (This was a recommendation during the previous two audit cycles.)**
3. **Ensure the local agencies fingerprint all agency terminal operators, IT, and unescorted custodial, support, and contract personnel with direct access to CJI.**
4. **Ensure the local agencies provide security awareness training to all agency terminal operators, IT, noncriminal justice agency and private contractor personnel who manage and/or have access to CJI within six months of assignment and at least once every two years. (This was a recommendation during the previous two audit cycles.)**
5. **Ensure the local agencies have a written policy for sanitization and destruction of electronic media.**
6. **Ensure the local agencies' passwords used for authentication follow the secure password attributes. (This was a recommendation during the previous two audit cycles.)**
7. **Ensure the local agencies use advanced authentication for personnel that manage or access CJI from nonsecure locations. (This was a recommendation during the previous audit cycle.)**
8. **Ensure the local agencies encrypt all network segments that access CJI with at least 128-bit NIST certified encryption to comply with the FIPS 140-2 requirement. (This was a recommendation during the previous two audit cycles.)**
9. **Ensure the local agencies develop an information security incident response policy.**

New Policy Overview

The *CJIS Security Policy* contains current requirements carried over from previous versions along with new requirements for agencies to implement. These new policy requirements, although assessed, will not be forwarded through the APB Compliance Evaluation Subcommittee during the current zero cycle audit that is specified with "required by" and the year. The intent is for agencies to start working toward compliance immediately, where possible. The audit, as well as the Requirements and Transition Document, can be used as a tool for financial planning and justification to meet these new requirements. Adherence to all new policies and procedures is required for FBI CJIS systems access.

New Policy: Areas of Concern (Zero Cycle)

Although not recommendations at this time, the following Area(s) of Concern were identified:

1. Ensure the local agencies provide the first tier of security awareness training to all unescorted personnel with access to CJI.
2. Ensure the local agencies have a written procedures for electronic and physical media tat restricts access to authorized individuals.
3. Ensure the local agencies document and implement all physical and electronic media policies.
4. Ensure the local agencies display an approved system use notification message on all information systems accessing CJI.
5. Ensure the local agencies document the validation of system accounts.
6. Ensure the local agencies follow all audit log requirements as set forth in the CJIS Security Policy.

The following terms are used in compliance summary charts throughout the report.

IN	Agency is *IN* compliance with policy/procedure.
OUT	Agency is *OUT* of compliance with policy/procedure. **Corrective Action is needed.**
N/A (Not Applicable)	Policy/procedure is not applicable to the agency and therefore not assessed.
NPI (New Policy IN)	New policy: Agency is *IN* compliance but policy is in zero cycle and will not be reported to the APB Compliance Evaluation Subcommittee.
NPO (New Policy OUT)	New policy: Agency is *OUT* of compliance but policy is in zero cycle and will not be reported to the APB Compliance Evaluation Subcommittee. **Corrective Action is needed.**
NPN (New Policy N/A)	New policy: Policy is not applicable to the agency and will not be reported to the APB Compliance Evaluation Subcommittee.

ITSA Policy Compliance Summary

The following chart provides a listing of policies assessed during the audit and indicates overall compliance by the California Department of Justice.

Policy	Finding
System Administration	
CJIS Systems Officer (CSO)	**IN**
Information Security Officer (ISO)	**IN**
Local Agency Security Officer (LASO)	**IN**
Administration of Criminal Justice Functions	
Noncriminal Justice Agency (NCJA)	**OUT**
Private Contractor	**OUT**
Agency Coordinator	**IN**
Management Control	**IN**
Information Protection	
IT Security Program	**IN**
Standards of Discipline	**IN**
Personnel Security	**OUT**
Security Awareness Training	**OUT**
Physical Security	**IN**
Security Audits	**IN**
Media Disposal	**OUT**

Policy	Finding
Network Infrastructure	
Network Configuration	IN
Identification/UserID	IN
Authentication	OUT
Session Lock	IN
Event Logging	IN
Advanced Authentication	OUT
Encryption	OUT
Dial-up Access	
Mobile Devices	IN
Personal Firewalls	IN
Boundary Protection	IN
Malicious Code Protection	IN
Security Incident Response	OUT

ITSA New Policy Requirements Compliance Summary

The following chart details the new policies assessed during the audit and the overall adherence to new policy requirements as defined in the most current version of the *CJIS Security Policy*.

New Policy	Finding
Information Protection	
Personnel Security	**NPI**
Security Awareness Training	**NPO**
Physical Security	**NPI**
Media Protection	**NPO**
Media Transport	**NPI**
Media Disposal	**NPO**
Network Infrastructure	
Personally Owned Information Systems	
Publicly Accessible Computers	**NPI**
System Use Notification	**NPO**
Identification/UserID	**NPO**
Authentication	**NPI**
Session Lock	**NPI**
Event Logging	**NPO**
Remote Maintenance	**NPI**
Encryption	**NPI**
Mobile Devices	**NPI**
Cellular Access	**NPI**
Bluetooth Access	

Wireless (802.11x) Access	
Boundary Protection	**NPI**
Intrusion Detection Tools & Techniques	
Malicious Code Protection	**NPI**
Spam and Spyware Protection	**NPI**
Security Alerts and Advisories	**NPI**
Patch Management	**NPI**
Voice over Internet Protocol (VoIP)	**NPI**
Partitioning and Virtualization	**NPI**
Cloud Computing	
Security Incident Response	**NPI**

Introduction

Background

In 1992, the FBI incorporated the CJIS security policies as part of the *NCIC Operating Manual*. With increased technological advances in telecommunications and systems architecture, the APB recommended in 1998 that the FBI CJIS Division authorize the establishment of a security management infrastructure. As a result, the FBI CJIS Division wrote the *CJIS Security Policy* which was approved by the FBI Director in 1999. The FBI CAU's ITSA was incorporated as a component of the NCIC audit process in 2000. In October 2004, the ITSA evolved into a separate audit program to ensure further compliance with the *CJIS Security Policy*.

Scope

The FBI's objective is to audit each CSA that provides FBI CJIS systems data access to user agencies and verify that users comply with the policies and procedures set forth in the *CJIS Security Policy*. The FBI's intent is to ensure the security and integrity of FBI CJIS systems information through a review and analysis of the CSA's administrative and technical security policies. Assessments are made based on policies set forth in the *CJIS Security Policy*; APB Bylaws and meeting minutes; and applicable federal laws.

Methodology

On-site audits of CSAs and local agencies consist of administrative interviews and network inspections. Administrative interviews are conducted with appropriate agency personnel and are designed to evaluate the security posture of criminal justice agencies directly connected with the FBI CJIS systems. Network inspections consist of system inquiries and test scenarios to assess, evaluate, and verify technical security compliance and to provide guidance for achieving compliance.

About This Report

The ITSA Report is divided into the following policy sections: System Administration, Administration of Criminal Justice Functions, Information Protection, and Network Infrastructure. Each section contains a summary chart which displays the audit results for each agency as well as overall compliance for the CSA. Policies which are not assessed as part of the audit are displayed as shaded areas within each summary chart. Red text within a summary chart indicates a policy violation. Each policy is defined and referenced. Policy violations are detailed as necessary and presented in an audit analysis following their respective policy definitions. Violations which are determined to be system-wide compliance issues are presented as bolded text for emphasis and ease of reference. These violations result in recommendations which correspond to the recommendations in the executive summary. Violations which are not considered to be system-wide compliance issues as well as any other areas of concern which do not require corrective action are presented as non-bolded and noted in the analysis following the corresponding policy definition.

New *CJIS Security Policy* Requirements

Where applicable, a separate summary chart containing areas of concern for the new policy requirements has been included following each current policy compliance summary chart which displays the audit results of each local agency as well as overall compliance for the CSA. The new policy requirements, which are not applicable, are not assessed as part of the audit and are displayed as shaded areas within the new policy chart. Red text within a summary chart indicates an area of concern for the new policy requirements. Each policy is defined and referenced. Areas of concern for new policy requirements are detailed as necessary and presented as italicized text for emphasis and ease of reference. All system-wide areas of concern of new policy requirements correspond to the recommendations in the "New Policy: Areas of Concern (Zero Cycle)" section within the executive summary. Although corrective action is required, these areas of concern will not be forwarded to the APB Compliance Evaluation Subcommittee.

Audit Schedule

The chart below lists all participant(s) in the FBI Information Technology Security Audit of the California Department of Justice during this audit cycle. The agencies are listed in alphabetical order following the CJIS Systems Agency (CSA). The originating agency identifier (ORI) is also provided for identification purposes.

	ORI
CSA - California Department of Justice	CA0349400
Anaheim Police Department	CA0300100
Lodi Police Department	CA0390200
Los Angeles County Sheriff's Office	CA0190000
Los Angeles Police Department	CA0194200
Monterey Police Department	CA0270600
San Francisco County Sheriff's Office	CA0380000
San Francisco Police Department	CA0380100
Santa Ana Police Department	CA0301900
Stockton Police Department	CA0390500
Total Agencies Audited	**9**

System Administration Policy Compliance Summary Chart

	CJIS Systems Officer (CSO)	Information Security Officer (ISO)	Local Agency Security Officer (LASO)
CSA - California Department of Justice	IN	IN	
Anaheim Police Department			IN
Lodi Police Department			IN
Los Angeles County Sheriff's Office			IN
Los Angeles Police Department			IN
Monterey Police Department			IN
San Francisco County Sheriff's Office			IN
San Francisco Police Department			IN
Santa Ana Police Department			IN
Stockton Police Department			IN
Overall Audit Compliance	**IN**	**IN**	**IN**

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. (*CJIS Security Policy*, Version 5.2, August 2013, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.2 CJIS Systems Officer (CSO), pp. 5-6)

[redacted]

Finding: In Compliance

Recommendation: None

Information Security Officer (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. (*CJIS Security Policy*, Version 5.2, August 2013, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.8 CJIS System Agency Information Security Officer (CSA ISO), pp. 7-8)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.1 Reporting Information Security Events, 5.3.1.1 Reporting Structure and Responsibilities, 5.3.1.1.2 CSA ISO Responsibilities, pp. 23-24)

Finding: In Compliance

Recommendation: None

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 CSA ISO is promptly informed of security incidents. (*CJIS Security Policy*, Version 5.1, July 2012, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.9 Local Agency Security Officer (LASO), p. 8)

Finding: In Compliance

Recommendation: None

Administration of Criminal Justice Functions Policy Compliance Summary Chart

	Noncriminal Justice Agency (NCJA)	Private Contractors	Agency Coordinator (AC)	Management Control
CSA - California Department of Justice		IN	IN	IN
Anaheim Police Department		OUT	IN	IN
Lodi Police Department	OUT	OUT	IN	IN
Los Angeles County Sheriff's Office		IN	IN	IN
Los Angeles Police Department	IN	OUT	IN	IN
Monterey Police Department	IN	OUT	IN	IN
San Francisco County Sheriff's Office	IN	OUT	IN	IN
San Francisco Police Department	IN	OUT	IN	IN
Santa Ana Police Department	IN	OUT	IN	IN
Stockton Police Department	OUT	OUT	IN	IN
Overall Audit Compliance	**OUT**	**OUT**	**IN**	**IN**

Definition: Administration of Criminal Justice is defined as 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. (*CJIS Security Policy*, Version 5.1, July 2012, Appendix A, Terms and Definitions)

Noncriminal Justice Agency (NCJA)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.1 Policy Area 1: Information Exchange Agreements, 5.1.1 Information Exchange, 5.1.1.4 Inter-Agency and Management Control Agreements, p. 16)

Finding: **Out of Compliance**

Recommendation: Ensure the local agencies implement appropriate agreements with their respective noncriminal justice agencies.

Analysis: The following local agencies received IT services from their respective noncriminal justice agencies. No agreements were in place between attributes:

- Lodi Police Department – City of Lodi IT
- Stockton Police Department – City of Stockton IT

Private Contractors

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). (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.1 Policy Area 1: Information Exchange Agreements, 5.1.1 Information Exchange, 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum, pp. 16-17)

Finding: **Out of Compliance**

Recommendation: Ensure the local agencies implement the CJIS Security Addendum with their servicing private contractor personnel.

Analysis: The following local agencies received IT services from their perspective private contractors. No CJIS security addendums were in place and signed by these private contractor's personnel:

- Anaheim Police Department – Versaterm, HP Enterprise Services, Cogent, and RCS Investigations and Consulting.
- Lodi Police Department – Secure Link, Sunguard, Delta Wireless
- Los Angeles Police Department – Palantir, Praescient Analytics, JSS Contractors, and Iron Mountain.
- Monterey Police Department – Cintas
- San Francisco County Sheriff's Office – Iron Mountain
- San Francisco Police Department – Level II, Inc., and Shred Works
- Santa Ana Police Department – Softmaster, Crossroads Software, Inc., Tiberon, and Paper Recycling Shredding Services.
- Stockton Police Department – Tiberon, Iron Mountain, Delta Wireless, and NEKO

Agency Coordinator (AC)

Agency Coordinator (AC) Designated

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. (*CJIS Security Policy*, Version 5.2, August 2013, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.6 Contracting Government Agency (CGA), p. 7)

Agency Coordinator (AC) Responsibilities

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 CJA (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. (*CJIS Security Policy*, Version 5.2, August 2013, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.7 Agency Coordinator (AC), p. 7)

Finding: In Compliance

Recommendation: None

Management Control

The CSO shall set, maintain, and enforce the following:

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. (*CJIS Security Policy*, Version 5.2, August 2013, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.2 CJIS Systems Officer (CSO), pp. 5-6)

Finding: In Compliance

Recommendation: None

Information Protection Policy Compliance Summary Chart

	IT Security Program	Standards of Discipline	Personnel Security	Security Awareness Training	Physical Security	Security Audits	Media Disposal
CSA - California Department of Justice	IN	IN	IN	IN	IN	IN	IN
Anaheim Police Department	IN	IN	OUT	OUT	IN		OUT
Lodi Police Department	IN	IN	OUT	OUT	IN		OUT
Los Angeles County Sheriff's Office	IN	IN	IN	OUT	IN		IN
Los Angeles Police Department	IN	IN	OUT	OUT	IN		OUT
Monterey Police Department	IN	IN	OUT	OUT	IN		IN
San Francisco County Sheriff's Office	IN	IN	IN	IN	IN		IN
San Francisco Police Department	IN	IN	IN	OUT	IN		IN
Santa Ana Police Department	IN	IN	OUT	OUT	IN		OUT
Stockton Police Department	IN	IN	OUT	OUT	IN		OUT
Overall Audit Compliance	**IN**	**IN**	**OUT**	**OUT**	**IN**	**IN**	**OUT**

New Policy Requirements for Information Protection Compliance Summary Chart

	Personnel Security	Security Awareness Training	Physical Security	Media Protection	Media Transport	Media Disposal
CSA - California Department of Justice	NPI	NPI	NPI	NPI	NPI	NPI
Anaheim Police Department	NPI		NPI	NPI	NPI	NPO
Lodi Police Department	NPI	NPI	NPO	NPO	NPI	NPO
Los Angeles County Sheriff's Office	NPI	NPO	NPI	NPI	NPI	NPI
Los Angeles Police Department	NPI		NPI	NPI	NPI	NPO
Monterey Police Department	NPI	NPO	NPI	NPI	NPI	NPI
San Francisco County Sheriff's Office	NPI	NPI	NPI	NPO		NPI
San Francisco Police Department	NPI	NPI	NPI	NPI	NPI	NPI
Santa Ana Police Department	NPI		NPI	NPI	NPI	NPO
Stockton Police Department	NPI	NPO	NPO	NPO	NPI	NPO
Overall Audit Compliance	**NPI**	**NPO**	**NPI**	**NPO**	**NPI**	**NPO**

IT Security Program

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. (*CJIS Security Policy*, Version 5.2, August 2013, 1 Introduction, 1.3 Relationship to Local Security Policy and Other Policies, pp. 1-2)

Finding: In Compliance

Recommendation: None

Standards of Discipline

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.12 Policy Area 12: Personnel Security, 5.12.4 Personnel Sanctions, p. 65)

Finding: In Compliance

Recommendation: None

Personnel Security

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.
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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.12 Policy Area 12: Personnel Security, 5.12.1 Personnel Security Policy and Procedure, 5.12.1.1 Minimum Screening requirements for Individuals Requiring Access to CJI, pp. 63-64)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.12 Policy Area 12: Personnel

Security, 5.12.1 Personnel Security Policy and Procedure, 5.12.1.2 Personnel Screening for Contractors and Vendors, p. 64)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.12 Policy Area 12: Personnel Security, 5.12.3 Personnel Transfer, p. 65)

Finding: Out of Compliance

Recommendation: Ensure the local agencies fingerprint all agency terminal operators, IT, and unescorted custodial, support, and contract personnel with direct access to CJI.

Analysis: The following local agencies did not fingerprint all personnel with unescorted access to CJI:

- Anaheim Police Department – Versaterm and RCS Investigations and Consulting personnel
- Lodi Police Department – City IT, OSSI, Secure Llink, and Delta Wireless personnel
- Los Angeles Police Department – Iron Mountain personnel
- Monterey Police Department – Cintas personnel
- Santa Ana Police Department - Paper Recycling Shredding Services personnel
- Stockton Police Department – Tiberon, Iron Mountain, Delta Wireless, and NEKO personnel

New Policy Finding: In Compliance

Recommendation: *None*

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. 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5. 2 Policy Area 2: Security Awareness Training, pp. 20-22)

Security Awareness Training 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5. 2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, p. 20)

At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to CJI usage.
2. Implications of noncompliance.
3. Incident response (Points of contact; Individual actions).
4. Media protection.
5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
6. Protect information subject to confidentiality concerns — hardcopy through destruction.
7. Proper handling and marking of CJI.
8. Threats, vulnerabilities, and risks associated with handling of CJI.
9. Social engineering.
10. Dissemination and destruction. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, 5.2.1.1 All Personnel, p. 20)

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 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation,

5.2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, 5.2.1.2 Personnel with Physical and Logical Access, pp. 20-21)

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 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, 5.2.1.3 Personnel with Information Technology Roles, p. 21)

Security Awareness 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/Compact Officer. Maintenance of training records can be delegated to the local level. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.2 Security Training Records, p. 21)

Finding: Out of Compliance

Recommendation: Ensure the local agencies provide security awareness training to all agency terminal operators, IT, noncriminal justice agency and private contractor personnel who manage and/or have access to CJI within six months of assignment and at least every two years.

Analysis: The following agencies did not ensure personnel, who managed or had access to CJI, received security awareness training:

- Anaheim Police Department – local agency personnel, Versaterm, HP Enterprises, Cogent, and RCS Investigations and Consulting
- Lodi Police Department - local agency personnel, City IT, OSSI, Secure Link, and Delta Wireless
- Los Angeles County Sheriff's Office - local agency personnel and private contractors
- Los Angeles Police Department - local agency personnel, City IT, Palantir, Iron Mountain, Prascient Analytics, and JSS Contractors
- Monterey Police Department - Cintas
- San Francisco Police Department – Shred Works
- Santa Ana Police Department - local agency personnel, City IT, Softmaster, Crossroads Software, Inc., Tiberon, and Paper Recycling Shredding Services
- Stockton Police Department – IT personnel, Tiberon, Iron Mountain, Delta Wireless, and NEKO

New Policy Finding: ***Out of Compliance***

Recommendation: *Ensure the local agencies provide the first tier security awareness training to all unescorted personnel with physical access to CJI.*

Analysis: *The following areas of concern were identified for the new policy requirements assessed. Although corrective action is required, the area of concern will not be forwarded to the APB Compliance Evaluation Subcommittee. The following agencies did not provide the first tier of security awareness training to unescorted janitorial staff.*

- *Monterey Police Department*
- *Stockton Police Department*

The Los Angeles County Sheriff's Office did not have the required topics covered in their security awareness training.

Physical Security

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, p. 53)

A physically secure location is a facility 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 section 5.12 describes the minimum personnel security controls required for unescorted access to a physically secure location. Section 5.6.2.2.1 describes the requirements for technical security controls required to access CJI within the perimeter of a physically secure location without AA.

For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2014. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with section 5.9.1.3. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, p. 53)

The perimeter of 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.1 Security Perimeter, p. 53)

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. (*CJIS*

Security Policy, Version 5.2, August 2013, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.2 Physical Access Authorizations, p. 53)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.3 Physical Access Control, p. 53)

The agency shall control physical access to information system distribution and transmission lines within the physically secure location. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.4 Access Control for Transmission Medium, p. 53)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.5 Access Control for Display Medium, p. 53)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.7 Visitor Control, p. 54)

The agency shall authorize and control information system-related items entering and exiting the physically secure location. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.8 Delivery and Removal, p. 54)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.2 Controlled Area, p. 54)

[redacted]

Finding: In Compliance

Recommendation: None

New Policy Finding: In Compliance

Recommendation: *None*

Analysis: *The following agencies did not have a written physical protection policy.*

- *Lodi Police Department*
- *Stockton Police Department*

Security Audits

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.11 Policy Area 11: Formal Audits, 5.11.2 Audits by the CSA, p. 61)

Finding: In Compliance

Recommendation: None

Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, p. 51)

The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.1 Media Storage and Access, p. 51)

New Policy Finding: ***Out of Compliance***

Recommendation: *Ensure the local agencies have a written policy for electronic and physical media that restricts access to authorized individuals.*

Analysis: *The following areas of concern were identified for the new policy requirements assessed. Although corrective action is required, the area of concern will not be forwarded to the APB Compliance Evaluation Subcommittee. The following agencies did not have a written policy to restrict the access to electronic and physical media to authorized personnel:*

- *Lodi Police Department*
- *San Francisco County Sheriff's Office*
- *Stockton Police Department*

Media Transport

The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.2 Media Transport, p. 51)

"Electronic media" means electronic storage media including 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.

Controls shall be in place 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 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 other controls to ensure the security of the data. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.2 Media Transport, 5.8.2.1 Electronic Media in Transit, p. 51)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.2 Media Transport, 5.8.2.2 Physical Media in Transit, p. 51)

New Policy Finding: In Compliance

Recommendation: *None*

Media Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.3 Electronic Media Sanitization and Disposal, p. 51)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, 5.8.4 Disposal of Physical Media, pp. 51-52)

Finding: Out of Compliance

Recommendation: Ensure the local agencies have a written policy for sanitization and destruction of electronic media.

Analysis: The following agencies did not have a written policy for sanitization and destruction of electronic media.

- Anaheim Police Department
- Lodi Police Department
- Los Angeles Police Department
- Santa Ana Police Department
- Stockton Police Department

New Policy Finding: Out of Compliance

Recommendation: Ensure the local agencies document and implement all physical media disposal policies.

Analysis: *The following areas of concern were identified for the new policy requirements assessed. Although corrective action is required, the area of concern will not be forwarded to the APB Compliance Evaluation Subcommittee.*

The following local agencies did not have written procedures for physical media disposal:

- *Anaheim Police Department*
- *Lodi Police Department*
- *Los Angeles Police Department*
- *Stockton Police Department*

The following local agencies did not witness physical media destruction by unauthorized individuals:

- *Los Angeles Police Department*
- *Santa Ana Police Department*

Network Infrastructure Policy Compliance Summary Chart

	Network Configuration	Identification/UserID	Authentication	Session Lock	Event Logging	Advanced Authentication	Encryption	Dial-up Access	Mobile Devices	Personal Firewalls	Boundary Protection	Malicious Code Protection	Security Incident Response
CSA - California Department of Justice	IN	IN	IN	IN	IN	IN	IN		IN	IN	IN	IN	IN
Anaheim Police Department	IN	IN	OUT	OUT	IN	IN	IN			IN	IN	IN	IN
Lodi Police Department	OUT	IN	OUT	IN	OUT	OUT	OUT		IN	OUT	IN	IN	OUT
Los Angeles County Sheriff's Office	IN	IN	IN	IN	IN	IN	IN			IN	IN	IN	IN
Los Angeles Police Department	IN	IN	IN	IN	IN		OUT			IN	IN	IN	IN
Monterey Police Department	IN	IN	IN	IN	OUT		OUT		IN	IN	IN	IN	IN
San Francisco County Sheriff's Office	IN	IN	IN	IN	IN	OUT	IN		IN	IN	IN	IN	OUT
San Francisco Police Department	IN	IN	IN	IN	IN	IN	IN		IN	IN	IN	OUT	IN
Santa Ana Police Department	IN	IN	OUT	OUT	IN	IN	IN			IN	IN	IN	OUT
Stockton Police Department	IN	IN	OUT	IN	IN	OUT	OUT		IN	IN	IN	IN	OUT
Overall Audit Compliance	**IN**	**IN**	**OUT**	**IN**	**IN**	**OUT**	**OUT**	**N/A**	**IN**	**IN**	**IN**	**IN**	**OUT**

New Policy Requirements for Network Infrastructure Compliance Summary Chart

	Personally Owned Information Systems	Publicly Accessible Computers	System Use Notification	Identification/UserID	Authentication	Session Lock	Event Logging	Remote Maintenance	Encryption	Mobile Devices	Cellular Access	Bluetooth Access
CSA - California Department of Justice		NPI	NPI	NPI	NPI	NPI	NPI	NPI	NPI	NPI		
Anaheim Police Department		NPI	NPO	NPO	NPI	NPI	NPO	NPI		NPI	NPI	
Lodi Police Department		NPI	NPO	NPO	NPI	NPI	NPO		NPI	NPI	NPI	
Los Angeles County Sheriff's Office		NPI	NPI	NPO	NPI	NPI	NPI	NPI	NPI	NPI		
Los Angeles Police Department		NPI	NPO	NPO	NPI	NPI	NPI			NPI		
Monterey Police Department		NPI	NPI	NPO	NPI	NPI	NPO	NPI	NPI	NPI	NPI	
San Francisco County Sheriff's Office		NPI	NPO	NPO	NPI	NPI	NPO	NPI		NPI	NPI	
San Francisco Police Department		NPI	NPI	NPI	NPI	NPI	NPO	NPI		NPI	NPI	
Santa Ana Police Department		NPI	NPI	NPI	NPI	NPI	NPO	NPI		NPI	NPI	
Stockton Police Department		NPI	NPO	NPO	NPI	NPI	NPI	NPI	NPI	NPI		

Overall Audit Compliance	**NPN**	**NPI**	**NPO**	**NPO**	**NPI**	**NPI**	**NPO**	**NPI**	**NPI**	**NPI**	**NPI**	**NPN**

New Policy Requirements for Network Infrastructure Compliance Summary Chart (continued)

	Wireless (802.11x) Access	Boundary Protection	Intrusion Detection Tools & Techniques	Malicious Code Protection	Spam and Spyware Protection	Security Alerts and Advisories	Patch Management	Voice over Internet Protocol (VoIP)	Partitioning and Virtualization	Cloud Computing	Security Incident Response
CSA - California Department of Justice		NPI	NPI	NPI	NPI	NPI	NPI		NPI		NPI
Anaheim Police Department		NPI		NPI	NPI	NPI	NPI		NPI		NPI
Lodi Police Department		NPI		NPI	NPI	NPI	NPI		NPI		NPI
Los Angeles County Sheriff's Office		NPI		NPI	NPI	NPI	NPI				NPI
Los Angeles Police Department		NPI		NPI	NPI	NPI	NPI				NPI
Monterey Police Department		NPI		NPI	NPI	NPI	NPI		NPI		NPI
San Francisco County Sheriff's Office		NPI		NPI	NPI	NPI	NPI		NPI		NPI
San Francisco Police Department		NPI		NPI	NPI	NPI	NPO				NPI
Santa Ana Police Department		NPI		NPI	NPI	NPI	NPI				NPI
Stockton Police Department		NPI		NPI	NPI	NPI	NPI				NPI

Overall Audit Compliance	**NPN**	**NPI**	**NPN**	**NPI**	**NPI**	**NPI**	**NPI**	**NPI**	**NPI**	**NPN**	**NPI**

Network Configuration

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.7 Policy Area 7: Configuration Management, 5.7.1 Access Restrictions for Changes, 5.7.1.2 Network Diagram, p. 49)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.7 Policy Area 7: Configuration Management, 5.7.2 Security of Configuration Documentation, p. 49)

Finding: In Compliance

Recommendation: None

Analysis: Lodi Police Department did not have a network diagram.

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 bring your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.5.7.3 Cellular.

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). (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.6.1 Personally Owned Information Systems, p. 32)

New Policy Finding: Not Applicable

Recommendation: *None*

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.6.2 Publicly Accessible Computers, p. 32)

***New Policy Finding:* In Compliance**

Recommendation: *None*

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.4 System Use Notification, p. 31)

New Policy Finding:* *Out of Compliance

Recommendation:* *Ensure the local agencies display an approved system use notification message on all information systems accessing CJI.

Analysis: *The following areas of concern were identified for the new policy requirements assessed. Although corrective action is required, the area of concern will not be forwarded to the APB Compliance Evaluation Subcommittee.*

The following local agencies did not display an approved system use notification message on all information systems accessing CJI:

- *Anaheim Police Department*
- *Lodi Police Department*
- *Los Angeles Police Department*
- *San Francisco Sheriff's Office*
- *Stockton Police Department*

Identification/Userid

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.1 Identification Policy and Procedures, p. 38)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.3 Identification and Authenticator Management, 5.6.3.1 Identifier Management, p. 43)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5. 5 Policy Area 5: Access Control, 5.5.1 Account Management, p. 29)

Finding: In Compliance

Recommendation: None

New Policy Finding: ***Out of Compliance***

Recommendation: Ensure the local agencies document the validation of system accounts.

Analysis: *The following areas of concern were identified for the new policy requirements assessed. Although corrective action is required, the area of concern will not be forwarded to the APB Compliance Evaluation Subcommittee.*

The following local agencies did not document the validation process of system accounts:

- *Anaheim Police Department*
- *Lodi Police Department*
- *Los Angeles Sheriff's Office*
- *Los Angeles Police Department*
- *Monterey Police Department*
- *San Francisco Sheriff's Office*
- *Stockton Police Department*

Authentication

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation,

5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, pp. 38-39)

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). Agencies shall not allow the same authenticator (i.e., password, PIN) to be used multiple times on a device or system. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authenticators, p. 39)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.1 Standard Authenticators, 5.6.2.1.1 Password, p. 39)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.3 Identifier and Authenticator Management, 5.6.3.2 Authenticator Management, p. 43)

Finding: **Out of Compliance**

Recommendation: Ensure the local agencies passwords used for authentication follow the secure password attributes.

Analysis: The Anaheim Police Department's network passwords did not have a password history of eight. The Elite RMS, Cogent, and Versaterm passwords did not meet any of the password requirements.

The Lodi Police Department's passwords were less than eight characters and did not have a password history of at least ten.

The Santa Ana Police Department's Elite RMS and IQ cad passwords did not meet any secure password attributes.

The Stockton Police Department's Tiberon passwords did not expire within a maximum of 90 days.

New Policy Finding: In Compliance

Recommendation: *None*

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 officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement. Note: an example of a session lock is a screen saver with password. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.5 Session Lock, pp. 31-32)

Finding: In Compliance

Recommendation: None

Analysis: The following agencies did not initiate a session lock after a maximum of 30 minutes of inactivity on all information systems accessing CJI:

- Anaheim Police Department – Elite and Versaterm application (on Elite terminals located outside of dispatch and police vehicle)
- Santa Ana Police Department

New Policy Finding: In Compliance

Recommendation: *None*

Event Logging

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5. 4 Policy Area 4: Auditing and Accountability, 5.4.1 Auditable Event and Content (Information Systems), p. 26)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.1 Auditable Event and Content (Information Systems), 5.4.1.1 Events, pp. 26-27)

The following content shall be included with every audited event:

1. Date and time of 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.1 Auditable Event and Content (Information Systems), 5.4.1.1 Events, 5.4.1.1.1 Content, p. 27)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.2 Response to Audit Processing Failures, p. 27)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.3 Audit Monitoring, Analysis, and Reporting, p. 27)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.4 Time Stamps, p. 27)

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.5 Protection of Audit Information, p. 27)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.6 Audit Record Retention, pp. 27-28)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.7 Logging NCIC and III Transactions, p. 28)

Finding: In Compliance

Recommendation: None

Analysis: Ensure the following local agencies log successful and unsuccessful logon attempts and password changes:

- Lodi Police Department
- Monterey Police Department

New Policy Finding: ***Out of Compliance***

Recommendation: **Ensure the local agencies follow all audit log requirements as forth in the CJIS Security Policy.**

Analysis: *The following local agencies did not log successful and successful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource for all information systems accessing CJI.*

- *Lodi Police Department*
- *San Francisco Sheriff's Office*
- *San Francisco Police Department*

The following local agencies did not review their system audit logs, at a minimum of once a week, for appropriate, unusual, or suspicious activity:

- *Anaheim Police Department*
- *San Francisco Sheriff's Office*
- *Santa Ana Police Department*

The Monterey Police Department did not retain audit records for at least 365 days.

Remote Maintenance

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 rationale for such access in the security plan for the information system. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.6 Remote Access, p. 32)

New Policy Finding: ***In Compliance***

Recommendation: *None*

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 public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.2 Advanced Authentication, p. 39)

The requirement to use or not use AA is dependent upon the physical, personnel and technical security controls associated with the user location. 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). 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 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).

INTERIM COMPLIANCE:

1. For interim compliance, users accessing CJI from devices associated with, and located within, a police vehicle are exempt from the AA requirement until September 30th 2014 if the information system being used has not been procured or upgraded anytime after September 30th, 2005. For the purposes of this Policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.
2. Internet Protocol Security (IPSec) does not meet the 2011 requirements for advanced authentication; however, agencies that have funded/implemented IPSec in order to meet the AA requirements of CJIS Security Policy v.4.5 may continue to utilize IPSec for AA until September 30, 2014. Examples:
    a. A police officer runs a query for CJI from his/her laptop mounted in a police vehicle. The police officer leverages a cellular network as the transmission medium; authenticates the device using IPSec key exchange; and tunnels across the cellular network using the IPSec virtual private network (VPN). IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until September 30, 2014.
    b. A detective accesses CJI from various locations while investigating a crime scene. The detective uses an agency managed laptop with IPSec installed and leverages a cellular network as the transmission medium. IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until September 30, 2014.

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 LEO website. The LEO 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.2 Authentication Policy and Procedures, 5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale, pp. 39-40)

Finding: Out of Compliance

Recommendation: Ensure the local agencies use advanced authentication for personnel that manage or access CJI from nonsecure locations.

Analysis: The Lodi Police Department did not provide advanced authentication for remote access to CJI from non-secure locations, for IT staff and private contractors.

The San Francisco County Sheriff's Office did not provide advanced authentication for remote access to their New World system.

The Stockton Police Department did not provide advanced authentication for remote access to their NEKO and Tiberon sytems from non-secure locations.

Encryption

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: See sections 5.5.7.3.2 and 5.10.2.
3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).
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.
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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.2 Encryption, p. 56)

Finding: Out of Compliance

Recommendation: Ensure the local agencies encrypt all network segments that access CJI with at least 128-bit NIST certified encryption to comply with the FIPS 140-2 requirement.

Analysis: The following local agencies did not encrypt all network segments which access or transmit CJI with at least 128-bit NIST certified encryption to comply with the FIPS 140-2 requirement:

- Lodi Police Department did not encrypt their data backup. Also, the agency was unable to provide verification that the encryption used on the wireless and the Internet network segments were at least 128-bit NIST certified.

- Los Angeles Police Department transmitted CJI over the city network which was encrypted but the agency was unable to provide verification that the encryption used was at least 128-bit NIST certified.

- The Monterey Police Department did not encrypt the city network that transmitted CJI to their backup site. Also, the agency was unable to provide verification that the encryption used on the wireless network segments were at least 128-bit NIST certified.

- The Stockton Police Department did not encrypt the public network segment between their buildings. Also, the agency was unable to provide verification that the encryption used on the wireless network segments were at least 128-bit NIST certified.

New Policy Finding: In Compliance

Recommendation: *None*

Dial-up 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 rationale for such access in the security

plan for the information system. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.6 Remote Access, p. 32)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.2 Access Enforcement, pp. 29)

Finding: Not Applicable

Recommendation: None

Mobile Devices

The agency shall: (i) establish usage restrictions and implementation guidance for wireless technologies; 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.

Examples of wireless technologies include, but are not limited to: 802.11x, cellular networks, Bluetooth, satellite and microwave. Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology, may require some additional security controls as described below. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.7 Wireless Access Restrictions, p. 32)

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].

Devices that have been rooted, jailbroken, or have had any unauthorized changes made to them shall not be used to process, store, or transmit CJI data at any time. In addition to the security controls described in this Policy, agencies shall implement the following controls when allowing CJI access from cell/smart phones and tablet devices:

1. CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration capable of at least:
    i. Remote locking of device
    ii. Remote wiping of device
    iii. Setting and locking device configuration
    iv. Detection of "rooted" and "jailbroken" devices
    v. Enforce folder or disk level encryption (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.7 Wireless Access Restrictions, 5.5.7.3 Cellular, 5.5.7.3.3 Mobile Device Management (MDM), p. 35)

Finding: In Compliance

Recommendation: None

New Policy Finding: In Compliance

Recommendation: *None*

Personal Firewalls

A personal firewall shall be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.). 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. 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 PC.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10. 4 System and Information Integrity Policy and Procedures, 5.10.4.4 Personal Firewall, pp. 59-60)

Finding: In Compliance

Recommendation: None

Analysis: The Lodi Police department did not implement personal firewalls on their wireless access devices.

Cellular Access

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), personal digital assistants (PDA), and "aircards" are examples of cellular handheld devices or devices that employ 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. Cellular devices are at risk due to a multitude of threats and consequently pose a risk to the enterprise.

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 law enforcement officer).
7. Cloning (not as prevalent with later generation cellular technologies). \
8. Server-resident data. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.7 Wireless Access Restrictions, 5.5.7.3 Cellular, p. 34)

Organizations shall, at a minimum, ensure that cellular 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.
3. Use advanced authentication.
4. Encrypt all CJI resident on the device.
5. Erase cached information 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 antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.7 Wireless Access Restrictions, 5.5.7.3 Cellular, 5.5.7.3.1 Cellular Risk Mitigations, pp. 34-35)

New Policy Finding: In Compliance

Recommendation: *None*

Bluetooth Access

Bluetooth is an open standard for short-range radio frequency (RF) communication and is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc networks or piconets. A piconet is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence and can scale to include up to seven active slave devices and up to 255 inactive slave devices. Bluetooth voice and data transfer technology has been integrated into many types of business and consumer

devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets.

Bluetooth does not provide end-to-end, audit, or non-repudiation security services. If such services are needed, they shall be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards.

The cryptographic algorithms employed by the Bluetooth standard are not FIPS approved. When communications require FIPS-approved cryptographic protection, this can be achieved by employing application-level FIPS-approved encryption over the native Bluetooth encryption. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.7 Wireless Access Restrictions, 5.5.7.4 Bluetooth, pp. 35-36)

***New Policy Finding:* Not Applicable**

Recommendation: *None*

Wireless (802.11x) Access

Agencies shall:

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 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 unless the environment is such that the risk has been assessed and is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.

12. Disable all nonessential management protocols on the APs and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption.
13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
14. Segregate, 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.
15. 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.7 Wireless Access Restrictions, 5.5.7.1 All 802.11x Wireless Protocols, pp. 32-33)

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and are to be used only if additional security controls are employed.

Agencies shall follow the guidelines below regarding wireless implementation and cases where the WEP and WPA security features are used to provide wireless security in conjunction with the CJIS required minimum encryption specifications.

1. Deploy media access control (MAC) access control lists (ACL); however, MAC ACLs do not represent a strong defense mechanism by themselves because they are transmitted in the clear from WLAN clients to APs so they can be captured easily.
2. Enable WEP/WPA.
3. Ensure the default shared keys are replaced by more secure unique keys.
4. Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.7 Wireless Access Restrictions, 5.5.7.2 Legacy 802.11 Protocols, p. 34)

New Policy Finding: ***Not Applicable***

Recommendation: *None*

Boundary Protection

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, p. 55)

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 5.10.4.4 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.1 Boundary Protection, pp. 55-56)

Finding: In Compliance

Recommendation: None

New Policy Finding: In Compliance

Recommendation: *None*

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.3 Intrusion Detection Tools and Techniques, p. 56)

New Policy Finding: Not Applicable

Recommendation: *None*

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10. 4 System and Information Integrity Policy and Procedures, 5.10.4.2 Malicious Code Protection, p. 59)

Finding: In Compliance

Recommendation: None

New Policy Finding: In Compliance

Recommendation: *None*

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/or 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10. 4 System and Information Integrity Policy and Procedures, 5.10.4.3 Spam and Spyware Protection, p. 59)

New Policy Finding: In Compliance

Recommendation: *None*

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.4 System and Information Integrity Policy and Procedures, 5.10.4.5 Security Alerts and Advisories, p. 60)

New Policy Finding: In Compliance

Recommendation: *None*

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications

Protection and Information Integrity, 5.10.4 System and Information Integrity Policy and Procedures, 5.10.4.1 Patch Management, pp. 58-59)

New Policy Finding: In Compliance

Recommendation: *None*

Voice over Internet Protocol (VoIP)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.4 Voice Over Internet Protocol, pp. 56-57)

New Policy Finding: In Compliance

Recommendation: *None*

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.3 Partitioning and Virtualization, p. 57)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.3 Partitioning and Virtualization, 5.10.3.1 Partitioning, pp. 57-58)

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 that process CJI internally.
4. Device drivers that are "critical" shall be contained within a separate guest.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Encrypt network traffic between the virtual machine and host.
2. Implement IDS and IPS monitoring within the virtual machine environment.
3. Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact.
4. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.3 Partitioning and Virtualization, 5.10.3.2 Virtualization, p. 58)

New Policy Finding: In Compliance

Recommendation: *None*

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, 5.10.1.5 Cloud Computing, p. 57)

New Policy Finding: Not Applicable

Recommendation: *None*

Security Incident Response

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. Agencies shall: (i) establish an operational incident handling capability for agency information systems that includes 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 an incident to the FBI CJIS ISO. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, p. 23)

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems 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

information security events and weaknesses as quickly as possible to the designated point of contact. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.1 Reporting Information Security Events, p. 23)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.1 Reporting Information Security Events, 5.3.1.1 Reporting Structure and Responsibilities, 5.3.1.1.2 CSA ISO Responsibilities, pp. 23-24)

A consistent and effective approach shall be applied to the management of information security incidents. Responsibilities and procedures shall be in place to handle information security events and weaknesses effectively once they have been reported. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.2 Management of Information Security Incidents, p. 24)

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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.2 Management of Information Security Incidents, 5.3.2.1 Incident Handling, p. 23)

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). (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.2 Management of Information Security Incidents, 5.3.2.2 Collection of Evidence, p. 24)

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.3 Incident Response Training, p. 24)

The agency shall track and document information system 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. (*CJIS Security Policy*, Version 5.2, August 2013, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.4 Incident Monitoring, pp. 24-25)

Finding: Out of Compliance

Recommendation: Ensure the local agencies develop an information security incident response policy.

Analysis: The following local agencies did not have an operational information security incident response policy which includes written reporting procedures:

- Lodi Police Department
- San Francisco Sheriff's Office
- Santa Ana Police Department
- Stockton Police Department

New Policy Finding: In Compliance

Recommendation: *None*