Information Technology Security Audit (ITSA)

Local Agency Policy Assessment

<table>
<thead>
<tr>
<th>Agency Name and ORI</th>
<th>Asheville Police Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Date</td>
<td>Thursday, May 9, 2013 @ 1:00 pm</td>
</tr>
<tr>
<td>FBI's CJIS Division Auditor(s):</td>
<td>Christopher Wright – 304-625-2933</td>
</tr>
</tbody>
</table>
Table of Contents

INTRODUCTION
Information Technology Security Audit (ITSA) .................................................. 2
FBI CJIS Security Policy 5.1 Transition Document Introduction .......................... 3

1.0 SYSTEM ADMINISTRATION
Local Agency Security Officer (LASO) .............................................................. 4

2.0 ADMINISTRATION OF CRIMINAL JUSTICE FUNCTIONS
Noncriminal Justice Agencies ............................................................................. 5
Private Contractors .......................................................................................... 5
Agency Coordinator ......................................................................................... 6
Management Control ....................................................................................... 7

3.0 INFORMATION PROTECTION
IT Security Program ........................................................................................ 8
Standards of Enforcement .............................................................................. 8
Standards of Discipline .................................................................................. 9
Personnel Security .......................................................................................... 9
Security Awareness Training ....................................................................... 11
Physical Security ............................................................................................ 13
Media Protection ............................................................................................ 15
Media Transport ............................................................................................. 15
Media Disposal ............................................................................................... 16

4.0 NETWORK INFRASTRUCTURE
Network Configuration .................................................................................... 17
Personally Owned Information Systems ....................................................... 17
Publicly Accessible Computers .................................................................... 18
Identification/UserID ..................................................................................... 18
Authentication ............................................................................................... 19
Event Logging ............................................................................................... 20
Advanced Authentication .............................................................................. 22
Encryption ...................................................................................................... 23
Dial-up Access ............................................................................................... 24
Mobile Devices ............................................................................................. 25
Personal Firewalls ......................................................................................... 25
Cellular Access ............................................................................................. 26
Bluetooth Access .......................................................................................... 26
Wireless (802.11x) Access .......................................................................... 28
Boundary Protection ...................................................................................... 29
Malicious Code Protection .......................................................................... 30
Spam and Spyware Protection .................................................................... 31
Security Alerts and Advisories .................................................................... 31
Patch Management ......................................................................................... 31
Voice over Internet Protocol ......................................................................... 32
Partitioning and Virtualization .................................................................... 33
Security Incident Response .......................................................................... 34

APPENDIX A - CRIMINAL JUSTICE INFORMATION (CJI) AND PERSONALLY IDENTIFIABLE INFORMATION (PII)
Criminal Justice Information (CJI) ............................................................... 37
Personally Identifiable Information (PII) ...................................................... 38

APPENDIX B - TERMS AND DEFINITIONS .................................................. 39
Introduction

Information Technology Security Audit (ITSA)

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.

The CJIS Security Policy provides the minimum level of IT security requirements determined acceptable for the transmission, processing, and storage of the nation's CJIS data. The full application of these requirements is necessary to establish uniformity and consistency in safeguarding FBI CJIS systems data which is accessed via networks throughout the local, state, tribal, and federal user communities.

The ITSA is an important tool for determining the potential need for additional security controls to protect FBI CJIS systems information. The ITSA is conducted to assess and evaluate the security posture of criminal justice agencies directly connected with the FBI CJIS systems. The FBI CJIS Division auditors analyze the CSA's enforcement of security controls through meetings with personnel assigned to both the CSA and local agencies. During these meetings, auditors discuss and assess policy requirements to include, but not limited to: security enforcement, physical and technical security, encryption, identification, authentication, firewalls, and virus protection. The FBI CJIS Division auditors review methods used by the CSA to administer the policies and procedures contained in the CJIS Security Policy to the agencies which it provides service. Additionally, the ITSA is comprised of network inspections, system inquiries, and test scenarios of the FBI CJIS systems to assess, evaluate, and verify technical security compliance and to provide guidance for achieving compliance.

A policy assessment packet is provided to each agency at the close of the ITSA to assist agencies in understanding and implementing crucial policies and procedures related to IT security and the protection of FBI CJIS systems data. Each policy assessed during the ITSA is provided along with its location within the CJIS Security Policy. The FBI CJIS Division auditor's assessment is provided below each policy. To further aid agencies in following the assessment, terms used are explained below.

<table>
<thead>
<tr>
<th>IN</th>
<th>OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency is IN compliance with policy/procedure.</td>
<td>Agency is OUT of compliance with policy/procedure. <strong>Corrective Action is needed.</strong></td>
</tr>
<tr>
<td>N/A (Not Applicable)</td>
<td>Policy/procedure is not applicable to the agency and therefore not assessed.</td>
</tr>
<tr>
<td>NPI (New Policy IN)</td>
<td>New policy required by January 1st, of &quot;required by&quot; year noted in policy. Agency is IN compliance but policy is in zero cycle and will not be reported to the APB Compliance Evaluation Subcommittee.</td>
</tr>
<tr>
<td>NPO (New Policy OUT)</td>
<td>New policy required by January 1st, of &quot;required by&quot; year noted in policy. Agency is OUT of compliance but policy is in zero cycle and will not be reported to the APB Compliance Evaluation Subcommittee. <strong>Corrective Action is needed.</strong></td>
</tr>
<tr>
<td>NPN (New Policy N/A)</td>
<td>New policy required by January 1st of &quot;required by&quot; year noted in policy. Policy is not applicable to the agency and will not be reported to the APB Compliance Evaluation Subcommittee.</td>
</tr>
</tbody>
</table>

Revised 201300401
Requirements and Transition Document
FBI CJIS Security Policy Version 5.1
07/12/2012

Requirement Dates Between 2011-2014

Changes to the CJIS Security Policy v5.0 were approved by the Advisory Policy Board (APB) in 2011, and subsequently approved by the Direct, FBI, on June 1, 2012. The policy contains current requirements carried over from version 4.5 and 5.0 along with new requirements for agencies to implement.

This document lists every new requirement and its “required by” year from 2011-2014* based on a number of factors including, among other things: cost, threat, technological innovations, and realistic need. Those cases where prior version requirements were assigned a specific “required by” date, i.e. September 30th, 2013, that date has been carried over. CJIS auditors will conduct zero-cycle audits beginning October 1st of the “required by” year. For example, new requirements with a “required by” year of 2012 will fall under the zero-cycle audit beginning October 1st, 2012. Noncriminal Justice Agencies that have not previously been subject to CJIS Security Policy audit and whose only access to FBI CJIS data is for the purpose of civil fingerprint-based background checks or other noncriminal justice purposes will not undergo zero-cycle audits until October 1st, 2013.

The “Summary of Changes” page lists requirements that were added, deleted, or changed from version 5.0 and now reflect in version 5.1. Within the transition document, these modifications are highlighted for ease of location. For continuity, there are columns on the left that reflect policy locations from version 4.5 forward. As new versions are released, these columns will change to indicate current requirement locations in the policy.

Though the dates applied to requirements are spread across several years, the intent is for agencies to start working toward them immediately, where possible, and leverage the requirements document as a tool for financial planning and justification to meet requirements that cannot be met immediately.

Please refer questions or comments about this requirements document or version 5.1 of the CJIS Security Policy to your respective Information Security Officer, CJIS Security Officer, or Compact Officer.

* A requirement with “required by” year without a corresponding month and day is to be read as January 1st of that year.
1.0 System Administration

1.1 Local Agency Security Officer (LASO)

(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)

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.

Compliance:
2.0 Administration of Criminal Justice Functions

2.1 Noncriminal Justice Agencies

(CJIS Security Policy, Version 5.1, July 2012, 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)

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 IT department.

Compliance:

2.2 Private Contractors

(CJIS Security Policy, Version 5.1, July 2012, 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)

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 criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information 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
2.2 Private Contractors (continued)

3. 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).

Compliance: 


2.3 Agency Coordinator

(CJIS Security Policy, Version 5.1, July 2012, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.6 Contracting Government Agency (CGA), p. 7)

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 is to appoint an agency coordinator.

(CJIS Security Policy, Version 5.0, February 2011, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.7 Agency Coordinator (AC), p. 7)

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.
2.3 Agency Coordinator (continued)

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.

2.4 Management Control

(CJIS Security Policy, Version 5.1, July 2012, 3 Roles and Responsibilities, 3.2 Roles and Responsibilities for Agencies and Parties, 3.2.2 CJIS Systems Officer (CSO), pp. 5-6)

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 CJIS data; and to guarantee the priority service as determined by the criminal justice community.
3.0 Information Protection

3.1 IT Security Program

(CJIS Security Policy, Version 5.1, July 2012, 1 Introduction, 1.3 Relationship to Local Security Policy and Other Policies, p. 1)

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 (2011 Requirement) 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.

Compliance:

3.2 Standards of Enforcement

(CJIS Security Policy, Version 5.1, July 2012, 3 Roles and Responsibilities, 3.2 Roles and responsibilities for Agencies and Parties, p. 4)

It is the responsibility of all agencies covered under this policy to ensure the protection of CJI between the FBI CJIS Division and its user community.


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.

Compliance:
3.3 Standards of Discipline


The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Compliance:

3.4 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 CJII and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJII. However, if the person resides in a different state than that of the assigned agency, the agency shall (2013 Requirement) 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 (2012 Requirement) 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. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJII. All CSO designees shall be from an authorized criminal justice agency.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJII. 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 CJII. 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 CJII 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 CJII 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 CJII 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 CJII and is subsequently arrested and or convicted, continued access to CJII shall (2011 Requirement) be determined by the
3.4 Personnel Security (continued)

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.


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 a 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. (2012 Requirement)

5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants. (2012 Requirement)

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. (2012 Requirement)

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.
3.4 Personnel Security (continued)

The agency shall (2012 Requirement) 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.

Compliance: 

NP Compliance: 

3.5 Security Awareness Training

Basic security awareness training shall (2013 Requirement) 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 5.1, July 2012, 5 Policy and Implementation, 5. 2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, p. 19)
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 5.1, July 2012, 5 Policy and Implementation, 5.2 Policy Area 2: Security Awareness Training, 5.2.1 Awareness Topics, 5.2.1.1 All Personnel, p. 19)
At a minimum, the following topics shall (2013 Requirement) 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. Dissemination and destruction.
3.5 Security Awareness Training (continued)

(CJIS Security Policy, Version 5.1, July 2012, 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. 19-20)

In addition to 5.2.1.1 above, the following topics, at a minimum, shall (2013 Requirement) be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJIS:

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.
7. Social engineering.
8. Physical Security—increases in risks to systems and data.
10. Handheld device security issues—address both physical and wireless security issues.
11. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
12. Laptop security—address both physical and information security issues.
13. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
14. Access control issues—address least privilege and separation of duties.
15. Individual accountability—explain what this means in the agency.
16. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
17. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
18. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
19. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

(CJIS Security Policy, Version 5.1, July 2012, 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. 20)

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics at a minimum shall (2013 Requirement) 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.
3.5 Security Awareness Training (continued)

3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

Records of individual basic security awareness training and specific information system security training shall (2013 Requirement) be documented, kept current, and maintained by the CSO/SIB/Compact Officer. Maintenance of training records can be delegated to the local level.

3.6 Physical Security
Physical protection policy and procedures shall (2011 Requirement) 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 5.1, July 2012, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, p. 49)
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 – 5.9.1.9 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.

For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall (2011 Requirement) be considered a physically secure location until September 30th 2013. 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 5.1, July 2012, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.1 Security Perimeter, p. 49)
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 5.1, July 2012, 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. 49)
The agency shall (2013 Requirement) 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 (2013 Requirement) issue credentials to authorized personnel.

(CJIS Security Policy, Version 5.1, July 2012, 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. 49)
The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall (2011 Requirement) verify individual access authorizations before granting access.

(CJIS Security Policy, Version 5.1, July 2012, 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. 49)
The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

(CJIS Security Policy, Version 5.1, July 2012, 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. 49)
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 5.1, July 2012, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.7 Visitor Control, p. 50)
The agency shall (2011 Requirement) 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 5.1, July 2012, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.1 Physically Secure Location, 5.9.1.9 Delivery and Removal, p. 50)
The agency shall (2013 Requirement) authorize and control information system-related items entering and exiting the physically secure location.

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.9 Policy Area 9: Physical Protection, 5.9.2 Controlled Area, p. 50)
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 (2013 Requirement) 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 (2012 Requirement), 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.
3.6 Physical Security (continued)

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.

Compliance:

NP Compliance: Does not have a written physical protection policy

3.7 Media Protection

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.8 Policy Area 8: Media Protection, p. 47)
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.

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.

NP Compliance:

3.8 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.

“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

Revised 201300401
3.8 Media Transport (continued)

optimal control during transport; however, if encryption of the data isn’t possible then each agency shall (2011 Requirement) institute other controls to ensure the security of the data.

(CJIS Security Policy, Version 5.1, July 2012, 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 47)
The controls and security measures in this document also apply to CJIs in physical (printed documents, printed imagery, etc.) form. Physical media shall (2011 Requirement) be protected at the same level as the information would be protected in electronic form.

NP ☑ Compliance:

3.9 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 (2011 Requirement) ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

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 (2011 Requirement) minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall (2011 Requirement) ensure the disposal or destruction is witnessed or carried out by authorized personnel.

☑ Compliance:

NP ☑ Compliance:
4.0 Network Infrastructure

4.1 Network Configuration
(CJIS Security Policy, Version 5.1, July 2012, 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. 45)
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” (FOOU) markings.
4. The agency name and date (day, month, and year) drawing was created or updated. (2012 Requirement)

The system configuration documentation often contains sensitive details (e.g., descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall (2012 Requirement) protect the system documentation from unauthorized access consistent with the provisions described in section 5.5 Access Control.

Compliance: 

4.2 Personally Owned Information Systems
(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.6.1 Personally Owned Information Systems, p. 31)
A personally owned information system shall (2011 Requirement) not be authorized to access, process, store or transmit CJIS unless the agency has established and documented the specific terms and conditions for personally owned information system usage.

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).

Compliance: 

Revised 20130421
4.3 Publicly Accessible Computers

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.6.2 Publicly Accessible Computers, p. 31)

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

NP \( \checkmark \) Compliance:

4.4 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 5.1, July 2012, 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. 41)

In order to manage user identifiers, agencies shall (2012 Requirement):

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 5.1, July 2012, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.1 Account Management, p. 28)

The agency shall (2012 Requirement) manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall (2012 Requirement) validate information system accounts at least annually and shall (2012 Requirement) 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 (2013 Requirement) identify authorized users of the information system and specify access rights/privileges. The agency shall (2012 Requirement) grant access to the information system based on:
4.4 Identification/User ID (continued)

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 (2013 Requirement) 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.

TKS Compliance:

NP O Compliance: Does not document the validation process for system accounts

4.5 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 (2011 Requirement) 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.


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. (2012 Requirement)
4.5 Authentication (continued)

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.6 Policy Area 6: Identification and Authentication, 5.6.3 Identifier and Authenticator Management, 5.6.5.2 Authenticator Management, pp. 41-42)

In order to manage information system authenticators, agencies shall (2012 Requirement):

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.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall (2012 Requirement) 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.

\[
\begin{align*}
\text{IN} & \quad \text{Compliance:} \\
\text{NP} & \quad \text{Compliance: Does not verify identity of all users who need password record.}
\end{align*}
\]

4.6 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 (2013 Requirement) 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 (2013 Requirement) 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 (2013 Requirement) still take place.

(CJIS Security Policy, Version 5.1, July 2012, 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, p. 25)

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource. (2013 Requirement)
3. Successful and unsuccessful attempts to change account passwords.
4.6 Event Logging (continued)

4. Successful end unsuccessful actions by privileged accounts. *(2013 Requirement)*
5. Successful end unsuccessful attempts for users to access, modify, or destroy the audit log file. *(2013 Requirement)*

*(CJIS Security Policy, Version 5.1, July 2012, 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, pp. 25-26)*

The following content *shall* *(2013 Requirement)* 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.
5. Outcome (success or failure) of the event.

*(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.2 Response to Audit Processing Failures, p. 26)*

The agency’s information system *shall* *(2013 Requirement)* 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.


The responsible management official *shall* *(2013 Requirement)* 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* *(2013 Requirement)* 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* *(2013 Requirement)* 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 5.1, July 2012, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.4 Time Stamps, p. 26)*

The agency’s information system *shall* *(2013 Requirement)* provide time stamps for use in audit record generation. The time stamps *shall* *(2013 Requirement)* 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 5.1, July 2012, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.5 Protection of Audit Information, p. 26)*

The agency’s information system *shall* *(2013 Requirement)* protect audit information and audit tools from modification, deletion and unauthorized access.
4.6 Event Logging (continued)

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.6 Audit Record Retention, p. 26)
The agency shall (2012 Requirement) retain audit records for at least 365 days. Once the minimum retention time period has passed, the agency shall (2013 Requirement) 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 5.1, July 2012, 5 Policy and Implementation, 5.4 Policy Area 4: Auditing and Accountability, 5.4.7 Logging NCIC and III Transactions, p. 26) 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. I.I 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.

Compliance:

NP  Compliance:

4.7 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 5.1, July 2012, 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. 38-39) The requirement to use or not use AA is dependent upon the physical, personnel and technical security controls associated with the user location. For example, 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.
4.7 Advanced Authentication (continued)

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 2013 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 2013. 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 2013.

   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 2013.

EXCEPTION:

AA shall (2012 Requirement) 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.

\[\text{Compliance:}\]

4.8 Encryption

(CJIS Security Policy, Version 5.1, July 2012, 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. 53)

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.
4.8 Encryption (continued)

3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall (2013 Requirement) 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 compliance 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 (2013 Requirement) 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 (2013 Requirement):
   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.

4.9 Dial-up Access

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.6 Remote Access, p. 31)

The agency shall (2013 Requirement) 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 (2013 Requirement) employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall (2013 Requirement) 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 (2013 Requirement) document the rationale for such access in the security plan for the information system.

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.2 Access Enforcement, pp. 28)

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall (2012 Requirement) restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.
4.9 Dial-up Access (continued)

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 (2013 Requirement) 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.

\[ \text{Compliance:} \]

4.10 Mobile Devices

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.7 Wireless Access Restrictions, p. 31)

The agency shall (2012 Requirement): (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.

\[ \text{NP \ Compliance:} \]

4.11 Personal Firewall

(CJIS Security Policy, Version 5.1, July 2012, 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, p. 56)

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 computer, 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.

\[ \text{Compliance:} \]
4.12 Cellular Access

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.7 Wireless Access Restrictions, 5.5.7.3 Cellular, pp. 33)

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 5.1, July 2012, 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. 33-34)

Organizations shall (2012 Requirement), at a minimum, ensure that cellular devices:

1. Apply available critical patches and upgrades to the operating system.
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.
7. Employ antivirus software.

NP Compliance:

4.13 Bluetooth Access

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.5 Policy Area 5: Access Control, 5.5.7 Wireless Access Restrictions, 5.5.7.4 Bluetooth, pp. 34-35)

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,
4.13 Bluetooth Access (continued)

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.

Agencies shall:

1. Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization’s information system resource.

2. Maintain a complete inventory of all Bluetooth-enabled wireless devices and addresses (BD_ADDRs). A complete inventory of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.

3. Change the default setting of the Bluetooth device to reflect the organization’s security policy. Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the organization’s security policy.

4. Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization. Setting Bluetooth devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users. The use of Class 1 devices should be avoided due to their extended range (approximately 100 meters).

5. Choose personal identification number (PIN) codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes. PIN codes should be random so that they cannot be easily reproduced by malicious users. Longer PIN codes are more resistant to brute force attacks. For Bluetooth v2.0 (or earlier) devices, an eight-character alphanumeric PIN shall be used.

6. For v2.1 devices using Secure Simple Pairing, avoid using the “Just Works” model. The “Just Works” model does not provide protection against man-in-the-middle (MITM) attacks. Devices that only support Just Works should not be procured if similarly qualified devices that support one of the association models (i.e. Numeric Comparison, Out of Band, or Passkey Entry) are available.

7. Bluetooth devices should be configured by default as, and remain, undiscoverable except as needed for pairing. Bluetooth interfaces should be configured as non-discoverable, which prevents visibility to other Bluetooth devices except when discovery is specifically needed. Also, the default self-identifying or discoverable names provided on Bluetooth devices should be changed to anonymous, unidentifiable names.
4.13 Bluetooth Access (continued)

8. Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e. no Security Mode 1). Link encryption should be used to secure all data transmissions during a Bluetooth connection; otherwise, transmitted data is vulnerable to eavesdropping.

9. If multi-hop wireless communication is being utilized, ensure that encryption is enabled on every link in the communication chain. Every link should be secured because one unsecured link results in compromising the entire communication chain.

10. Ensure device mutual authentication is performed for all accesses. Mutual authentication is required to provide verification that all devices on the network are legitimate.

11. Enable encryption for all broadcast transmission (Encryption Mode 3). Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user intercept for malicious purposes.

12. Configure encryption key sizes to the maximum allowable. Using maximum allowable key sizes provides protection from brute force attacks.

13. Establish a "minimum key size" for any negotiation process. Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks. See Section 5.10.1.2 for minimum key encryption standards.

14. Use Security Mode 3 in order to provide link-level security prior to link establishment.

15. Users do not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, and images. With the increase in the number of Bluetooth enabled devices, it is important that users only establish connections with other trusted devices and only accept content from these trusted devices.

NP  \[\_\_\_\_\_\_\_\_\_\_\_\_] Compliance:

4.14 Wireless (802.11x) Access

(CJIS Security Policy, Version 5.1, July 2012, 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. 31-32)

Agencies shall (2012 Requirement):

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 5.1, July 2012, 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. 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 (2012 Requirement) 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.

NP \[\checkmark\] Compliance:
4.15 Boundary Protection

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.1 Information Flow Enforcement, p. 52)

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 5.1, July 2012, 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. 52-53)

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. (2013 Requirement)
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. (2013 Requirement)
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”). (2011 Requirement)
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. (2012 Requirement)

TJ Compliance: 

NP Compliance: 

4.16 Malicious Code Protection

(CJIS Security Policy, Version 5.1, July 2012, 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, pp. 55-56)

The agency shall (2012 Requirement) implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall (2012 Requirement) 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 (2011 Requirement) ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

Compliance:

4.17 Spam and Spyware Protection

(CJIS Security Policy, Version 5.1, July 2012, 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. 56)

The agency shall (2012 Requirement) implement spam and spyware protection.

The agency shall (2012 Requirement):

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 document.

Compliance:

4.18 Security Alerts and Advisories

(CJIS Security Policy, Version 5.1, July 2012, 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, pp. 56-57)

The agency shall (2012 Requirement):

1. Receive information system security alerts/advisories on a regular basis.
4.18 Security Alerts and Advisories (continued)

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.

NP Compliance:

4.19 Patch Management

(CJIS Security Policy, Version 5.1, July 2012, 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, p. 55)

The agency shall (2011 Requirement) 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 (2011 Requirement) 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 (2012 Requirement) also be addressed expeditiously.

NP Compliance:

4.20 Voice over Internet Protocol

(CJIS Security Policy, Version 5.1, July 2012, 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. 53-54)

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 (2011 Requirement) be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:
4.20 Voice over Internet Protocol (continued)

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. (2013 Requirement)

NP ∨ Compliance:

4.21 Partitioning and Virtualization
(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.10 Policy Area 10: System and Communications Protection and Information Integrity, 5.10.3 Partitioning and Virtualization, p. 54)
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 5.1, July 2012, 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, p. 54)
The application, service, or information system shall (2012 Requirement) separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall (2012 Requirement) 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 5.1, July 2012, 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, pp. 54-55)
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 (2012 Requirement) 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.

Revised 2013060401
4.21 Partitioning and Virtualization (continued)

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 (2012 Requirement) 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 provides some reference and additional background information on virtualization.

NP □ Compliance:

4.22 Security Incident Response
(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, p. 22)

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 (2012 Requirement): (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 (2012 Requirement) 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 5.1, July 2012, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.1 Reporting Information Security Events, p. 22)

The agency shall (2012 Requirement) promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall (2012 Requirement) 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 (2012 Requirement) employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall (2012 Requirement) 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 5.1, July 2012, 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. 22-23)

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.


A consistent and effective approach shall (2012 Requirement) 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 5.1, July 2012, 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)

The agency shall (2013 Requirement) implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall (2013 Requirement) 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 implements the procedures accordingly.
4.22 Security Incident Response (continued)

(CJIS Security Policy, Version 5.1, July 2012, 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. 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 (2012 Requirement) be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

(CJIS Security Policy, Version 5.1, July 2012, 5 Policy and Implementation, 5.3 Policy Area 3: Incident Response, 5.3.3 Incident Response Training, p. 23)
The agency shall (2012 Requirement) ensure general incident response roles responsibilities are included as part of required security awareness training.

The agency shall (2012 Requirement) track and document information system security incidents on an ongoing basis. The CSA ISO shall (2012 Requirement) 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.

\[ \text{Compliance:} \] \\
\[ \text{NP} \

\[ \text{Compliance:} \]
APPENDIX A – CRIMINAL JUSTICE INFORMATION (CJI) AND PERSONALLY IDENTIFIABLE INFORMATION (PII)

The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI from: creation through dissemination, whether at rest or in transit. It is the responsibility of all agencies covered under the CJIS Security Policy to ensure the protection of CJI between the FBI CJIS Division and its user community.

Any information system(s) containing CJI, which includes the subset of personally identifiable information (PII) and criminal history record information (CHRI), must meet the minimum security standards as required by the CJIS Security Policy. (PLEASE NOTE: CAD and/or RMS systems that store CJI data must meet all technical security requirements including such things as encryption, authentication, virus protection, boundary protection, advanced authentication, etc.)

Criminal Justice Information (CJI)

(CJIS Security Policy, Version 5.1, July 2012, 4 Criminal Justice Information and Personally Identifiable Information, 4.1 Criminal Justice Information (CJI), p. 10)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.

2. Identity History Data—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

4. Property Data—information about vehicles and property associated with crime.

5. Case/Incident History—information about the history of criminal incidents.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.
Personally Identifiable Information (PII)
(CJIS Security Policy, Version 5.1, July 2012, 4 Criminal Justice Information and
Personally Identifiable Information, 4.3 Personally Identifiable Information (PII), p. 12)

For the purposes of this document, PII is information which can be used to distinguish or
trace an individual's identity, such as name, social security number, or biometric
records, alone or when combined with other personal or identifying information which is
linked or linkable to a specific individual, such as date and place of birth, or mother’s
maiden name. Any FBI CJIS provided data maintained by an agency, including but not
limited to, education, financial transactions, medical history, and criminal or
employment history may include PII. A criminal history record for example inherently
contains PII as would an N-DEx case file.

PII shall (2012 Requirement) be extracted from CJI for the purpose of official business only.
Agencies shall (2012 Requirement) develop policies, based on state and local privacy rules, to
ensure appropriate controls are applied when handling PII extracted from CJI. Due to
the expansive nature of PII, this policy does not specify auditing, logging, or personnel
security requirements associated with the life cycle of PII.
Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g., record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI data.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user’s responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.
Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Escort — Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Identity History Data — Textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA’s authority remains with regard to all aspects of section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Physically Secure Location — 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. For interim compliance, a police vehicle shall be considered a physically secure location until September 30th, 2013. 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.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual’s identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name.

Property Data — Information about vehicles and property associated with a crime.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.