CJIS Security Policy

2016 CJIS Training Conference

Jeff Campbell
FBI CJIS Assistant Information Security Officer
AGENDA

• CJIS Security Policy Shared Management Philosophy
• Advisory Policy Overview
• CJIS Security Policy New Changes in v5.5
• FBI CJIS ISO Resources
CJIS Security Policy

Shared Management Philosophy
Where does criminal justice information (CJI) come from?

- State
- Local
- Tribal
- Federal

Because the information is shared...

- The FBI CJIS Division employs a shared management philosophy with state, local, tribal, and federal law enforcement agencies.

What does ‘shared management’ mean?

- Through the Advisory Policy Board process, the FBI along with state, local, tribal, and federal data providers and system users share responsibility for the protection of CJI and the operation and management of all systems administered by the CJIS Division for the benefit of the criminal justice community.
How does ‘shared management’ work?

- Designation of a CJIS Systems Agency (CSA)
- Designation of a CJIS Systems Officer (CSO)
- CJIS Advisory Process

The CJIS Advisory Process is used to...

- obtain the user community’s advice and guidance on the operation of all of the CJIS programs
- establish a minimum standard of requirements to ensure continuity of information protection (write minimum policy standards)
- represent the shared responsibility between the FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI
Advisory Policy Overview
CJIS ADVISORY PROCESS

Two Cycles Annually
• Spring and Fall
• Working Groups, Subcommittees, Board
• FBI Director approval
• Topic Papers

CJIS Advisory Policy Board

9 Subcommittees

5 Working Groups
WHAT DO THE WORKING GROUPS (WGs) DO?

• Review operational, policy, and technical issues related to CJIS Division programs and policies and make recommendations to the APB or one of its subcommittees

• All 50 states, as well as U.S. territories and the Canadian Police Information Centre (CPIC) are organized into 5 Working Groups: Northeastern, North Central, Southern, Western, and Federal

• The four regional WGs are composed of:
  - One state-level agency representative selected by the Administrator of each state's CJIS System Agency (CSA)
  - One local-level agency representative selected by the International Association of Chiefs of Police (IACP) or National Sheriffs’ Association (NSA) along with State Chiefs’ or Sheriffs’ Association
  - One representative for the District of Columbia, Guam, RCMP, Puerto Rico, and the U. S. Virgin Islands
  - One Tribal law enforcement representative for each region.

• The Director has the option to designate one additional representative for each 5 WGs.
CJIS ADVISORY PROCESS

FIVE WORKING GROUPS:

- Western Working Group
- Northern Central Working Group
- Northeastern Working Group
- Federal Working Group
- Southern Working Group
CJIS ADVISORY PROCESS

NINE SUBCOMMITTEES:

- Uniform Crime Reporting (UCR)
- APB Executive Committee
- Compliance Evaluation (formerly Sanctions)
- National Crime Information Center (NCIC)
- Identification Services (IS)
- N-DEx (formerly Information Sharing)
- Security and Access
- National Instant Criminal Background Check System (NICS)
- Bylaws
CJIS ADVISORY PROCESS

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL

- Compact Council
  - 2 Committees
    - Two Cycles Annually
      - Spring and Fall
      - Committees, Council
      - Topic Papers
    - Standards & Policy
    - Planning & Outreach
CJIS ADVISORY PROCESS

An idea is born... is sent to the state’s CSO evaluates and forwards to the WG Chairman forwards it to the FBI’s CJIS Div. DFO DFO directs it to proper CJIS unit for research and development Deliberates and makes a recommendation which is forwarded to the Subcommittee Considers and sends recommendation to the Board.

If deemed feasible, CJIS writes staff paper and forwards to the Working Groups for consideration. The APB’s recommendation is forwarded to the FBI Director for approval and implementation by CJIS.
Minimum requirements for the protection of criminal justice information (CJI)

Annual release cycle

July / August Time Frame

Incorporates APB approved changes from previous year (2 cycles: Spring / Fall)

Incorporates administrative changes
CJIS Security Policy
Changes for v5.5
Assigning Tier Numbers to CJIS Security Policy

Requirements

• Connecting systems to existing state network

• Tier 1 – requirements must be met by a system before a CSO can allow connection to the state system.

• Tier 2 – requirements must be met by the date indicated in the plan approved by the CSO.

• Requirements & Tiering Document
NEW CHANGES IN v5.5

Section 5.2
Policy Area 2: Security Awareness Training

“Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB ...”

Four “Levels” of training:

1. Personnel with Unescorted Access to Physically Secure Location
2. Personnel with Unescorted Access to CJI (hard copy)
3. Personnel with Physical and Logical Access
4. Personnel with Technology Roles
Section 5.2.1

Policy Area 2: Security Awareness Training

5.2.1.1 Level 1 Security Awareness Training – Unescorted Access to a Physically Secure Location

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI and/or terminals.
2. Implications of noncompliance.
3. Incident response (identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.
Section 5.2.1

Policy Area 2: Security Awareness Training

5.2.1.2 Level 2 Security Awareness Training – Authorized Access to Criminal Justice Information

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Dissemination and destruction.
NEW CHANGES IN v5.5

Section 5.2.1

Policy Area 2: Security Awareness Training

5.2.1.3 Level 3 Security Awareness Training – Authorized Personnel with Physical and Logical Access
- Name change only
- No change in required topics

5.2.1.4 Level 4 Security Awareness Training – Information Technology Personnel
- Name change only
- No change in required topics

Figure 4 Security Awareness Training Use Cases
- Four (4) new use cases
Section 5.3

Policy Area 3: Incident Response

There has been an increase in the number of The security risk of both accidental or and malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile, remains persistent in both physical and logical environments. To ensure protection of CJI, Agencies shall: (i) establish operational incident handling procedures capability for agency information systems that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of an CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.
Section 5.3
Policy Area 3: Incident Response

5.3.1 Reporting Information Security Events

The agency shall promptly report incident information to appropriate authorities. Information security events, and including any identified weaknesses associated with information systems, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.
Section 5.3
Policy Area 3: Incident Response

5.3.2 Management of Information-Security Incidents

A consistent and effective approach shall be applied to the management of information-security incidents. Responsibilities and procedures shall be in place to handle information-security events and weaknesses effectively once they have been reported.

5.3.4 Incident Monitoring

The agency shall track and document information-system security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.
NEW CHANGES IN v5.5

Section 5.6.2.2

Policy Area 6: Identification and Authentication

Clarification of Out-of-Band Authentication for AA

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, **out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.),** or “Risk-based Authentication” that includes...
NEW CHANGES IN v5.5

Section 5.6.2.2

Policy Area 6: Identification and Authentication

Clarification of Out-of-Band Authentication for AA

Appendix A Terms and Definitions

Out-of-band – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

In-band – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.
Section 5.10.2

Policy Area 10: System and Communications Protection and Information Integrity

5.10.2 Facsimile Transmission of CJI

CJI transmitted via facsimile a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.
NEW CHANGES IN v5.5

PSTN/POTS: Encryption Not Required

Email-like: Encryption Required
Appendix A Terms and Definitions

Facsimile (Fax) – Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, or service which implements email-like technology and transfers documents over a network.
NEW CHANGES IN v5.5

Section 5.11.2

Policy Area 11: Formal Audits

5.11.2 Audits by the CSA
Each CSA shall:

1. At a minimum, triennially audit …
2. …
3. …
4. Have the authority; on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility; the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.
NEW CHANGES IN v5.5

Section 5.11.2

Policy Area 11: Formal Audits

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channelers and Channelers related to outsourcing noncriminal justice administrative functions.
Section 5.12.1.1

Policy Area 12: Personnel Security

5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:

7. If the person already has access to CJIS and is subsequently arrested and/or convicted, continued access to CJI shall be determined by the CSO. *For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.* This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI.
NEW CHANGES IN v5.5

Section 5.13
Policy Area 13: Mobile Devices

• Mobile appendix added in v5.2
• Section 5.13 added in v5.3
• Mobile Security Task Force
  o Chaired by SA Subcommittee members with local technical SMEs
  o Reviewed Section 5.13 and made several recommended changes
  o On-going process to review all things mobile with regards to the CJIS Security Policy
  o Periodic meetings to discuss technology and potential Policy changes
NEW CHANGES IN v5.5

Section 5.13
Policy Area 13: Mobile Devices

5.13.1 Wireless Communications Technology
Examples of wireless communication technologies include, but are not limited to: 802.11x

5.13.1.1 All 802.11 Wireless Protocols
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 shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency’s network that processes unencrypted CJI.
Section 5.13

Policy Area 13: Mobile Devices

5.13.1.1 All 802.11 Wireless Protocols (continued)

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. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.

5.13.1.2 Cellular Devices
NEW CHANGES IN v5.5

Section 5.13

Policy Area 13: Mobile Devices

5.13.1.2.1 Cellular Service Abroad

When devices are authorized for use to access CJi outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency’s policies prior to and after deployment outside of the U.S.
Section 5.13
Policy Area 13: Mobile Devices

5.13.1.4 Wireless Hotspot Capability—Mobile Hotspots

Many mobile devices include the capability to function as a wireless access point or WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a wireless access point—WiFi hotspot connecting to the Internet, they shall be configured:

1. In accordance with the requirements in Section 5.13.1.1 802.11 Wireless Protocols—Enable encryption on the hotspot
2. To only allow connections from agency authorized devices—Change the hotspot’s default SSID a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot’s port filtering / blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 Encryption for item #1. Refer to the requirements in Section 5.6.2.1.1 Password for item #3. Only password attributes #1, #2, and #3 are required.

Or

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.
5.13.2 Mobile Device Management (MDM)

2. MDM with centralized administration configured and implemented to perform at least the:

vii. Detection of unauthorized configurations or software/applications
viii. Detection of unauthorized software or applications
ix. Ability to determine the location of agency controlled devices
x. Prevention of unpatched devices from accessing CJI or CJI systems
xi. Automatic device wiping after a specified number of failed attempts
Section 5.13

Policy Area 13: Mobile Devices

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that cellular wireless devices:

3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.

7. Employ antivirus software malicious code protection or run a MDM system that facilitates the ability to provide antivirus anti-malware services from the agency level.
NEW CHANGES IN v5.5

Section 5.13

Policy Area 13: Mobile Devices

Remove the current 5.13.4.3 Physical Protection
- Incorporate into MDM

Remove the current 5.13.6 Auditing and Accountability
- Adequately covered in Section 5.4 and by MDM requirements

Section 5.13.6 Access Control
- CJI application must provide access control (Section 5.5 Access Control)
Section 5.13

Policy Area 13: Mobile Devices

Relocate Compensating Controls from Section 5.6.2.2.1 to (new) Section 5.13.7.2.1 Compensating Controls
- CSO considers approval however MDM shall be implemented

New mobile-centric definitions
- Full-feature Operating System
- Limited-feature Operating System
- Mobile (WiFi) Hotspot
- Wireless Access Point
- Wireless (WiFi) Hotspot
NEW CHANGES IN v5.5

Appendix K Criminal Justice Agency Supplemental Guidance

- Updated
- From 2 pages to 8
- Expanded explanation of Policy sections
- Use Cases

“This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as “terminal agencies.”
Appendix G.5 Least Privilege

New Best Practice

Assigning access to system resources based on individual user requirements

• Most accounts are created with admin privileges by default
• Most users do not need admin privileges for their duties

Reduces risk by limiting access if account is compromised

Separation of duties is related

• System administrator not the same person as security administrator
• Protection of logs, audit trails
2013 Microsoft Vulnerabilities Study: Mitigating Risk by Removing User Privileges

Analysis of Microsoft Security Bulletins from 2013 highlights that 92% of Critical vulnerabilities would be mitigated by removing admin rights across an enterprise.
Total Microsoft Vulnerabilities Mitigated by Removal of Admin Rights

40%  60%

Note: Based on ALL vulnerabilities published by MS.
Critical Microsoft Vulnerabilities Mitigated by Removal of Admin Rights

- 8%
- 92%

Note: Based on the 147 critical vulnerabilities published by MS.
The report highlights the following key findings:

- Of the 147 vulnerabilities published by Microsoft in 2013 with a Critical rating, 92% were concluded to be mitigated by removing administrator rights.
- 96% of Critical vulnerabilities affecting Windows operating systems could be mitigated by removing admin rights.
- 100% of all vulnerabilities affecting Internet Explorer could be mitigated by removing admin rights.
- 91% of vulnerabilities affecting Microsoft Office could be mitigated by removing admin rights.
- 100% of Critical Remote Code Execution vulnerabilities and 80% of Critical Information Disclosure vulnerabilities could be mitigated by removing admin rights.
- 60% of all Microsoft vulnerabilities published in 2013 could be mitigated by removing admin rights.
FBI CJIS ISO Resources
ISO RESOURCES

CJIS ISO Program

- Steward the CJIS Security Policy for the Advisory Policy Board
  - Draft and present topic papers at the APB meetings
- Provide Policy support to state ISOs and CSOs
  - Policy Clarification
  - Solution technical analysis for compliance with the Policy
  - Operate a public facing web site on FBI.gov: CJIS Security Policy Resource Center
- Provide training support to ISOs
- Provide policy clarification to vendors in coordination with ISOs

iso@ic.fbi.gov
ISO RESOURCES

CJIS Security Policy Requirements and Tiering Document

- Companion document to the CJIS Security Policy
- Lists every requirement, “shall” statement, and corresponding location and effective date
- Lists the priority tier for each requirement
  - Tier 1 – requirements must be met by a system before a CSO can allow connection to the state system.
  - Tier 2 – requirements must be met by the date indicated in the plan approved by the CSO.
- Updated annually in conjunction with the CJIS Security Policy

iso@ic.fbi.gov
ISO RESOURCES

CJIS Security Policy Mapping to NIST 800-63 rev 4

- Companion document to the CJIS Security Policy
- Maps Policy sections to related NIST SP800-53r4 controls
  - Moderate impact level controls plus some related controls
- Technical assessments for federal systems require the use of NIST controls for compliance evaluation (e.g. FISMA, FedRAMP)
- Not all Policy requirements map to NIST controls
  - Policy requirements originate from 28 CFR
  - Policy requirements unique to CJI

iso@ic.fbi.gov
ISO RESOURCES

CJIS Security Policy Resource Center

- Publically Available:
  

- Features:
  
  - Search and download the CJIS Security Policy
  - Download the CJIS Security Policy Requirements and Tiering Document
  - Use Cases (Advanced Authentication and others to follow)
  - Cloud Computing Report & Cloud Report Control Catalog
  - Mobile Appendix
  - Submit a Question (question forwarded to CJIS ISO Program)
  - Links of importance

iso@ic.fbi.gov
ISO RESOURCES

CJIS Security Policy Resource Center


Step #1
Select “Services”
Step #2 Select “CJIS”
CJIS Security Policy Resource Center

Criminal Justice Information Services (CJIS)

Overview

Mission
To equip our law enforcement, national security, and intelligence community partners with the criminal justice information they need to protect the United States while preserving civil liberties.

History
Step #4
Select “CSPRC”
Criminal Justice Information Services (CJIS) Security Policy

Version 5.5
06/01/2016

CIJSI-ITS-DOC-08140-5.5

Prepared by:
CJIS Information Security Officer
CJIS Security Policy Frequently Asked Questions Submission

This page is intended for use by members of law enforcement and non-criminal justice agencies of the CJIS community as well as vendors who provide support to law enforcement and non-criminal justice agencies. All submitted questions should specifically pertain to the CJIS Security Policy and its application—not to any other business processes performed by the CJIS Division or the FBI in general. Submissions received that are unrelated to the CJIS Security Policy will neither be answered nor retained.

Please fill out the form below. The red square indicates a required field.

First Name

Last Name

Your E-Mail Address

Your State

Subject

Comments

3000 characters remaining

ReCaptcha
CJIS ISO CONTACT INFORMATION

iso@ic.fbi.gov