

CJIS Information Technology

Security Audit

Pre-Audit Questionnaire



**Information Technology Security Audit**

**Pre-Audit Questionnaire**

**Why is my agency receiving an audit?**

OSP is required to conduct security audits of each Criminal Justice Agency (CJA), once every three (3) years at a minimum, to assess agency compliance with the *CJIS Security Policy*. Your agency has been selected to participate because the agency accepts access to criminal justice information (CJI) through your state CJIS Systems Agency (CSA), the Oregon State Police.

The essential premise of the *CJIS Security Policy* is to provide appropriate controls to protect the full lifecycle of criminal justice information (CJI), whether at rest or in transit. The policies and procedures governing the security of CJI are examined during the audit to ensure the security and integrity of FBI CJIS systems information.

**What should I expect from the audit process?**

This pre-audit questionnaire is the first step in completing your audit. The pre-audit questionnaire should be completed prior to your selected audit date. The pre-audit questionnaire does several things to help the audit process. First, it provides your agency with a description of what to expect during your onsite audit including a general idea of the topic areas that will be discussed. Second, it provides a list of the documentation your agency is required to provide to the OSP CJIS ISO. Finally, the pre-audit questionnaire provides the OSP CJIS ISO with fundamental insight into your agency’s IT Security policies and procedures during the audit. The completed questionnaire assists the OSP CJIS ISO in narrowing the scope of the audit so they can ask only those questions related to your agency during the onsite audit. Documentation requested that the agency deems sensitive or unable to be released from the agency, should be retained onsite and available at the time of the audit. Please note: onsite review of documentation could extend the length of your audit.

On the date of the onsite audit, an administrative interview is conducted with appropriate agency personnel. Following the interview, the OSP CJIS ISO will perform a physical security inspection, which involves a tour of the facility, including anywhere the agency is processing, storing, or accessing CJI. Typically, this will be your agency’s terminal areas, which could include the communications center, records area, or the agency’s dispatch, as well as the agency’s data center, the location where the networking equipment is housed.

At the conclusion of your agency’s audit, the agency will receive an audit findings report. The report summarizes those policy requirements assessed during the audit and provides the agency’s compliance status. Any concerns or compliance issues found will be discussed with appropriate agency personnel at the time of the audit.

**When and where is my agency’s audit?**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Agency Name:** |  | | | | | | |
|  |  | | | | | | |
| **Date:** |  | | | | | | |
|  | | | | | | | |
| **Time:** |  | | | | | | |
|  | | | | | | | |
| **Audit Location:** | Street Address: | |  | | | | |
|  | City: |  | | State: |  | Zip: |  |

**Who needs to be present during the audit?**

The administrative interview conducted during the onsite audit covers a variety of topics. The opening section deals with administrative topics such as, noncriminal justice agency support (county IT/city IT if they are providing services), private contractors/vendors, personnel sanctions (misuse policy), personnel security (fingerprint background checks), security awareness training, physical security policies, as well as physical and electronic media security (storage, transport, and disposal). The remaining section involves the agency’s network infrastructure and covers topics including, but not limited to: the network diagram, personally owned information systems, creation/validation of userID, authentication of users/IT personnel (passwords), advanced authentication, encryption, dial-up access restrictions, wireless access restrictions (cellular, Bluetooth, 802.11x, etc.), boundary protection (firewalls), malicious code (virus) protection, spam and spyware, patch management, and incident response. Please make sure that agency personnel responsible for all of the topics discussed above are present during the audit. This could include: the agency TAC, LASO, Network Administrator, City IT/County IT, Private Contractors/Vendors in charge of IT systems.

**What documentation do I need to provide to the OSP CJIS ISO for the audit?**

The following documentation should be returned with your completed pre-audit questionnaire. ***(For documentation deemed sensitive or unable to be released from the agency, please retain onsite and have available at the time of the audit. Please note: onsite review could extend the length of your audit.)***

|  |  |
| --- | --- |
|  | **Interagency/Management Control** **Agreements** (if applicable) between the agency and NCJAs |
|  | (NCJA = city IT, county IT, etc.)(Sample agreement is provided in Appendix D, page D-9) |
|  |  |
|  | **Security Addendums** (if applicable) between the agency and private contractor personnel (Security |
|  | Addendum is provided in Appendix H, page H-7) |
|  |  |
|  | **List of all Private Contractor Personnel with Access to CJI** |
|  |  |
|  | **Security Awareness Training List and Materials** |
|  | *(Due to the possible size of this list and/or materials, you can either send a digital copy of this information,* |
|  | *or be able to show it during the on-site inspection.)* |
|  |  |
|  | **Procedures for Security Incident Reporting/Handling** |
|  |  |
|  | **Procedures/Forms for requesting and/or removing access to Information Systems** – include |
|  | account management policies and procedures (how does a user get an account, what happens when a user is |
|  | transferred or terminated, etc.) |
|  |  |
|  | **Network Diagram** – High-level diagram that shows all forms of FBI CJIS data systems access [including |
|  | wireless, dial-up, etc.] by system users and/or IT personnel. *(do* ***NOT*** *include specific IP addresses)* |
|  |  |
|  | **Physical and Electronic Media Protection Policies and Procedures** – to include handling, |
|  | storage, transport, sanitization, and disposal/destruction *(Where is media stored? How is it moved from one* |
|  | *secure location to another? How is it destroyed? Who destroys?)* |
|  |  |
|  | **Encryption Certificates** – see the NIST or CSE certificates section on page 8 regarding how to obtain |
|  | these certificates |

**Agency Contact Information**

**Please complete the following, where applicable only:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Terminal Agency Coordinator (TAC):** | | | | | | | | | | | | |
| Name: | |  | | | | | | | Title: |  | | |
| Street Address: | | |  | | | City: |  | | State: |  | Zip: |  |
| Phone: |  | | | Alt. Phone: |  | | Email: |  | | | | |
|  | | | | | | | | | | | | |
| **Local Agency Security Officer (LASO):** | | | | | | | | | | | | |
| Name: | |  | | | | | | | Title: |  | | |
| Street Address: | | |  | | | City: |  | | State: |  | Zip: |  |
| Phone: |  | | | Alt. Phone: |  | | Email: |  | | | | |
|  | | | | | | | | | | | | |
| **Agency Coordinator (AC) (if required by utilizing contractor services):** | | | | | | | | | | | | |
| Name: | |  | | | | | | | Title: |  | | |
| Street Address: | | |  | | | City: |  | | State: |  | Zip: |  |
| Phone: |  | | | Alt. Phone: |  | | Email: |  | | | | |
|  | | | | | | | | | | | | |
| **Physical Address (main address where CJI is accessed):** | | | | | | | | | | | | |
| Contact Name: | | |  | | | | | | Title: |  | | |
| Street Address: | | |  | | | City: |  | | State: |  | Zip: |  |
| Phone: |  | | | Alt. Phone: |  | | Email: |  | | | | |
|  | | | | | | | | | | | | |
| **Data Center (if different from physical address):** | | | | | | | | | | | | |
| Contact Name: | | |  | | | | | | Title: |  | | |
| Street Address: | | |  | | | City: |  | | State: |  | Zip: |  |
| Phone: |  | | | Alt. Phone: |  | | Email: |  | | | | |
|  | | | | | | | | | | | | |
| **Offsite Media Storage (where media containing CJI is stored outside of the agency):** | | | | | | | | | | | | |
| Contact Name: | | |  | | | | | | Title: |  | | |
| Street Address: | | |  | | | City: |  | | State: |  | Zip: |  |
| Phone: |  | | | Alt. Phone: |  | | Email: |  | | | | |
|  | | | | | | | | | | | | |
| **Back-up Recovery Site (disaster recovery site/where system back-ups are stored):** | | | | | | | | | | | | |
| Contact Name: | | |  | | | | | | Title: |  | | |
| Street Address: | | |  | | | City: |  | | State: |  | Zip: |  |
| Phone: |  | | | Alt. Phone: |  | | Email: |  | | | | |
|  | | | | | | | | | | | | |

**ADMINISTRATION OF CRIMINAL JUSTICE FUNCTIONS**

1. Does the agency have any noncriminal justice agency (NCJA) personnel providing criminal justice services on behalf of the agency? (City IT/County IT with access to CJI)

|  |  |
| --- | --- |
|  | Yes |
|  |  |
|  | No |

1. Is your network, which provides access to FBI CJIS systems and/or data, shared with **noncriminal** justice agencies? *(For example, an agency’s criminal justice network infrastructure is on the same network as the county governments [Noncriminal Justice Agency] network infrastructure)*

|  |  |  |  |
| --- | --- | --- | --- |
|  | Yes | Please list agencies: |  |
|  |  |
|  | No |

1. Does the agency have private contractor(s) personnel that perform criminal justice functions on the behalf of the agency? *(any private contractor personnel with physical or logical unescorted access to CJI)*

|  |  |  |
| --- | --- | --- |
|  | Yes | (**Reminder:** please provide copies of all contracts and/or agreements, if applicable) |
|  |  |
|  | No |

**Example 1:** TheXYZ Shredding Company provides FBI CJIS document shredding. XYZ Personnel comes to the local agency to pick up the documents. They are unescorted, on-site, and take the documents off-site to shred. An Agreement with the FBI CJIS security addendum is required.

**Example 2:** Mobile Computing Company ABC provides FBI CJIS systems network support for the mobile computing software/hardware.

**NETWORK INFRASTRUCTURE**

1. What software application(s) is used to access FBI CJIS systems and/or data? *(Examples include Datamaxx, OpenFox, Voyager, WebLEDS, ForseCom, etc.)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| STATE PROVIDED: | | | |  | |
| DESKTOPS: | | |  | | |
| MOBILES: | |  | | | |
| LAPTOPS: | |  | | | |
| RMS/CAD (if applicable): | | | | |  |
| OTHER: |  | | | | |
|  |  | | | | |

1. Does the agency store FBI CJI *(criminal justice information obtained solely from NCIC or III)* in a RMS or CAD system? *(i.e., FBI #’s, Names or DOB obtained from NCIC/III, etc.)*

|  |  |  |  |
| --- | --- | --- | --- |
|  | Yes | Please list RMS/CAD application: |  |
|  |  |
|  | No |

1. Which agency is responsible for the creation and deletion of system user accounts to gain access to FBI CJIS data? *(Application Level)*

|  |  |
| --- | --- |
|  | CSA |
|  |  |
|  | Local Agency |
|  |  |
|  | Hosting Agency |
|  |  |
|  | Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

1. Does the agency validate user accounts for accuracy?

|  |  |  |  |
| --- | --- | --- | --- |
|  | Yes | If yes, how often? |  |
|  |  |
|  | No |

1. Which agency is responsible for authenticating users to gain access to FBI CJIS data?

|  |  |
| --- | --- |
|  | CSA |
|  |  |
|  | Local Agency |
|  |  |
|  | Hosting Agency |
|  |  |
|  | Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

1. List the method used to authenticate users that have access to FBI CJIS systems and/or data.

|  |
| --- |
|  |

1. Please provide agency’s password construction requirements?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| How many characters? | | |  | |
| Attributes/special characters? | | | |  |
| Expiration? | |  | | |
| History? |  | | | |
| Other: |  | | | |

1. If advance authentication, please provide method the agency is using? *(Examples include Tokens, Biometrics, PKI, Smart Cards, etc.)*

|  |
| --- |
|  |

1. Please identify all networks used to access, transmit, and/or store CJI:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Public Networks | | | *(defined by the* ***CJIS Security Policy*** *as telecommunications infrastructure* |
|  | *consisting of network components that are not owned, operated, and managed solely by a criminal justice agency. Public network connections could include any remote locations such as precincts and/or substations, special operations centers, or other law enforcements entities.)* | | | |
|  |  | | | |
|  | Wireless | | |  |
|  |  | | | |
|  |  | Cellular (smartphones (Blackberry, iPhones, etc.), personal digital assistants (PDA), “aircards”, etc) | | |
|  |  | | | |
|  |  | Bluetooth | | |
|  |  | | | |
|  |  | Wireless (802.11) | | |
|  |  | | | |
|  |  | Other: |  | |
|  |  | | | |
|  | Internet | | |  |
|  |  | | | |
|  |  | Transmit | | |
|  |  | | | |
|  |  | Remote Access (Administrator) | | |
|  |  | | | |
|  | Dial-up | | |  |
|  |  | | | |
|  |  | Transmit | | |
|  |  | | | |
|  |  | Remote Maintenance (Administrator) | | |
|  |  | | | |

1. Please identify the following hardware devices and software applications used to access and/or transport CJI:
2. Boundary Protection (firewalls, routers, encrypted tunnels, proxies, gateways, and guards)

|  |  |  |
| --- | --- | --- |
| Network |  | |
|  |  | |
|  |  | |
| Personal Firewall | |  |
|  | |  |
|  | | *(Examples include laptops, PDAs, Blackberry devices, etc.)* |

1. Malicious Code (Virus) Protection Software

|  |
| --- |
|  |
|  |

1. Spam and Spyware Protection Software

|  |
| --- |
|  |
|  |

1. Encryption Method(s) *(Hardware/Software)*

|  |
| --- |
|  |
|  |

1. Does the agency host CJI related systems or applications in a virtualized environment?

|  |  |
| --- | --- |
|  | Yes |
|  |  |
|  | No |

**NIST or CSE ENCRYPTION CERTIFICATES**

The *CJIS Security Policy* requires that all CJIS data transmitted through any public network segment or over dial-up or Internet connections shall be immediately protected with a minimum 128-bit encryption. Systems that transmit data over radio frequencies to a network with access to CJIS data are also subject to this requirement. This 128-bit encryption must be certified by the National Institute of Standards and Technology (NIST) or Canada’s Communications Security Establishment (CSE) to ensure that the cryptographic modules meet Federal Information Processing Standard (FIPS) 140-2 certification requirements. **Please submit a copy of any applicable encryption certificates with your completed pre-audit questionnaire or have them available at the time of the audit.**

To retrieve the certificate for the FIPS 140-2 validated cryptographic module, complete the following steps:

1. Visit <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>
2. Locate your particular cryptographic module vendor and product.
3. Click on “Certificate” and print.

**Where do I return the pre-audit questionnaire with all the above documentation?**

**Please complete the information and email to** [**nharris@osp.state.or.us**](mailto:nharris@osp.state.or.us)

**Returning the audit questionnaire is not a requirement, however, it WILL decrease the amount of time required to complete the audit on-site.**

**TERMS AND DEFINITIONS**

**Access to Criminal Justice Information** — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

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

**Agency 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.

**CJIS Systems Agency (CSA)** — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

**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.

**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.

**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.

**Information Exchange Agreement** — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party’s information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

**Information System** — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

**Interstate Identification Index (III)** — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

**Local Agency Security Officer (LASO)** — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

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

**National Crime Information Center (NCIC)** — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

**National 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.

**NCJA (Government)** — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

**Physical Access –** The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

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

**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.

**Terminal Agency Coordinator (TAC)** — serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency’s compliance with CJIS systems policies.

**Virtualization** — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.