Information Technology

Security Audit

**Criminal Justice Agency**

Pre-Audit Questionnaire

****

**Criminal Justice Information Technology Security Audit**

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

The FBI CJIS Division is required to conduct security audits of each state, once every three (3) years at a minimum, to assess agency compliance with the *CJIS Security Policy*.  The essential premise of the *CJIS Security Policy* is to provide appropriate controls to protect the full lifecycle of criminal justice information (CJI) and its subset criminal history record information (CHRI), whether at rest or in transit.  Your agency has been selected to participate because the agency accepts access to national CHRI through your state’s CJIS Systems Agency (CSA).  The policies and procedures governing the technical security of CJI and/or CHRI are examined during the FBI’s Noncriminal Justice Information Technology (NCJITS) Audit to ensure the security and integrity of criminal justice information.  **Please note, CHRI is a subset of CJI and are interchangeable for the purposes of this document.**

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

To begin the audit process, your agency should have received an initial call from the FBI ITS auditor that will conduct your onsite audit.  This pre-audit questionnaire is the second step in completing your audit. The pre-audit questionnaire should be completed and returned to the auditor no later than the date noted. 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 auditor. Finally, once returned completed, the pre-audit questionnaire provides the auditor with fundamental insight into your agency’s IT Security policies and procedures.  The completed questionnaire assists the auditor 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 auditor will perform a physical security inspection, which involves a tour of the facility, including anywhere the agency is processing, storing, or accessing CHRI.

At the conclusion of your agency’s audit, the agency will receive a policy assessment packet.  The packet summarizes those policy requirements assessed during the audit, but the packet also 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.

**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, processing CHRI requests, dissemination of CHRI, governmental support (county/city IT departments), private contractors/vendors, personnel sanctions (misuse policy), personnel security (fingerprint 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, 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 SIB Chief, Network Administrator, State IT personnel, Private Contractors/Vendors in charge of IT systems, etc.

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

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

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

|  |  |
| --- | --- |
| **Attention:** |  |
| **Office:** |  | **Cell:** |  |
| **Email:** |  |
| **Mailing Address:** | Street: |  |
|  | City: |  | State: |  | Zip: |  |

**Agency Contact Information**

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

|  |
| --- |
| **Terminal Agency Coordinator (TAC) (primary point of contact):**  |
| Name: |  | Title: |  |
| Street Address: |  | City: |  | State: |  | Zip: |  |
| Phone: |  | Alt. Phone: |  | Email: |  |
|  |
| **Local Agency Security Officer (LASO) (technical POC, if applicable):** |
| Name: |  | Title: |  |
| Street Address: |  | City: |  | State: |  | Zip: |  |
| Phone: |  | Alt. Phone: |  | Email: |  |
|  |
| **Physical Address (main address where CHRI/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: |  |

**Supporting Documentation to be included as part of the audit…**

The following documentation should be returned with your completed questionnaire. ***(For documentation deemed sensitive or unable to be released from the agency, please contact your audit manager [contact information is included at the end of this questionnaire] for a secure delivery method.)***

|  |  |
| --- | --- |
|  | **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) |
|  |  |
|  | **Personnel Sanctions Policy** - rules of acceptable use of CJI and/or disciplinary actions for misuse |
|  |  |
|  | **Security Awareness Training List** -(include: first and last name, date of hire, date of |
|  | last security awareness training, access level [administrator, query-only, etc.], agency, and department).  |
|  | *(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.)* |
|  |  |
|  | **Security Awareness Training Materials** -(if applicable) provide only if the CSA does NOT create or  |
|  | maintain curriculum *(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.)* |
|  |  |
|  |  **Physical Protection Policies and Procedures** - a written policy that describes the agency’s physical |
|  |  protections for CJI (i.e. visitors are escorted, no unauthorized access in secure areas, etc.) |
|  |  **Physical and Digital Media Destruction 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?*  |
|  |  |
|  | **Network Diagram** - high-level diagram that shows all forms of FBI CJIS systems access [including |
|  | wireless, etc.] by system users and/or IT personnel. *(do not include specific IP addresses)* |
|  |  |
|  | **Event Logs** - (if applicable) screen shot or word document containing a sample of the event logs for each  |
|  | information system accessing CJI (successful and unsuccessful log on attempts, password changes,  |
|  | transactions, etc.) *(Please note, the CSA will be asked to provide this information for applications the CSA* |
|  | *manages so you do not need to include CSA managed information systems/applications)* |
|  |  |
|  | **Encryption Certificates** - see the NIST or CSE certificates section on page 8 regarding how to obtain |
|  | these certificates |
|  |  |
|  | **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, account validation procedures, how a user is approved for remote access with  |
|  | privileged functions, etc.) |
|  |  |
|  | **Procedures for Security Incident Reporting/Handling** -written procedures for reporting a breach of  |
|  | CJI; also include any documentation for security incidents reported within the last three years. |

**ADMINISTRATION OF CRIMINAL JUSTICE FUNCTIONS**

**\*\*\*Please note: 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. 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. (i.e. CJI is any information obtained from the FBI information systems) The *CJIS Security Policy* applies only to information systems accessing, storing, or transmitting CJI. When completing the remainder of this questionnaire please remember that the questions only apply to those information systems with access to CJI. \*\*\***

1. How is the agency accessing/transmitting criminal justice information (CJI)? [i.e. what software application(s) is/are used to access FBI CJIS systems and/or data? *(Examples include Datamaxx, OpenFox, Voyager, LInX, RISSNET, etc.)]*

|  |  |
| --- | --- |
| CSA PROVIDED: |  |
| DESKTOPS: |  |
| MOBILES: |  |
| LAPTOPS: |  |
| RMS/CAD: |  |
| N-DEx: |  |
| LIVESCAN: |  |
| 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 [ ]  NO
	1. If **YES**, please list application and details?

|  |
| --- |
|   |
|  |
|  |
|  |

NONCRIMINAL JUSTICE [GOVERNMENTAL] SERVICES

1. Does the agency have any noncriminal justice agency personnel providing criminal justice services on behalf of the agency? (City IT/County IT with unescorted access to CJI) [ ]  YES [ ]  NO
2. If **YES**, what criminal justice administrative functions are being performed?

|  |  |
| --- | --- |
|  | IT services (network/system administrations, desktop support, etc.) |
|  | Data destruction (paper shredding, hard drives, etc.) |  |
|  | Off-site media storage (data centers, backup, paper storage archives, etc.) |  |
|  | other: |  |

1. Please list governmental agencies performing criminal justice functions that allows unescorted access to CJI on behalf of the agency.

|  |
| --- |
|   |
|  |
|  |
|  |

1. Has the agency implemented a management control agreement signed by the criminal justice agency head (e.g., Chief of Police, Sheriff, etc.) and the noncriminal justice agency head (e.g., IT Director, etc.)? [ ]  YES [ ]  NO [ ]  N/A

***\*Please provide a copy of the signed management control agreement with the completed audit questionnairr.***

PRIVATE CONTRACTORS

1. Does the agency outsource (use private contractor personnel/vendors) any criminal justice function that provides private contractor personnel with unescorted access to CJI? *(unescorted access could be logical access for remote maintenance aka VPN access or could be physical access to datacenter/terminals, etc.)* [ ]  YES [ ]  NO
2. If **YES**, what criminal justice functions are private contractors performing?

|  |  |
| --- | --- |
|  | Data destruction (paper shredding, hard drives, etc.) |
|  | IT services (network/system administrations, desktop support, etc.) |  |
|  | Off-site media storage (data centers, backup, paper storage archives, etc.) |  |
|  | other: |  |

1. Please list all private contractors/vendors performing criminal justice functions that allows unescorted access to CJI on behalf of the agency. *(e.g. New World, Iron Mountain, CPI, etc.)*

|  |
| --- |
|   |
|  |
|  |
|  |

1. Has each unescorted private contractor/vendor personnel signed the CJIS Security Addendum?

 [ ]  YES [ ]  NO [ ]  N/A

***\*Please provide a copy of the signed security addendums and signed contracts with the completed audit questionnaire.***

**INFORMATION PROTECTION**

PERSONNEL SECURITY

1. Are state and national fingerprint-based record checks conducted prior to initial employment or assignment for all personnel who have authorized unescorted access to FBI CJIS systems and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS Systems? *(e.g., record clerks, terminal operators, IT personnel, servicing NCJA (government) personnel, servicing PC personnel, custodial personnel, vending machine providers, maintenance personnel, building land lords, etc. – anyone with unescorted access to physically secure locations. CJI must be stored in physically secure location – so any unescorted access is covered)*

 [ ]  YES [ ]  NO

* 1. Has the above mentioned fingerprint based check been completed by all agency employed personnel with physical or logical access? [ ]  YES [ ]  NO
	2. Has the above mentioned fingerprint based check been completed by all unescorted noncriminal justice [governmental] personnel? [ ]  YES [ ]  NO [ ]  N/A
	3. Has the above mentioned fingerprint based check been completed by all private contractor/vendor personnel? [ ]  YES [ ]  NO [ ]  N/A
	4. Has the above mentioned fingerprint based check been completed for all unescorted personnel with only physical access *(custodial, maintenance, etc.)*? [ ]  YES [ ]  NO [ ]  N/A
1. If the agency has discovered a felony conviction(s) during the applicant fingerprint based record check *(i.e. an applicant has a criminal history with a felony conviction)* has the agency requested a waiver for access from the CSO prior to allowing access to CJI? [ ]  YES [ ]  NO [ ]  N/A
2. For individuals who already have unescorted access to CJI *(current personnel with unescorted access)* and have subsequently been arrested or convicted *(e.g., an employee is arrested for a DUI)*, has the agency notified and requested a waiver for access from the CSO prior to allowing the individual to regain unescorted access to CJI? [ ]  YES [ ]  NO [ ]  N/A
3. Does the agency have a written policy for the discipline of personnel failing to comply with established information security policies and procedures *(i.e. misuse of the system)*?

 [ ]  YES [ ]  NO

***\*Please provide a copy of the agency’s discipline/misuse policy.***

SECURITY AWARENESS TRAINING

1. Does the agency ensure all personnel with unescorted access to CHRI/CJI have completed security awareness training within six months of assignments and at least every two years after? *(should include agency personnel, IT staff, private contractors, cleaning/maintenance personnel with physical access to information)* [ ]  YES [ ]  NO
2. If **YES**, is documentation of individual security awareness training maintained in a current status, to include private contractors if applicable? [ ]  YES [ ]  NO

***\*Please provide a copy of the training documentation.***

1. Is the agency using the CSA provided training curriculum? (If **NO**, please provide training materials for review) [ ]  YES [ ]  NO

SECURITY INCIDENTS AND VIOLATIONS

1. Does the agency provide and enforce the *CJIS Security Policy* to all authorized users, to include private contractor personnel? [ ]  YES [ ]  NO
2. What are the procedures when a security violation or incident is detected?

|  |
| --- |
|  |
|  |
|  |

1. Does the agency report the security violation or incident to anyone? Who? [ ]  YES [ ]  NO

|  |
| --- |
|  |
|  |
|  |

1. Are all employees and/or private contractors made aware of the reporting procedures?

 [ ]  YES [ ]  NO

1. Are the procedures described above written in agency policy? [ ]  YES [ ]  NO

***\*Please provide a copy of the agency’s security incident response policy.***

1. Has the agency reported/had any security violations or incidents in the last 3 years? *(incidents in which security of CHRI/CJI was compromised or put at risk)*  [ ]  YES [ ]  NO

|  |
| --- |
|  |
|  |
|  |
|  |

MEDIA PROTECTION AND DISPOSAL

1. Describe all locations where and how criminal justice information is retained. (e.g. locked file cabinet, locked office, off-site storage facility, records archive, etc.)

|  |
| --- |
|  |
|  |
|  |
|  |

1. Is the storage location physically secured? (i.e. unauthorized personnel cannot access CHRI/CJI, within a locked file with limited access, in a locked office, in a safe, etc.) [ ]  YES [ ]  NO

* 1. Does the agency house files that contain CJI in an off-site record storage facility?

 [ ]  YES [ ]  NO

* 1. Who owns/manages the facility? (i.e. who controls access)

|  |
| --- |
|  |

* 1. How are records transported to the off-site facility?

|  |
| --- |
|  |

* 1. How are the records stored at the off-site facility?

|  |
| --- |
|  |

1. Does the agency have a written policy that describes physical protections? (i.e. how and where the information must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.)

 [ ]  YES [ ]  NO

***\*Please provide a copy of the agency’s media protection policy.***

1. Are visitors escorted by authorized personnel in physically secure locations at all times (in all access and storage areas to include off-site facilities if designated physically secure)? [ ]  YES [ ]  NO
2. How does the agency dispose of physical (hard copy/paper) media containing CHRI/CJI?

|  |
| --- |
|  |
|  |
|  |
|  |

* 1. Does the agency have written procedures for physical destruction? [ ]  YES [ ]  NO

***\*Please provide a copy of the agency’s media destruction policy.***

* 1. If the agency personnel does not conduct the destruction of the physical media and it is performed by another entity, is the process witnessed by authorized personnel?

 [ ]  YES [ ]  NO [ ]  N/A

1. When electronic media reaches end of life (no longer works) or is to be replaced/upgraded, how does the agency destroy the media (e.g., hard drives, etc.)?

|  |
| --- |
|  |
|  |
|  |
|  |

1. Does the agency have written procedures for the sanitization and/or destruction of digital media (hard drive, thumb drive, CDs, etc.)? [ ]  YES [ ]  NO

***\*Please provide a copy of the agency’s media destruction policy.***

1. If the agency personnel does not conduct the sanitization or destruction of the digital media and it is performed by another entity, is the process witnessed by authorized personnel?

 [ ]  YES [ ]  NO [ ]  N/A

PHYSICAL SECURITY

1. Describe the physical location where the computer(s) with access to CJI is/are housed. (e.g., locked office, reception area, etc.)

|  |
| --- |
|  |
|  |
|  |

* 1. Are the locations physically secured? (i.e. unauthorized personnel cannot access CJI, computer is not left unattended, visitors are escorted while in area, etc.) [ ]  YES [ ]  NO
	2. Is the CJI encrypted at rest *(only required when stored at rest outside a physically secure location)*?

 [ ]  YES [ ]  NO [ ]  N/A

* 1. If encryption is used, please describe methods (bit level, hardware/software, etc.) of encryption. (e.g. Adobe Pro, WinZip, TrueCrypt, etc.)

|  |
| --- |
|  |
|  |
|  |

* 1. Does the agency protect the information using a passphrase (to unlock encryption)? Please describe.

|  |
| --- |
|  |
|  |
|  |

1. Does the agency have a written policy that describes physical protections? (i.e. how and where the information/equipment must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.) [ ]  YES [ ]  NO

***\*Please provide a copy of the agency’s physical security policies.***

1. Is the CHRI/CJI backed up to off-site storage or a disaster recovery location? [ ]  YES [ ]  NO

* 1. Who owns/manages the facility? (i.e. who controls access)

|  |
| --- |
|  |

* 1. How are backup records transported to the secondary facility? (i.e. disc to disc with encryption or physical tapes encrypted or in locked box, etc.)

|  |
| --- |
|  |

* 1. How are the records stored at the off-site facility?

|  |
| --- |
|  |

**NETWORK INFRASTRUCTURE**

NETWORK CONFIGURATION

1. Does the agency maintain and regularly update and protect a network diagram? [ ]  YES [ ]  NO

***\*Please provide a copy of the agency’s network diagram.***

PERSONALLY OWNED INFORMATION SYSTEMS

1. Does the agency allow personally owned devices to access, process, store, or transmit CJI?

 [ ]  YES [ ]  NO

1. If **YES**, does the agency have documented procedures in place outlining the terms and conditions for the use of these devices? [ ]  YES [ ]  NO [ ]  N/A

***\*Please provide a copy of the agency’s personally owned device policy.***

PUBLICALY OWNED INFORMATION SYSTEMS

* + - 1. Does the agency allow publicly owned computers to access, process, store, or transmit CJI? *(Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.)* [ ]  YES [ ]  NO

SYSTEM USE NOTIFICATION

1. Do all information systems accessing CJI display an approved system use notification message that includes the following? [ ]  YES [ ]  NO
* The user is accessing restricted information system
* System usage may be monitored, recorded, and subject to audit
* Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties
* Use of the system indicates consent to monitoring and recording
	1. If **YES**, does the approved system use notification message remain on the screen until the user acknowledges the notification? [ ]  YES [ ]  NO

AUTHENTICATION AND IDENTIFICATION/USER ID

* + - 1. When logging onto the application or network and accessing CJI does the user and/or administrator enter a password that utilizes secure password attributes that includes all of the following characteristics? [ ]  YES [ ]  NO

For network access: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| **YES** |  **NO** |  |
|  |  | Password length at least eight characters |
|  |  | Password cannot be dictionary word or proper name |
|  |  | Password and UserID cannot be the same |
|  |  | Password expiration is maximum of 90 days |
|  |  | Password history is set to a minimum of (10) ten |
|  |  | Password is not displayed when entered |

For records management type systems or applications: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| **YES** |  **NO** |  |
|  |  | Password length at least eight characters |
|  |  | Password cannot be dictionary word or proper name |
|  |  | Password and UserID cannot be the same |
|  |  | Password expiration is maximum of 90 days |
|  |  | Password history is set to a minimum of (10) ten |
|  |  | Password is not displayed when entered |

Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| **YES** |  **NO** |  |
|  |  | Password length at least eight characters |
|  |  | Password cannot be dictionary word or proper name |
|  |  | Password and UserID cannot be the same |
|  |  | Password expiration is maximum of 90 days |
|  |  | Password history is set to a minimum of (10) ten |
|  |  | Password is not displayed when entered |

1. Do users or IT administrators ever share their usernames or passwords or have generic group accounts? [ ]  YES [ ]  NO
2. Has the agency implemented “advanced password standards” in lieu of “basic password standards” for information systems accessing CJI? [ ]  YES [ ]  NO

a. If **YES**, does advanced password standards meet all of the following:

* Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed. *(e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable)*
* Password Verifiers shall not permit the use of a stored “hint” for forgotten passwords and/or prompt subscribers to use specific types of information *(e.g., “What was the name of your first pet?”)*when choosing a password.
* Verifiers shall maintain a list of “banned passwords” that contains values known to be commonly-used, expected, or compromised.
* When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the “banned passwords” list.
* If the chosen password is found to be part of a “banned passwords” list, the Verifier shall: advise the subscriber that they need to select a different password, provide the reason for rejection, and require the subscriber to choose a different password.
* Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.
* Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.
* Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.
* Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.  The salt shall be at least 32 bits in length.  The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.
* For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.

1. Describe the agency’s process for issuing user accounts, deleting/disabling user accounts, and periodic validation of user accounts:

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

* 1. Are these procedures written? [ ]  YES [ ]  NO

***\*Please provide a copy of the agency’s account management policies.***

SESSION LOCK

1. Does the information system or application initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity? [ ]  YES [ ]  NO
	1. If a user leaves the computer, do they log out of the computer or lock the screen?

 [ ]  YES [ ]  NO

UNSUCCESSFUL LOGIN ATTEMPTS

1. Where technically feasible, does the system enforce a limit of no more than five consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI)?

 [ ]  YES [ ]  NO

1. Does the system automatically lock the account/node for a 10 minute time period unless released by an administrator?

 [ ]  YES [ ]  NO

EVENT LOGGING

1. Are the following events logged in all applications accessing CJI *(could be at a network/server level for active directory based authentication)*: [ ]  YES [ ]  NO [ ]  N/A

For network access: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
|  | successful and unsuccessful log on attempts |
|  | successful and unsuccessful password changes |  |
|  | successful and unsuccessful actions by privileged accounts (adding users, deleting users, etc.) |  |
|  | successful and unsuccessful actions related to CHRI (delete records, edits of information, access to the record, etc.) |

For records management type systems or applications: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
|  | successful and unsuccessful log on attempts |
|  | successful and unsuccessful password changes |  |
|  | successful and unsuccessful actions by privileged accounts (adding users, deleting users, etc.) |  |
|  | successful and unsuccessful actions related to CHRI (delete records, edits of information, access to the record, etc.) |

Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
|  | successful and unsuccessful log on attempts |
|  | successful and unsuccessful password changes |  |
|  | successful and unsuccessful actions by privileged accounts (adding users, deleting users, etc.) |  |
|  | successful and unsuccessful actions related to CHRI (delete records, edits of information, access to the record, etc.) |

* 1. Does each logged event include: date, time, component (where it occurred), type of event, user, outcome (success or failure)? [ ]  YES [ ]  NO [ ]  N/A
	2. If a security incident happened in relation to the release or misuse of CJI, could you identify the individual who carried out the action and when? [ ]  YES [ ]  NO [ ]  N/A
	3. Does the agency check logs (who accessed CJI, logged in, etc.) at least weekly?

 [ ]  YES [ ]  NO [ ]  N/A

* 1. How long are logs kept?

|  |
| --- |
|  |

ENCRYPTION

* + - 1. What type of connections does the agency utilize to access/transmit CJI?
	+ Public (*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.)* *(e.g.,‘private’ fiber, T-1s, Verizon/AT&T telecommunications, county/city WAN, etc.)*
	+ Other serviced law enforcement agencies *(shared systems or services connected through larger public (WAN)networks)*
	+ Precincts and/or substations *(alternate agency facilities with access to CJI through public networks/city/county WAN, etc.)*
	+ Disaster recovery or back-up datacenter locations *(disc-to-disc backup transfers to alt locations)*
	+ Livescan *(results are returned to machine; email or transmit results from machine)*
	+ Wireless
		- Mobile Data Terminals
		- Cellular *(smartphones (iPhones, Androids, etc.), tablets (without full operating systems)*
		- WirelessLAN *(Wifi)*
		- Bluetooth
	+ Internet
		- Web-based *(ISP, LEO, Citrix, etc.)*
		- Remote Access *(maintenance/VPN)*
* Land Mobile Radio *(LMR)*
1. How is CJI encrypted when transmitted outside the physically secure location where it is stored? (i.e., how is the data encrypted when a user is accessing from an internet connection, etc.) Include details for each connection type utilized (listed above). (e.g., methods of encryption, bit level, hardware/software/application, FIPS certificate numbers, etc.)

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. Please provide the FIPS 140-2 certification for each method of encryption noted above.

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.

ADVANCED AUTHENTICATION

1. Does the agency utilize advanced authentication (i.e. second factor) for direct access to CJI from outside the physically secure location? *(for remote administration/VPN access by IT administrators, MDTs/MCTs that can run transaction in the field/not mounted in car)* [ ]  YES [ ]  NO
2. If **YES**, please describe methods? *(e.g., tokens, OTP, smart cards, etc.)*

|  |
| --- |
|  |
|  |
|  |
|  |

MOBILE DEVICES

* + - 1. Does the agency use wireless network devices to access CJI?[ ]  YES [ ]  NO

|  |  |
| --- | --- |
|  | MDTs *(large form factor)* |
|  | Laptops *(used for remote access/maintenance)(large form factor)* |
|  | Tablets/iPads *(medium form factor)* |
|  | Smartphones *(small form factor)* |
| Other: |  |

* + - 1. For all large form factor mobile devices *(i.e., devices that have full-feature operating systems)* is a personal firewall enable and virus protection implemented? [ ]  YES [ ]  NO [ ]  N/A
			2. For medium or small form factor mobile devices *(i.e. devices that do NOT have a full-feature operating system)*, does the agency use a mobile device manager (MDM) to control smartphones and tablets accessing CJI capable of the following: [ ]  YES [ ]  NO [ ]  N/A
* Remote locking of device
* Remote wiping of device
* Setting and locking device configuration
* Detection of “rooted” and “jail broken” devices
* Enforce folder or disk level encryption
* Application of mandatory policy settings on the device
* Detection of unauthorized configurations or software/applications
	+ - 1. Does the agency use any wireless devices to process, store, and/or transmit CJI that have been rooted, jail broken, or have had any unauthorized changes made to the device? [ ]  YES [ ]  NO [ ]  N/A
			2. If the agency uses smartphones or tablets to access CJI, is CJI only transferred between authorized applications and storage areas of the device? [ ]  YES [ ]  NO [ ]  N/A
			3. If applicable, does the agency monitor mobile devices not capable of an always –on cellular connection *(WiFi only or with cellular on demand)* to ensure their patch and update state is current?

 [ ]  YES [ ]  NO [ ]  N/A

* + - 1. Does the agency authorize cellular devices for use outside the boundary of the U.S.? [ ]  YES [ ]  NO

If **YES**, does the agency perform an inspection to ensure that all controls are in place and functioning properly to ensure cellular carrier has not modified or compromised certain internal functions of the device during international use? [ ]  YES [ ]  NO [ ]  N/A

BOUNDARY PROTECTION AND INTRUSION DETECTION

1. Describe the boundary protection used to protect the network. (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.)

|  |
| --- |
|  |
|  |
|  |

1. Is CHRI/CJI separated from non-CHRI/CJI related access? (i.e. can unauthorized users access application or locations of CHRI/CJI or is it separated in some way, such as a VLAN?)

Please describe. [ ]  YES [ ]  NO [ ]  N/A

|  |
| --- |
|  |
|  |
|  |

2.Has the agency implemented network-based and/or host based intrusion detections tools?

 [ ]  YES [ ]  NO

* Maintain current signatures
* Monitor inbound and outbound communications for unusual or unauthorized activities
* Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort
* Review intrusion detection or prevention logs weekly or implement automated event notification
* Employ automated tools to support near-real-time analysis of events in support of detecting system level attacks

MALICIOUS CODE PROTECTION

1. Does the agency enable virus protection at start-up and employ automatic scanning and updates on all computers and servers storing or accessing CJI? Please describe. (i.e. type and version)

 [ ]  YES [ ]  NO

|  |
| --- |
|  |
|  |

SECURITY ALERTS AND ADVISORIES

1. Does someone within the agency stay up to date with relevant security alerts and advisories?

 [ ]  YES [ ]  NO

PATCH MANAGEMENT

1. Does the agency apply routine patches and updates to all software and components? (i.e. Windows updates, firewall patches, etc.) [ ]  YES [ ]  NO

VIRTUALIZATION

1. Does the agency host any CJI in a virtualized environment? [ ]  YES [ ]  NO
	1. Please describe how CJI is protected in a virtual environment. (i.e. how is CJI protected from unauthorized access – partitions, separate virtual NICs, different hosts from non-CJI related systems or internet facing applications, etc.)

|  |
| --- |
|  |
|  |
|  |
|  |

CLOUD COMPUTING

1. Does the agency utilize a Cloud Provider to host or store CJI related information systems, applications, or data? [ ]  YES [ ]  NO

If so, what service do they provide?

|  |  |
| --- | --- |
|  | Software as a Service (SaaS) |
|  | Platform as a Service (PaaS) |
|  | Infrastructure as a Service (IaaS) |

1. Please provide details. Please include services provided (in relation to CJI) as well as details of how the agency is protecting CJI within the cloud environment.

|  |
| --- |
|  |
|  |
|  |

**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.

**Dissemination** – The transmission/distribution of CJI to Authorized Recipients with an agency.

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

**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.

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

**Noncriminal justice administrative functions** – means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following: making fitness determinations/recommendations, obtaining dispositions, disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General, and other authorized activates relating to the general handling, use, and storage of CHRI.

**Noncriminal justice purposes** – as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

**Outsourcing** – The process of delegating in-house operations to a third-party.

**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.

**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.

**\*\*\*\*\*\*\*\*\* FOR OFFICIAL USE ONLY\*\*\*\*\*\*\*\*\***

|  |
| --- |
| **Auditor Review** |
| Auditor Name: |  | Date of Review: |  |
| Comments/Documents Provided/Notes: |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Secondary Reviewer: |  | Date of Review: |  |
| Additional Comments: |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |