COMPLETED by:

[AGENCY CONTACT]

[AGENCY name]

[AGENCY address]

Version 2.0

August 1, 2017



CJIS Security Policy Questionnaire

Technical risk assessment

# INFORMATION

The following risk assessment questionnaire is a condensed version of the FBI Criminal Justice Information Services (CJIS) Security Policy. This document was created in order to assist Montana agencies and their vendors/contractors in their compliance with the FBI CJIS Security Policy. The certification page (in Appendix E) is an acknowledgement, by the local law enforcement agency, along with the vendor and its individual employees, that they have read and understand the requirements contained within this document. All references are codified in the FBI CJIS Security Policy itself. Any questions regarding the implementation of the FBI CJIS Security Addendum should be directed to the DOJ Security Team via telephone (406) 444-2412 or email to: DOJSecurity@mt.gov.

**Agencies are urged, prior to the agency’s entire packet submission to DOJ, to perform a review of the vendor/contractor responses to the following Security Addendum requirements, as lack of completeness delays the DOJ Security Team’s review process, which in turn, can ultimately lead to the criminal justice agency’s lack of connectivity to the DOJ network or delays in other criminal justice interfaces and projects.**

The responsibility for contractor compliance with the FBI requirements, and the enforcement thereof, resides with the criminal justice agency.

# CJIS Security Policy Questionnaire

## INTRODUCtion

The CJIS Security Policy outlines a minimum set of required security controls for managing and maintaining Criminal Justice Information (CJI). The CJIS Advisory Policy Board (APB) manages the policy with national oversight from the CJIS division of the FBI with delegated authority being given to each state. In Montana that delegated authority sits with the Montana Department of Justice.

There are 13 Policy Areas covering over 131 security requirements defined in the CJIS Security Policy. Most are technical in nature. The following guide is intended to assist agencies and organizations in understanding and implementing the requirements of the Criminal Justice Information Services (CJIS) Security Policy (CSP). The Montana Department of Justice, as the CJIS Systems Agency (CSA) for the State of Montana, is responsible for establishing, administering, monitoring and auditing information security that pertains to CJI.

**DISCLAIMER:** This questionnaire is intended as a measurement of risk and should not be considered a final judgment as to if an agency would pass an audit conducted by the FBI or the Montana Department of Justice.

Complete and return this risk assessment to the Montana Department of Justice, Information Security Office. Because of the sensitive nature of the information contained in this document, it is suggested that you send this document through the MT File Transfer Service (FTS) (<http://transfer.mt.gov>) or your FBI LEEP account if you have one.

DOJ Information Security Office: [DOJSecurity@mt.gov](mailto:DOJSecurity@mt.gov) 406-444-2412

DOJ Service Desk: [DOJServiceDesk@mt.gov](mailto:DOJServiceDesk@mt.gov) 406-444-3993

DOJ CJIN Services Help Desk: DOJDCICJINServices@mt.gov 406-444-2800

Montana FTS Help Desk: [ServiceDesk@mt.gov](mailto:ServiceDesk@mt.gov) 406-444-2000

DOJ Fax: 406-444-1264

Due to the range of policy areas being reviewed, completion of this questionnaire may require input from both agency operations and IT support personnel or vendor. Please include appropriate personnel for completion of all sections of this document.

## Definitions

You will see the following common terms and abbreviations used throughout this document.

**BYOD – Bring Your Own Device**

Use of personally owned devices for purposes related to criminal justice or noncriminal justice activities where criminal justice information may be obtained, received, stored, and/or shared.

**CAD – Computer-assisted or Computer-aided Dispatch System or Software**

Computer based system or software to assist or aid with dispatch law enforcement and emergency services. Often is integrated with other law enforcement or emergency services systems.

**CJA** – **Criminal Justice Agency**  
This term is used for any state, local, tribal, or territorial government that interfaces through the Montana Department of Justice to CJIN. This includes any court, governmental agency, or subunits of governmental agencies performing the administration of criminal justice.

**CSA** – **CJIS Systems Agency**  
This term is used for the Montana Department of Justice as the agency responsible for establishing and administering an information security program throughout the State of Montana.

**CJI – Criminal Justice Information**Any and all FBI CJIS provided data. This includes biometric, identity history, biographic, property, and case/incident history data.

**CJIS** – **Criminal Justice Information Services**CJIS refers to the FBI’s Criminal Justice Information Services Division

**CSO -** **CJIS Systems Officer**

Person appointed by CSA to be responsible for establishing and administering an information technology security program throughout the CSA’s user community, to include the local levels.

**CSP** – **CJIS Security Policy**  
This is the Policy produced by the FBI CJIS Division outlining the lawful use and appropriate protection of Criminal Justice Information.

**JMS – Jail Management System**

System or software used to manage jail or detention centers. It is often integrated with other law enforcement or emergency services systems.

**Noncriminal Justice Purpose**

The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice. These include employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

**PIN – Personal Identification Number**

A number code known only by you to authenticate into a system.

**RMS – Records Management System or Software**

System or software used by law enforcement agencies to track and manage criminal justice records and cases. These may be interfaced with one or more other criminal justice systems.

## CJA’s vs. NCJA’s

A Criminal Justice Agency(CJA) is defined as an agency which performs the administration of criminal justice pursuant to statute or executive order and which allocates a substantial part of its budget to the administration of criminal justice.

A noncriminal Justice Agency (NCJA) is an entity or sub-unit that provides services primarily for purposes other than the administration of criminal justice.

Is your agency a CJA or a NCJA? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please complete all the following information fields below.

|  |  |
| --- | --- |
| **Agency Name** | **ORI** |
| **Agency Address** | **Phone #** |
| **Agency Alternate Address** | **Phone #** |
| **City / State** | **Zip** |
| **Agency Information Technology Contact** | **Phone #** |
| **Agency Internet Service Provider & Contact** | **Phone #** |

**LASO/Terminal Agency Coordinator**

Every agency having access to CJIS data through their own network must designate someone as the Local Agency Security Officer (LASO). The LASO for this agency has been designated as:

|  |  |
| --- | --- |
| **LASO/TAC First Name** | **Last Name** |
| **Phone #** | **Fax#** |
| **Email Address** | **Other** |

## Systems that will store criminal justice information

Please list all systems (e.g., CAD, RMS, JMS, email, etc.), or networks (SUMMITNET, local network, county network) that will transmit, store or process criminal justice information (CJI) that your agency utilizes.

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

### 1.a. Telecommunications, Radio, Wireless, Private and Public Cloud SeRvice Providers

If your organization **provides** any services for telecommunications, radio, wireless, private or public cloud services, please list what services you provide and customers/organizations that are affiliated with state or federal agencies and law enforcement that you serve.

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

## Information Exchange AGREEMENTS (CSP 5.1)

Information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 2.1 | Does the agency have a CAD, RMS, 911 or other system that contains CJI?  List them here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 2.2 | Does any of the agency systems that contain CJI have interfaces to other systems?  List the other systems here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 2.3 | Does the agency share a network, equipment closet or building with other entities?  List them here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 2.4 | If you answered yes to any of the last 3 questions, your agency is required to have an information exchange agreement(s) in place. Does the agency have signed information exchange agreement(s)? |  |
| 2.5 | Does the agency use contractors (i.e. janitors, HVAC) or vendors (i.e. IT personnel) to help maintain agency buildings, networks and systems that contain CJI? |  |
|  | 1. If yes, has each individual contractor/vendor signed a CJIS Contractor Security Addendum? |  |
| 2.6 | Does the agency use contractors/vendors to provide telecommunications, radio, wireless, public or private cloud services? If so, please list them here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

## Security Awareness Training (CSP 5.2)

Security awareness training shall be required of all unescorted personnel that might come in contact with CJI. Re-training is required on a biennial basis. **NOTE: If your agency uses the SANS training, skip to question 3.9.**

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 3.1 | Does the agency require all unescorted personnel to complete security awareness training within six months of access and biennially thereafter? |  |
| 3.2 | Does the agency accept documentation showing completion of security awareness training from another agency? |  |
| 3.3 | If so, is that training vetted through the DOJ Security Office? |  |
| 3.4 | Does your agency's training program meet the CJIS security requirements? |  |
| 3.5 | **Level One Security Awareness Training -** At a minimum the following topics shall be covered as a training baseline for all personnel who have unescorted access to a **physically secure location**. Are these areas covered?  **EXAMPLES:** Janitors, temporary construction staff   1. Individual responsibilities and expected behavior with regards to being in the vicinity of CJI usage and/or terminals |  |
|  | 1. Implications of non-compliance |  |
|  | 1. Incident response (Identify, tasks, points of contact and individual actions.) |  |
|  | 1. Visitor control and physical access to spaces (Discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity among staff or vendors, etc.) |  |
| 3.6 | **Level Two Security Awareness Training –** In addition to the above requirements, the following topics shall be covered as a minimum training baseline for all **authorized personnel with access to CJI**. Are these areas covered?  **EXAMPLES:** Records clerks, dispatchers, court clerks/staff, city/county attorneys, or people who deal with CJI in paper form only   1. Media Protection. |  |
|  | 1. Protect information subject to confidentiality concerns (Hardcopy through destruction.) |  |
|  | 1. Proper handling and marking of CJI. |  |
|  | 1. Threats, vulnerabilities, and risks associated with handling of CJI. |  |
|  | 1. Social engineering. |  |
|  | 1. Dissemination and destruction. |  |
| 3.7 | **Level Three Security Awareness Training –** In addition to the above Level 1 & 2 requirements, the following topics, shall be covered as a minimum training baseline for all **authorized personnel with both physical and logical access to CJI**. Are these areas covered?  **EXAMPLES:** Anyone with logical access such as terminal operators, law enforcement personnel, legal or court staff   1. Rules that describe responsibilities and expected behavior with regards to information system usage. |  |
|  | 1. Password usage and management—including creation, frequency of changes, and protection. |  |
|  | 1. Protection from viruses, worms, trojan horses, malware, ransomware and other malicious code. |  |
|  | 1. Social engineering. |  |
|  | 1. Unknown e-mail/attachments, SPAM, Phishing emails, etc. |  |
|  | 1. Web usage-allowed versus prohibited; work-related only, & monitoring user activity. |  |
|  | 1. Physical Security—increases in risks to systems and data. |  |
|  | 1. Handheld device security issues—address both physical and wireless security issues. |  |
|  | 1. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance. |  |
|  | 1. Laptop security—address both physical and information security issues. |  |
|  | 1. Personally owned equipment and software—state whether allowed or not (e.g., copyrights) |  |
|  | 1. Access control issues—address least privilege and separation of duties. |  |
|  | 1. Individual accountability—explain what this means in the agency, review of agency policy. |  |
|  | 1. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain. |  |
|  | 1. Desktop security—discuss use of screensavers, restricting visitors’ view of information on screen (mitigating “shoulder surfing”), battery backup devices, external/USB drives, allowed access to systems. |  |
|  | 1. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed. |  |
|  | 1. Threats, vulnerabilities, and risk associated with accessing CJIS networks, systems and services. |  |
| 3.8 | **Level Four Security Awareness Training –** In addition to the above Level 1,2 & 3 requirements, the following topics, shall be covered as a minimum training baseline for **all technology personnel**. Are these areas covered?  **EXAMPLES: T**echnical personnel and vendors, e.g. network or system administrators, telephone/ telecomm, radio and wireless technicians.   1. Protection from viruses, worms, trojan horses, email, malware, ransomware, and other malicious code—scanning, updating definitions. |  |
|  | 1. Data backup and storage—centralized or decentralized approach. |  |
|  | 1. Timely application of system patches—part of configuration management. |  |
|  | 1. Access control measures, e.g. physical security and logical security such as access limits to networks, system files or data. |  |
|  | 1. Network infrastructure protection measures, e.g. firewalls, routers, WAF’s, SIEM’s |  |
| 3.9 | Are all security awareness and specific information system security training records for individuals documented by the agency and kept current, and maintained in a secure location for periodic review? |  |

## Incident Response (CSP 5.3)

To protect CJI assets, agencies need to establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities. The agency must track, document, and report incidents to appropriate agency officials and/or authorities.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 4.1 | Does the agency receive information system security alerts and/or advisories on a regular basis?  If so, from whom? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 4.2 | Has your agency experienced a security event/incident within the last 24 months? (Examples would include infected machines that had to be manually cleaned, insider threats, compromises to websites or servers). |  |
| 4.3 | Are agency employees, contractors, vendors and third party users aware of the agency’s incident reporting procedures? |  |
| 4.4 | Does the agency employ automated mechanisms to make security alerts and advisory information available throughout the agency? If true, provide examples? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 4.5 | Are there staff member(s) assigned in the agency as a primary contact for interfacing with the DOJ Security Office concerning incident handling and response? Please list them here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 4.6 | Are there individuals who are assigned responsibility for reporting incidents within their areas? |  |
| 4.7 | Does the agency collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident? |  |
| 4.8 | Does the agency promptly report possible security incidents to the DOJ Information Security Officer? |  |
| 4.9 | Does the agency have an information security events/incident response policy/procedure in place? |  |
| 4.10 | Does the agency act as a single point of contact for their jurisdictional area for requesting incident response assistance? |  |
| 4.11 | Has the agency implemented an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery? |  |
| 4.12 | Does the agency employ automated mechanisms to support the incident handling process? Examples? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 4.13 | Does the agency obtain incident-related information from a variety of sources including, but not limited to, audit, network, physical access monitoring, and user/administrator reports? |  |
| 4.14 | Is there follow-up action/review against a person or agency after an information event security incident? |  |
| 4.15 | Is the security event/incident documented in writing? |  |
| 4.16 | Does the agency include incident response roles as part of the required security awareness training? |  |
| 4.17 | Does the agency track and document security incidents on an ongoing basis? |  |
| 4.18 | Does the agency know that the Montana DOJ has cyber security resources to assist your agency if you suspect there has been a security incident or event that you need assistance with? (NOTE: These events are kept confidential.) |  |

## Auditing and Accountability (CSP 5.4)

Agencies shall implement auditing and accountability controls to protect CJI and monitor user behavior. Agencies shall carefully inventory technical components, systems and architecture (including virtual) to determine which security controls are applicable. This section applies to any information system that houses CJI, interfaces with a system that contains CJI or any network that transmits CJI.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 5.1 | 1. Does the agency use a DOJ-leased CJIN system? |  |
|  | 2. Is this leased CJIN system used **to conduct CJI business use only (meaning no personal use)**? |  |
|  | 1. Does the agency use a SummitNet connection to access CJIN?   **If questions 1-3 are true, skip the rest of this section and proceed to the Access Control Section on the next page. (CSP 5.5)** |  |
| 5.2 | If the agency isn’t using OMNIXX to access CJIN, what system(s) are you using? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Fill out the following questions below (5.3-5.13) for the system you are using.** |  |
| 5.3 | Does the agency criminal justice information system log successful and unsuccessful log-on attempts? |  |
| 5.4 | Does the agency criminal justice information system log attempts to use any permissions on any user account, file, directory, or other system resource? |  |
| 5.5 | Does the agency criminal justice information system log successful and unsuccessful attempts to change account passwords? |  |
| 5.6 | Does the agency criminal justice information system log successful and unsuccessful actions to privileged accounts? |  |
| 5.7 | Does the agency criminal justice information system log successful and unsuccessful attempts to access the audit log file? |  |
| 5.8 | Does the agency criminal justice information system audit logs include the following:   1. Date and time of the event? |  |
|  | 1. Component (e.g. hardware, software) of information system where the event occurred? |  |
|  | 1. Type of event? |  |
|  | 1. User/subject identity (e.g., user who attempted to change password)? |  |
|  | 1. Outcome of event (success or failure)? |  |
| 5.9 | Does the agency information system alert appropriate officials in the event of an audit processing failure (e.g., the audit log storage capacity has been reached)? |  |
| 5.10 | Does the agency have assigned an individual or position to review the audit logs at least once a week? |  |
| 5.11 | Does the agency information system provide a timestamp for each audit record that is generated? |  |
| 5.12 | Does the agency information system protect audit information from modification, deletion, and unauthorized access? |  |
| 5.13 | Does the agency retain these audit logs for at least one (1) year? |  |
| 5.14 | If applicable, does the agency retain logs of all NCIC and Type III transactions for at least 1 year? |  |

## Access Control (CSP 5.5)

Access control provides appropriate restrictions to the processing and transmission of CJI. These restrictions include access to systems, applications, services and communication configurations that allow access to CJIS information

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 6.1 | Does the agency manage information system accounts (e.g., creating, modifying, reviewing, disabling, and removing accounts) for systems that contain, access, process or transmit CJI? Examples of these types of systems would be Active Directory, Windows workgroups, network shares, Microsoft documents, email, RMS, CAD, 911/dispatch, CJI interfaces, backups, cloud applications, or other applications? **If not, proceed to 4**.  **If yes, please list these information systems here**:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 6.2 | **Questions 2-9 must be answered for each system that contains, transmits, stores or accesses CJI.**  Does your agency information system restrict access of privileged functions to explicitly authorized personnel?   * Mobile……………………………………………………………………………………………………………………………….. * CAD……………………………………………………………………………………………………………………………………. * RMS…………………………………………………………………………………………………………………………………… * 911/Dispatch……………………………………………………………………………………………………………………… * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 6.3 | Does your agency implement the principle of *least privilege* (granting no more rights or permissions than necessary) to limit access to the **information system** to only authorized personnel with the need and the right to know?   * Mobile……………………………………………………………………………………………………………………………….. * CAD……………………………………………………………………………………………………………………………………. * RMS…………………………………………………………………………………………………………………………………… * 911/Dispatch……………………………………………………………………………………………………………………… * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 6.4 | Does the agency manage information system accounts (e.g., creating, modifying, reviewing, disabling, and removing accounts) for systems that access CJI?   * Mobile……………………………………………………………………………………………………………………………….. * CAD……………………………………………………………………………………………………………………………………. * RMS…………………………………………………………………………………………………………………………………… * 911/Dispatch……………………………………………………………………………………………………………………… * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 6.5 | Does the agency information system restrict access of privileged functions to explicitly authorized personnel?   * Mobile……………………………………………………………………………………………………………………………….. * CAD……………………………………………………………………………………………………………………………………. * RMS…………………………………………………………………………………………………………………………………… * 911/Dispatch……………………………………………………………………………………………………………………… * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 6.6 | Do these systems as defined in Question 1 lock an account after 5 consecutive invalid access attempts to access CJI.?   * Mobile……………………………………………………………………………………………………………………………….. * CAD……………………………………………………………………………………………………………………………………. * RMS…………………………………………………………………………………………………………………………………… * 911/Dispatch………………………………………………………………………………………………………………………- * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 6.7 | Does the system hold the account locked for at least 10 minutes unless released by an administrator?   * Mobile……………………………………………………………………………………………………………………………….. * CAD……………………………………………………………………………………………………………………………………. * RMS…………………………………………………………………………………………………………………………………… * 911/Dispatch……………………………………………………………………………………………………………………- Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 6.8 | Does the system display a warning banner informing users that they are accessing a restricted system, subject to audit, and that unauthorized use may be subject to criminal and/or civil penalties, and that they consent to monitoring or recording?   * Mobile……………………………………………………………………………………………………………………………….. * CAD……………………………………………………………………………………………………………………………………. * RMS…………………………………………………………………………………………………………………………………… * 911/Dispatch……………………………………………………………………………………………………………………… * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 6.9 | Does the agency manage information system accounts (e.g., creating, modifying, reviewing, disabling, and removing accounts) for **any other systems that contain or access CJI**? These systems are outlined in Question **6.1**. |  |
| 6.10 | Does the agency use any personally owned devices (BYOD) to access CJI? |  |
| 6.11 | Does the agency have any publicly accessible computers that might have access to CJI? |  |
| 6.12 | Does the agency authorize, monitor and control all methods of remote access to CJI systems? **If no remote access is provided to vendors, please skip to question #7.1.** |  |
| 6.13 | Does the agency have contractors/vendors that remotely access agency technology systems or networks?  Please list them here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 6.14 | Does the agency have documented the technical and administrative processes for enabling remote access? |  |
| 6.15 | Remote access requires the following conditions. Does the agency:   * Monitor the session at all times by an authorized escort………………………………………………………… * Have an escort that is familiar with the system in which the work is being performed……………. * Have the ability to end the session at any time……………………………………………………………………….. * Ensure that the connection is secured using FIPS 140-2 encryption………………………………………… * Ensure that remote connectivity is using Advanced Authentication………………………………………… |  |
| 6.16 | Has the remote access contractor/vendor signed the CJIS Contractor Security Addendum? |  |

## Identification and Authentication (CSP 5.6)

The agency shall uniquely identify information system users and processes and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems, services or networks.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 7.1 | Does the agency require a unique user ID for all users who access CJI or any system that accesses, stores, transmits or processes CJI? |  |
| 7.2 | Does the agency allow users to share user logins or ID’s? |  |
| 7.3 | Does the agency keeps a list of authorized users current by adding new users and deleting former users? |  |
| 7.4 | Does the agency enforce the following password rules for CJI system access?   1. Password is at least 8 characters………………………………………………………………………………………………… 2. Password is not a dictionary word or proper name…………………………………………………………………….. 3. Password is not the same as the user ID…………………………………………………………………………………….. 4. Passwords expire within a maximum of 90 calendar days…………………………………………………………… 5. Password is not identical to the previous ten (10) passwords…………………………………………………….. 6. Passwords are not transmitted in the clear (unencrypted) outside the secure location……………… 7. Passwords are not displayed when entered (e.g., displays \*\*\*\*\*\*\*\* instead of “password”)…….. |  |
| 7.5 | Does the agency disable or remove user access once that user no longer needs access to CJI? |  |
| 7.6 | Does the agency archive or store user ID’s for future auditing purposes? |  |
| 7.7 | Does the agency use PINs for authentication to systems processing or storing CJI? If not, proceed to **question 7.9.** |  |
| 7.8 | Is the PIN used by itself to authenticate (i.e., not in conjunction with something like a certificate or key-fob)? |  |
| 7.9 | Has the agency implemented Advanced Authentication (AA) as an additional security mechanism for access to systems or networks containing CJI? |  |

## Configuration Management (CSP 5.7)

Planned or unplanned changes to the hardware, software, and/or firmware components of an information system or network can have significant effects on the overall security of the system. Only qualified and authorized individuals should have access to initiate changes, upgrades or modifications.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 8.1 | Do you allow only qualified/authorized individuals access to information systems components and networks for purposes of initiating changes, upgrades or modifications? |  |
| 8.2 | Does the agency employ the principle of least privilege when allowing users access to an information system that contains or transmits CJI? |  |
| 8.3 | Does the agency configure CJI systems and networks to provide only essential capabilities and specifically prohibit/restrict the user to specified functions, ports, protocols or services? |  |
| 8.4 | Does the agency have a completed topological drawing (a network diagram) on file that depicts the interconnectivity of the agency network along with logical components (e.g., firewalls, routers, switches, servers, workstations) and communications paths (e.g., circuits, interfaces)? **See Appendix D for more information.** |  |
| 8.5 | Has the agency network diagram been completed in the last 24 months? |  |
| 8.6 | Has the agency network diagram been submitted to the DOJ Security Office for review? |  |
| 8.7 | Does the agency document system configuration information and protect it from unauthorized access? |  |
| 8.8 | Does the agency have a documented configuration (or change) management policy? |  |
| 8.9 | Does the agency regularly review and approve needed changes to technology systems and networks through a formal or informal process? |  |

## Media Protection (CSP 5.8)

Digital and physical media in all forms is restricted to authored individuals. Media protection policy and procedures must be in place for securely handling, transporting and storing media. (Digital media is any storage media such as memory devices in laptops and computers (hard drives) and removable, transportable digital memory media, includes magnetic tape or disk, optical disk, flash drives, external hard drives, digital memory card, etc. Physical media includes printouts, printed documents, images, etc.)

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 9.1 | 1. Does the agency use email or applications hosted by a vendor or 3rd party provider? **If no, skip to question #9.2.** |  |
|  | 1. Does this 3rd party provider have written documentation on how they handle backups, media protection and disposal? |  |
|  | 1. If yes, does it meet FIPS 140-2 compliance? |  |
| 9.2 | Does the agency securely store digital and physical media within a physically secure location? |  |
| 9.3 | Is access of digital and physical media restricted to only authorized staff? |  |
| 9.4 | Does the agency transport CJI outside the secured area which is restricted to authorized personnel? |  |
| 9.5 | Does this agency safeguard CJI during transport outside of the secure location? |  |
| 9.6 | Is CJI electronically stored outside of the physically secure location? |  |
|  | 1. If so, is this data encrypted to the FIPS 140-2 standard? |  |
| 9.7 | Does the agency use USB thumb drives or external drives to transfer CJI? |  |
|  | 1. If so, is this encrypted and inventoried? |  |
| 9.8 | Does the agency sanitize or degauss electronic media prior to disposal or release for reuse? |  |
|  | 1. If so, is the electronic media kept in a secure location prior to disposal? |  |
| 9.9 | Does this agency destroy inoperable electronic media? |  |
| 9.10 | Is the sanitization or destruction of electronic media witnessed or carried out by authorized personnel? |  |
| 9.11 | Does the agency securely dispose of physical media when no longer needed? |  |
|  | 1. If so, is the physical media kept in a secure location prior to disposal? |  |
| 9.12 | Are there written policies and/or procedures related to the above media protection requirements? |  |

## Physical Protection (CSP 5.9)

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 10.1 | Does the agency have written physical protection policies and procedures to ensure CJI information systems, networks, hardware, and software are physically protected? |  |
| 10.2 | Are the agency’s main entrances physically secured and posted that they are restricted areas? |  |
| 10.3 | Does the agency directly control all physical access points to secure locations including all telecommunications and wiring closets? |  |
| 10.4 | Is there a maintained list of all authorized personnel who are allowed access to secure locations? |  |
| 10.5 | Does this agency verify the identity of visitors before granting access to secure locations? |  |
| 10.6 | Does the agency directly control physical access to information systems and networks within the secure locations? |  |
| 10.7 | Does the agency share information systems, networks or office space with other entities in this location or other agency remote locations? |  |
| 10.8 | Does the agency control physical access to information system devices that display CJI by protecting such devices from unauthorized accessing and viewing of CJI? |  |
| 10.9 | Does the agency monitor physical access to the information systems and network closets to detect and respond to physical security incidents? |  |
| 10.10 | Does the agency control physical access by authenticating visitors before authorizing escorted access to the physically secure location and then monitoring their activity? |  |
| 10.11 | Does the agency authorize and control information system-related items entering and exiting the physically secure location? |  |

## System and Communications Protection and Information Integrity (CSP 5.10)

Applications, services, information systems, virtual environments, and networks must have the capability to ensure system integrity through the detection and protection against unauthorized changes.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 11.1 | If the agency transmits CJI outside the physically secure location or agency network, is this data encrypted to meets FIPS 140-2 standards? |  |
| 11.2 | If the agency shares a network infrastructure with non-criminal justice users (e.g., other county, state agencies, or private businesses), then the criminal justice information on your network should be protected from unauthorized access with the following methods:   * CJI is encrypted with a FIPS 140-2 compliant encryption mechanism * CJI is logically separated (e.g., CJI is only accessible on a secure VLAN) |  |
| 11.3 | If any of the systems listed in **Section 1** also interface with CJIS, is the criminal justice information protected from unauthorized access with the following methods:   * CJI is encrypted with a FIPS 140-2 compliant encryption mechanism * CJI is logically separated (e.g., CJI is only accessible on a secure VLAN) |  |
| 11.4 | Has the agency implemented network- and/or host-based intrusion detection tools?  List the tools that you use: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 11.5 | Does the agency monitor inbound and outbound communications for unusual or unauthorized activities? |  |
| 11.6 | Are intrusion detection logs sent to a central logging facility where correlation and analysis can be utilized to prevent intrusion detection for the agency technology environment? |  |
| 11.7 | Does the agency employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks (e.g. antivirus or anti-malware software)? |  |
| 11.8 | Does the agency utilize a network- and/or host-based firewall to prevent unauthorized access to the agency network and CJI systems and data?  If yes, what firewall make and model does the agency use? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 11.9 | Are all connections to the internet/other networks through controlled interfaces (e.g., proxies, switches, routers, firewalls, encrypted tunnels, etc.) secured? |  |
| 11.10 | Are agency controlled interfaces (e.g. firewalls, routers, switches, encrypted tunnels,) updated on a regular basis for security patches? |  |
| 11.11 | Are agency controlled interfaces configured with the following preventative measures:   1. Account lockout |  |
|  | 1. Password complexity |  |
|  | 1. Logging is turned on |  |
| 11.12 | Does the agency inspect controlled interfaces for unauthorized changes? |  |
| 11.12 | Does the agency use SSH or Encryption when logging on to controlled interfaces? |  |
| 11.13 | Does the agency block login access via wireless networks to controlled interfaces? |  |
| 11.14 | Is a backup taken of the controlled interfaces configuration and stored securely elsewhere? |  |
| 11.15 | Are all boundary protection devices (proxies, routers, firewalls, encrypted tunnels, etc.) configured to fail closed in the event of a failure? |  |
| 11.16 | Does the agency utilize a bridge network with SummitNet or any other network? |  |
| 11.17 | Are publicly accessible information system components (e.g., web servers) divided into physically or logically separated networks through separate network interfaces? |  |
| 11.18 | **If applicable,** any CJI stored outside of the physically secure location is encrypted to FIPS 140-2 standards. Does the agency store any CJI outside the physically secure location? |  |
| 11.19 | **If applicable,** any passphrases used to decrypt CJI must meet the following requirements. If used, the passphrase:   1. Is at least 10 characters |  |
|  | 1. Is not a dictionary word |  |
|  | 1. Includes at least 1 upper case letter, 1 lower case letter, 1 number, and 1 special character |  |
|  | 1. Can be changed or locked when previously authorized personnel no longer require access |  |
| 11.20 | Does the agency uses **public** cloud providers (e.g., Microsoft Azure, Amazon Web Services, Google, etc.) to host or store criminal justice information systems, applications, or data? |  |
|  | Does the agency use **private** cloud provides (e.g. State of Montana Data Center, vendor data center) to host or store criminal justice information systems, applications, or data?  **If your agency does use cloud providers, please list them in Appendix A and complete Appendix B.** |  |
| 11.21 | Does the agency transmit any CJI via fax (facsimile)? |  |
| 11.22 | Does the agency physically or electronically transmit CJI to courts, judges or attorneys as needed for ongoing law enforcement activities? |  |
| 11.23 | If the agency uses fax servers to send faxes through an application or service, does the transmission meets the encryption requirements of FIPS 140-2? |  |
| 11.24 | Does the application, service, or information system separate user functionality from system management functionality?  **EXAMPLES:** Running services on different computers, different central processing units, different instances of the operating system, and different network addresses.) |  |
| 11.25 | Does the agency utilize one or more Voice over Internet Protocol (VoIP) telephone systems? |  |
| 11.26 | Does the agency run applications or services that utilize CJI in a virtual environment (e.g., virtual machines)? **(If no, skip to Q 12.1.)** |  |
| 11.27 | Does the agency have a policy in place for regularly patching software and hardware? |  |
| 11.28 | Is malicious code protection implemented on all information technology systems that store and/or CJI? |  |
| 11.29 | Is malicious code protection software automatically updated if connected to the internet **OR** is regularly updated on systems that are not connected to the internet? |  |
| 11.30 | Does the agency implement spam protection on all information system entry points (e.g., mail servers, web servers)? |  |
| 11.31 | Does the agency implement spyware protection on all workstations, servers, and mobile devices on the network? |  |
| 11.32 | Is the agency able to receive recent security alerts and advisories and take appropriate action on those advisories? |  |
| 11.33 | Are appropriate personnel assigned to mitigate these alerts and advisories and document actions taken in response? |  |
| 11.34 | Are automated mechanisms employed to make this information available throughout the agency? |  |

## Formal Audits (CSP 5.11)

Formal audits are conducted to ensure compliance with applicable statues, regulations and policies.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 12.1 | Does the agency submit to random audits by the FBI CJIS Division at least once every three years? |  |
| 12.2 | Does the agency submit to audits (both technical and administrative) by the Montana DOJ Security Office? (Examples include FBI, CJIN and CRISS audits) |  |
| 12.3 | Does the agency understand it could be required to submit to unannounced security inspections? |  |
| 12.4 | Does the agency know that any contractor or vendor the agency uses must submit to unannounced security inspections? |  |
| 12.5 | Does the agency permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations? |  |

## Personnel Security (CSP 5.12)

Having proper security measures against insider threats is critical. Security requirements apply to all personnel who might be exposed or have access to CJI. This includes individuals who have physical, logical or virtual access to devices that store, process, or transmit CJI.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 13.1 | Is a state of residency and a national, fingerprint-based criminal record background check conducted on all personnel, including vendors, within 30 days of assignment? (NOTE: Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.) |  |
| 13.2 | Do all personnel who might be exposed or have physical or logical access to CJI re-investigated with fingerprint-based, national background checks every 5 years? |  |
| 13.3 | Minimum screening requirements for individuals requiring access to CJI:   1. Does the agency verify a state of residency and national fingerprint-based record checks within 30 days of assignment for all personnel and vendors (including technical staff) who have access to CJI? ………………………………………………………………………………………………………………….. 2. Has the agency ever granted access to anyone who had a felony arrest or conviction?...……….. 3. If there is a record, have you submitted a request to the CSO or his/her designee to review the matter to determine if access is appropriate? …………………………………………………………………………. 4. If a person already has access to CJI and is subsequently arrested and/or convicted, has your agency consulted the CSO or his/her designee to determine if access is appropriate? ……………. 5. Does any agency support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas that have not had national fingerprint-based record checks get escorted through secured areas by authorized personnel always? ……………… |  |
| 13.5 | In addition to meeting the requirements in 13.3, do contractors and vendors are required to meet the following requirements?   1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances….. 2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer……………………………………………………………………… 3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter…………………………………………………………………………………………………… 4. Any employee or contractor found to have a criminal record consisting of felony conviction(s) shall be disqualified………………………………………………………………………………………………………………….. 5. Applicants shall also be disqualified based on confirmations that arrest warrants are outstanding for such applicants………………………………………………………………………………………………… 6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO…………………………………………… |  |

## Mobile & Wireless Devices (CSP 5.13)

Considerations and requirements for mobile devices include smartphones, tablets and other small form factors. Mobile devices are not limited to a single form factor or communications medium. Examples of wireless communication technologies include 802.11, cellular, Bluetooth, satellite, microwave and land mobile radio.

|  | Wireless Technologies | Select if True |
| --- | --- | --- |
| 14.1 | Does the agency authorize, monitor and control access to wireless networks and information systems? **If no, please move to Section 15.0.** |  |
|  | 1. Who is your wireless equipment vendor(s)?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  | 1. Who maintains your wireless equipment? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 14.2 | Does the agency use any part of a wireless network to transmit CJI?   1. If yes, is CJI transmitted using FIPS 140-2 standards? |  |
|  | 1. Are encryption keys are at least 128-bits? |  |
|  | 1. Are default shared keys are replaced by unique keys? |  |
|  | 1. Has Ad hoc mode been disabled? |  |
|  | 1. Are all nonessential management protocols disabled on the AP’s? |  |
|  | 1. Are all management access and authentication occurring via FIPS compliant secure protocols? |  |
|  | 1. Are all non-FIPS compliant secure access to the management interface? |  |
| 14.3 | Are security features, including cryptographic authentication, firewall and other security and privacy features enabled to protect CJI? |  |
| 14.4 | Does the agency have logging enabled? |  |
|  | 1. Are the logs reviewed monthly and on a recurring basis? |  |
|  | 1. Who reviews these logs? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 14.5 | Does the agency:   1. Perform validation testing to ensure rogue Access Points (AP’s) don’t exist? |  |
|  | 1. Maintain a complete documented inventory of all AP’s? |  |
|  | 1. Place AP’s in secured areas to prevent tampering? |  |
|  | 1. Test AP range boundaries to determine extent of wireless coverage? |  |
|  | 1. Enable user authentication and encryption mechanisms for the management interface of AP’s? |  |
|  | 1. Ensure that all AP’s have strong administrative passwords and that they are changed regularly? |  |
|  | 1. Ensure that factory default settings are not utilized and important AP functions are customized and protected? |  |
|  | 1. Change the default service set identifier (SSID)? |  |
|  | 1. Disable the broadcast SSID feature so that the client SSID must match the AP device? |  |
|  | 1. Validate that the SSID character string does not contain any agency identifiable information? |  |
|  | 1. Insulate (virtually (VLAN’s or ACL’s) or physically) the wireless network from other networks and network infrastructure? |  |
| 14.6 | When disposing of access points, does the agency clear configurations, passwords, etc. to prevent disclosure of network configuration information? |  |
| 14.7 | Are critical patches and upgrades applied to wireless access points as they are released by the vendor? |  |
| 14.8 | Does the agency utilize mobile hotspots to allow connectivity to your agency network where CJI is used? |  |
|  | Are all agency hotspots configured to:   1. Enable encryption on the hotspot? …………………………………………………………………………………………. 2. Change the hotspot’s default SSID? …………………………………………………………………………………………. 3. Ensure the hotspot SSID doesn’t identify the device make/model or agency ownership? ……….. 4. Have complex wireless passwords? …………………………………………………………………………………………. 5. Enable the hotspot’s port filtering/blocking features? …………………………………………………………….. 6. Only allow connections from agency controlled devices? ………………………………………………………... |  |
| 14.9 | Does the agency use mobile devices to transmit CJI? (**If no, proceed to question 14.15)** |  |
| 14.10 | Does the agency utilize a mobile device management (MDM) solution for mobile devices (phones or tablets)? |  |
| 14.11 | Does the agency establish usage restrictions for mobile devices? |  |
| 14.12 | Does the agency have written policies and procedures on how mobile devices are to be used? |  |
| 14.13 | On mobile devices, does the agency:   1. Apply critical patches and upgrades to the operating system as soon as they are available for the device and after they have been tested? …………………………………………………………………………… 2. Configure for local device authentication? ……………………………………………………………………………… 3. Used advanced authentication or an approved compensating control? ………………………………….. 4. Encrypt all CJI resident on the device? ……………………………………………………………………………………. 5. Erase cached information, to include authenticators in applications, when the session is terminated? ……………………………………………………………………………………………………………………………. 6. Employ malicious code protection? ………………………………………………………………………………………… 7. Employ a personal firewall service to protect CJI on the device? …………………………………………….. |  |
| 14.14 | Has the agency ever experience a loss or compromise of a mobile device that contained CJI? |  |
| 14.15 | Does the agency use or maintain radio equipment or systems? **(If yes, please answer the following questions below.)** |  |
|  | 1. Is the radio equipment connected to the agency network? |  |
|  | 1. If so, is the radio traffic segregated from other agency network traffic? |  |
|  | 1. How are IP addresses assigned to radio equipment? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 14.16 | Does the agency utilize any Bluetooth technologies? If so, please list them here: \_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

## Application / Interface Security

Application security encompasses measures taken throughout the code's life-cycle to prevent gaps in the [security policy](https://en.wikipedia.org/wiki/Security_policy) of an [application](https://en.wikipedia.org/wiki/Application_software) or the underlying [system](https://en.wikipedia.org/wiki/Operating_system) ([vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability_(computer_science))) through flaws in the [design](https://en.wikipedia.org/wiki/Software_design), [development](https://en.wikipedia.org/wiki/Software_engineering), [deployment](https://en.wikipedia.org/wiki/Software_deployment), [upgrade](https://en.wikipedia.org/wiki/Software_upgrading), or [maintenance](https://en.wikipedia.org/wiki/Software_maintenance) or [database](https://en.wikipedia.org/wiki/Database) of the application. In most cases, completion will require input by the vendor technology staff that maintains your criminal justice information system, software or network.

NOTE: If there is more than one application or interface that stores CJI, this section must be filled out for each application or interface.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 15.1 | Has your agency completed a risk assessment with the vendor whose application you are using? |  |
| 15.2 | Does your vendor carry cyber security liability insurance? |  |
| 15.3 | Is database software installed using default or typical options?  If no, are:   * Unneeded roles locked or disabled? ……………………………………………………………………………………….. * Default role passwords change or locked? ………………………………………………………………………………. * Password management enabled? …………………………………………………………………………………………… * Auditing and logging turned on and monitored? ……………………………………………………………………. * Unnecessary tools uninstalled? ……………………………………………………………………………………………… |  |
| 15.4 | Is operating system access to the database server (or host) restricted to authorized users physically and logically? |  |
| 15.5 | Is traffic between clients, databases and the application encrypted? |  |
| 15.6 | Are security patches to the database and related components applied regularly?  Please explain your patch management strategy for this system: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 15.7 | Is operating system software installed using default or typical options?  If yes:   * Is anti-virus / anti-malware software installed? ………………………………………..………………….…………. * The firewall enabled? ………………………………………..………………………………………..……………………..…… * Unnecessary users disabled or deleted? ………………………………………..……………………………………….. * The guest account disabled? ………………………………………..………………………………………………………… * Do administrator, system administrators, or similar privileged account user passwords meet password complexity requirements? ……………………………………………..……………………………………. * Are unused services disabled or uninstalled? ………………………………………..……………………………….. * Are unnecessary ports disabled? ………………………………………..………………………………………………….. * Is the Operating System hardened per the [MT-ISAC Hardening Guide](http://sitsd.mt.gov/Portals/165/docs/MT-ISAC/2016/2016.09.15/Hardening%20of%20Devices.pdf?ver=2016-09-14-165436-047)? ……………..…………………… |  |
| 15.8 | What is the vendor and application name? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 15.9 | Is the application regularly tested for vulnerabilities?  If so, what methodology is used? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  If so, how often is it tested? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 15.10 | Is the vendor’s code digitally signed? |  |
| 15.11 | Is the application kept current to the latest version? |  |
| 15.12 | Does the vendor provide security patches and updates for the application? |  |
| 15.13 | Is the vendors product certified to run on Windows 7? Windows 8? Or Windows 10? Please list compatible versions of Windows here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 15.14 | Does the application use Java?  -If so, is it patched to the latest version? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| 15.15 | Does the application have auditing and logging functions turned on within the application?  -If so, how long are those records kept for? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  -Who reviews them? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

## Appendix A - service proviDers

### Cloud Providers

If applicable, please list all cloud providers, public and private (e.g., Microsoft Azure, Amazon Web Services, State of Montana Data Center, etc.) used to host or store criminal justice information systems, applications, or criminal justice data. If you do use any cloud providers, you must also complete **Appendix B.**

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

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 1 | Does your cloud provider fingerprint, background check and vet their employees? |  |
| 2 | Does your cloud provider fingerprint, background check and vet their vendors if they have unescorted or remote access to agency networks and systems? |  |
| 3 | Is CJI encrypted with FIPS 140-2-compliant encryption before entering the cloud? |  |
| 4 | If CJI is stored unencrypted by a 3rd party cloud provider, the following requirements must be met:  **2.1** Are Security Addendums signed by all unescorted private contractor/vendor personnel?  **2.2** Do all unescorted private contractor/vendor personnel meet the requirements of section **13. Personnel Security (see page 17)**?  **2.3** Is Security Awareness Training completed by all unescorted contractor/vendor personnel? |  |
| 5 | Is all agency CJI stored within a physically secured location (i.e., the agency knows which data center contains the data), and encrypted at rest in and in transit? |  |
| 6 | Can the agency provide a network diagram that can depict CJI in the cloud environment (if so, please attach the network diagram at the end of this questionnaire)? |  |
| 7 | Are private contractors/vendors with access uniquely identified? |  |
| 8 | Has the cloud provider provided details on how they meet the requirements of the CJIS Security Policy? If so, please attach any relevant documentation to the end of this questionnaire. |  |
| 9 | Does the cloud provider have written documentation on the following:   * + Backups, business continuity planning, and disaster recovery planning? |  |
|  | * + Media protection and disposal   If so, please attach any relevant documentation to the end of this questionnaire. |  |
| 10 | Does the cloud provider know they are contractually prohibited from using metadata derived from CJI for any purpose? |  |
| 11 | Does the cloud provider know they are contractually prohibited from scanning email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided? |  |

## Appendix B – VirtualizatioN [CSP 5.10.3.2]

Virtual environments are much more complex. Virtualization approaches added to current networks require additional security considerations. These questions attempt to identify the differences, issues, challenges, risks, etc. caused by virtualization, to make sure that this addition to the network is just as secure as the network before the addition of virtualization.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 1 | Is there limited physical access to the virtual hosts? (Meaning only authorized administrative personnel should have physical access to the host system to prevent unauthorized changes.) |  |
| 2 | Is the integrity of files verified prior to installation? (e.g. verify the hash values of system files, as provided by the vendor, prior to installation to ensure integrity) |  |
| 3 | Are hash values stored separately offline (e.g., on a CD-ROM or other read- only media) to ensure that a malicious user has not re-hashed any modified files? |  |
| 4 | Are only required operating system components and services loaded and enabled? (Meaning no unnecessary operating systems components (e.g., drivers) are loaded, and no unnecessary services are enabled (e.g., printing services, file sharing services)?) |  |
| 5 | Are passwords used for BIOS and bootloaders (e.g., GRUB) for both hosts and guests? |  |
| 6 | Is time synchronized for host and guests? |  |
| 7 | Do hosts only have accounts necessary for managing VMs? (RECOMMENDATION: Use of strong authentication (e.g., two factor authentication) is recommended, but if passwords are used then ensure that they are strong, hard to guess, changed frequently, and only provided to authorized administrators.) |  |
| 8 | Are credentials used for access to the host operating system (OS) also used for access to guest Oss? |  |
| 9 | Are all unnecessary programs uninstalled, and all unnecessary services disabled? |  |
| 10 | Is configuration management of host OSs centralized to ensure that configurations are standardized? |  |
| 11 | Are deployed configurations documented in order to be effectively managed? |  |
| 12 | Are host OSs patched regularly and in a timely fashion to ensure that the host OS is protecting the system itself and guest OSs properly? |  |
| 13 | Is virtualization software and firmware patched regularly? |  |
| 14 | Are host OSs hardened following an organization's approved hardening or build standard, or from independent or vendor guides? (e.g., the Center for Internet Security, Defense Information Systems Agency, National Security Agency) |  |
| 15 | Are only authorized administrators allowed to login to systems as “administrator” or “root”? |  |
| 16 | Are authorized administrators logging in with their own accounts, either set-up with sufficient administrative rights (e.g., using sudo), or su to “root”? |  |
| 17 | Are volumes or disk partitioning used to prevent inadvertent denials of service from virtual machines (guest operating systems, OSs) filling up available space allocations? |  |
| 18 | Are VM’s configured by default to disconnect unused physical or peripheral devices? |  |
| 19 | Are virtual devices for guest Oss associated with the appropriate physical devices on the host system? (e.g. mapping between virtual NICSs to the proper physical NICs) |  |
| 20 | Are physical switch ports connected to virtual trunk ports configured as static trunk links? |  |
| 21 | Are spanning tree protocols disabled? |  |
| 22 | Are layer 2 security configurations used to restrict the ability of virtual adapters from entering promiscuous mode and prevent them from examining switch traffic? |  |
| 23 | Is strong authentication used for host system access? (multi-factor authentication is recommended for access to host systems) |  |
| 24 | Is file sharing disabled between guest and host Oss? |  |
| 25 | Are warning banners used for both hosts and guests? (Warning banners are required to successfully prosecute unauthorized users who improperly use a computer. Banners should be displayed on all systems prior to access and warn users about: (a) what is considered the proper use of the system; (b) that the system is being monitored to detect improper use and other illicit activity, and; (c) that there is no expectation of privacy while using this system.) |  |
| 26 | Is administrative access for management of virtual servers separated from administrative access for management of virtual networks? |  |
| 27 | Is management and centralization of hypervisors restricted to administrators only? |  |
| 28 | Are virtual systems regularly backed up for error recovery? |  |
| 29 | Are test restore’s of virtual systems performed regularly? |  |
| 30 | Is the virtual environment logged and regularly audited? (Examples would include logging and auditing of all components of a virtualized environment, management capabilities, virtual switches, virtual and physical firewalls, and other security devices (e.g., intrusion detection systems, anti-malware capabilities). |  |
| 31 | Is logging for the virtual environment centralized? |  |
| 32 | Are guest OSs protected by a firewall? |  |
| 33 | Are host OSs protected by a firewall? |  |
| 34 | Are there separate VLANs for guest OSs? |  |
| 35 | Are guest OS’s restricted from having management network access? |  |
| 36 | Are the virtual machines (VMs) that store CJI hosted on different physical devices from non-criminal justice or internet-facing systems and applications? |  |
| 37 | Are the hosts isolated from virtual machine(s)? (i.e., VM users cannot access the host/hypervisor level). |  |
| 38 | Are virtual machines that are internet facing (websites, portals, etc.) either **physically separated** from virtual machines that process CJI or are **logically separated** by a virtual firewall or VLAN? |  |
| 39 | Are drivers that serve critical functions stored within the specific VM that they service (i.e., the drivers are not stored in the host/hypervisor)? |  |
| 40 | Is each VM treated as an independent system? |  |
| 41 | **If applicable,** where CJI is in a virtual environment where it will be comingled with non-CJI (**select all that apply**):   1. CJI is encrypted at rest 2. CJI is segregated and stored unencrypted within its own secure VM 3. CJI is encrypted in transit |  |
| 42 | The following best practices are implemented (**select all that apply**):   * Traffic in the virtual environment is monitored by an IDS (intrusion detection system) or IPS (intrusion prevention system)? * Each VM is virtually or physically firewalled in the virtual environment………………………………………. * Administrative duties for the host/hypervisor are segregated……………………………………………………… |  |

## Appendix C – NEtwork diagrams examples [CSP 5.10.3.2]

Provide a topological drawing depicting the interconnectivity of your agency network to the CJIN

network. The drawing must include:

· All communication paths, circuits and other components used for connection, beginning with the agency owned system(s) and traversing through all interconnected systems to the Internet.

· Depict all entry points into the network including any hardware components that are used to isolate the network from other networks at the agency.

· The location of all components (e.g. firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Do not show each workstation; the number of clients is sufficient.

· Depict the beginning point of data encryption and the point where data is decrypted. Identify each segment of the network that encrypted data passes through.

· Identify the transmission methods (data circuit, microwave, cellular technologies, fiber optics, copper

wiring, etc.) being used to transmit or receive CJIN systems data.

· Clearly indicate the boundaries of your criminal justice facility in relation to the equipment illustrated on the diagram

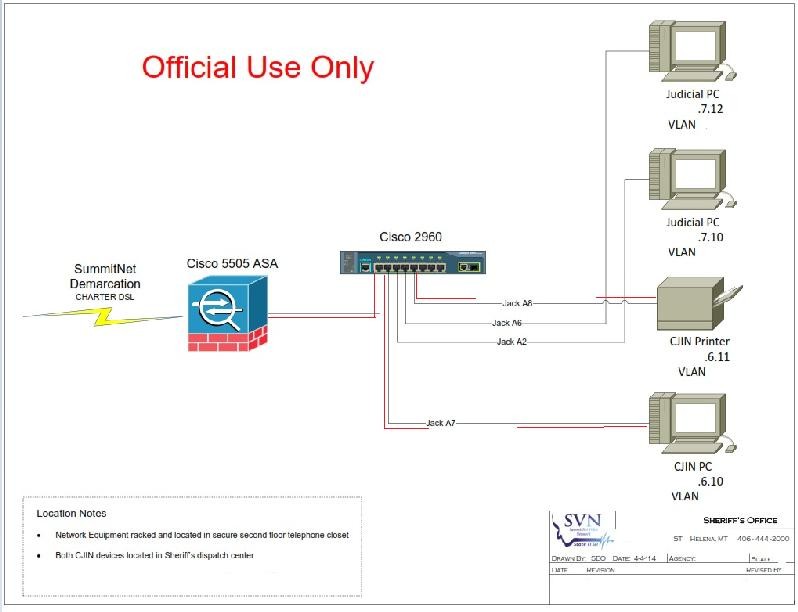
· “FOR OFFICIAL USE ONLY” markings.

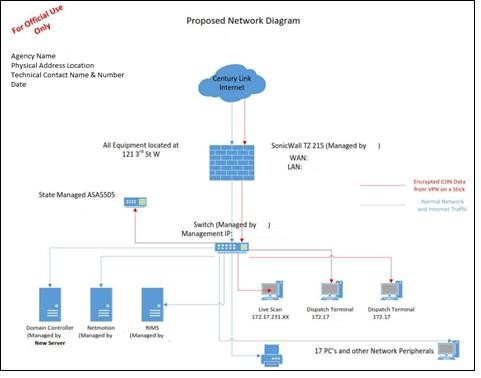
· Physical address of location and technical contact name and number for questions or emergencies.

· The agency name and date (day, month, and year) drawing was created or updated.

See additional examples here:

<http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view> Appendix C.





## Appendix D – router security

A router or firewall is typically the first line of defense to any network. Therefore, the security measures on these types of devices is most critical. Please answer the following questions about your router/firewall and how it is configured for the agency environment.

|  | CJIS requirements | Select if True |
| --- | --- | --- |
| 1 | Does the agency have a written router/firewall security policy? (This policy should contain such things as identifying who is allowed to log on, configure or update the router/firewall. Along with how auditing and logging management practices are handled.) |  |
| 2 | Does the agency back up your router/firewall configuration offline in a secure place in case of corruption/compromise on the router/firewall? |  |
| 4 | Does the agency implement access lists that allow **only** those protocols, ports and IP addresses that are required by your network users and services and that deny everything else? |  |
| 5 | Does the agency update your router/firewall with the latest security patches and firmware revisions as needed? |  |
| 6 | Does the agency test the security of your routers/firewalls regularly? Especially after any configuration changes or updates? |  |
| 7 | Are router user and passwords configured with complex passwords and restricted to limited technology personnel? |  |
| 8 | Is password encryption in use such as “enable secret” in order to secure administrative access? |  |
| 9 | Are access restrictions imposed on Console, Aux , VTY’s? |  |
| 10 | Are unneeded network servers and facilities disabled? |  |
| 11 | Are necessary network services configured correctly? (e.g. DNS) |  |
| 12 | Are unused interfaces and VTY’s shut down or disabled? |  |
| 13 | Are risky interface services disabled? |  |
| 14 | Are ports and protocols of the network identified and checked? |  |
| 15 | Do access lists block reserved and inappropriate addresses? |  |
| 16 | Are routing protocols configured to use integrity mechanisms? |  |
| 17 | Is logging enabled and log recipient hosts identified and configured? |  |
| 18 | Is the routers time of day set accurately and maintained with NTP? |  |
| 19 | Is logging set to include consistent time information? |  |
| 20 | Are logs checked, reviewed and archived in accordance with local policy or the CJIS Security Policy? |  |
| 21 | Is SNMP disabled?   * If SNMP is not disabled, is it enabled with good community strings and ACL’s? …………………………… |  |

## Appendix E – Signatures

**This certification page is an acknowledgement, by the local law enforcement agency, along with the vendor and its individual employees, that they have read and understand the requirements contained within this document. By signing this risk assessment, the local LEA and vendor are representing that the information is true and correct to the best of their knowledge and that the appropriate due diligence was considered during this review in order to minimize risks to the local LEA network and DOJ network.**

**Note that the responsibility for contractor compliance with the FBI requirements, and the enforcement thereof, resides with the criminal justice agency.**

Local Law Enforcement Official:

|  |  |
| --- | --- |
| Name: | Phone: |
| Signature: | Date: |
| Title: | Other: |

IT Staff Reviewing & Completing Form:

|  |  |
| --- | --- |
| Name: | Phone: |
| Signature: | Date: |
| Title: | Other: |

IT Vendor Reviewing & Completing Form:

|  |  |
| --- | --- |
| Name: | Phone: |
| Signature: | Date: |
| Title: | Other: |

DOJ Information Systems Security Officer:

|  |  |
| --- | --- |
| Name: | Phone: |
| Signature: | Date: |
| Title: | Other: |

CJIN or LIVESCAN Project Manager:

|  |  |
| --- | --- |
| Name: | Phone: |
| Signature: | Date: |
| Title: | Other: |