CJIS Security Audit

Cycle Two – 2013-2016

CJIS Security Policy Version 5.2 – V3

Auditor: Audit Date:

Agency Identification

Agency Name: ORI:

Street Address:

City: Zip Code:

Local Agency Security Officer

Name & Title:

Phone Number: Fax Number:

Email Address:

☐ LASO is same as TAC (If checked)

Terminal Agency Coordinator

Name & Title:

Phone Number: Fax Number:

Email Address:

5.1 MCA/Security Addendum

Do you have a Management Control Agreement for all non-law enforcement governmental support?

☐ IN ☐ OUT

Do you have a Security Addendum for all Vendors involved in CJI support or secure location access?

☐ IN ☐ OUT

5.2 Security Awareness

Have all personnel (Dispatchers, Law Enforcement, IT, Contractors) received Security Awareness training?

☐ IN ☐ OUT

5.3 Incident Response

Do you have a documented incident plan detailing incident handling, collection of evidence, incident response training, and incident monitoring to include contact names and numbers?

☐ IN ☐ OUT

5.4 Auditing and Accountability

5.4.1.1 Events

Are the following events logged and kept for a minimum of one year?

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

5.4.1.1.1 Content

Is the following content included with every audited event?

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event

☐ IN ☐ OUT

5.5 Access Control

Does the agency validate information system accounts at least annually and keep documentation?

☐ IN ☐ OUT

5.5.1 Account Management

Does the agency have a written policy for creating, activating, disabling and removing accounts with CJI access?

☐ IN ☐ OUT

5.5.3 Unsuccessful Login Attempts

Does the system which accesses CJI enforce a limit of no more than 5 consecutive invalid access attempts by a user, and does the system automatically lock the account/node for a 10 minute time period unless released by an administrator?

☐ IN ☐ OUT

5.5.4 System Use Notification

Does the system display an approved system use notification message before granting access informing potential users of various usages and monitoring rules?

☐ IN ☐ OUT

5.5.5 Session Lock

Does the information system accessing CJI prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures?

☐ IN ☐ OUT

5.5.6 Remote Access

Does the agency authorize, monitor, and control all methods of remote access to the information system by a user communicating temporarily through an external, non-agency-controlled network (e.g., the Internet)?

☐ IN ☐ OUT

5.5.6.1 & 5.5.6.2 Personally Owned Information Systems & Publicly Accessible Computers

Does the agency have a policy addressing personally owned or publicly accessible computers?

☐ IN ☐ OUT

5.5.7 Wireless Access Restrictions

Has the agency established written usage restrictions and implementation guidance for wireless technologies? (ex: BYOD policy or local SOP, MDM Policy)

☐ IN ☐ OUT

5.5.7.1 All 802.11x Wireless Protocols

Does the Agency maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices, and provide documentation of logging (if supported) and review on a recurring basis per local policy?

☐ IN ☐ OUT

5.5.7.3.1 Cellular Risk Mitigations

If agency utilizes cellular devices, are the following, minimum requirements being met?

Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in section 5.10.4.1.
Are configured for local device authentication.
Use advanced authentication.
Encrypt all CJI data resident on the device.
Erase cached information when session is terminated.
Employ personal firewalls or run a Mobile Device Management system that facilitates the ability to provide firewall services from the agency level.
Employ antivirus software or run a Mobile Device Management system that facilitates the ability to provide antivirus services from the agency level.

☐ IN ☐ OUT

5.5.7.3.3 Mobile Device Management (MDM)

If the agency allows CJI access from cell / smart phones and tablet devices that do not support firewalls or Antivirus the agency must utilize an MDM with centralized administration capable of at least:

☐ Remote locking of device
Remote wiping of device
Setting and locking device configuration
Detection of "rooted" and / or "jailbroken" devices
Enforce folder and / or disk level encryption

If applicable, please describe.

☐ IN ☐ OUT

5.6.1 User ID's

Have all users been issued their own login ID and there is no sharing of ID's allowed?

☐ IN ☐ OUT

5.6.2.1.1 Standard Authenticators

What are the requirements for passwords used at the agency?

☐ IN ☐ OUT

5.6.2.2 (A) Advanced Authentication for Laptops:

Is Advanced Authentication in use?

☐ YES ☐ NO

If not in use for laptop devices is a locking device or policy in place to ensure only access from a secure location?

☐ YES ☐ NO

Describe methods being deployed if applicable.

☐ IN ☐ OUT

5.6.2.2 (B) Advanced Authentication for Smart Phones / Tablet Devices:

Is Advanced Authentication in use?

☐ YES ☐ NO

If MDM is in place, select which of the compensating controls are in use (at least 4 required):

Possession of the agency issued smart phone as an indication it's the authorized user

☐ YES ☐ NO

Password protection on the Mobile Device Management application

☐ YES ☐ NO

Enable remote device locking

☐ YES ☐ NO

Enable remote data deletion

☐ YES ☐ NO

Enable automatic data wipe after predetermined number of failed authentication attempts

☐ YES ☐ NO

Remote device location (GPS) tracking

☐ YES ☐ NO

Require CJIS Security Policy compliant password to access the device

☐ YES ☐ NO

Use of device certificates

☐ YES ☐ NO

.

Describe methods being deployed if applicable.

☐ IN ☐ OUT

5.7 Network Diagram

Does the agency have a current Network Diagram?

☐ IN ☐ OUT

5.8 Media Protection

Does the Agency store any CJI outside of the Secure Location? Is the CJI encrypted?

☐ IN ☐ OUT

5.8.3 Electronic Media Sanitization and Disposal

Please provide the formal written procedures the agency has for the secure disposal or destruction of electronic media, and if these procedures are witnessed or carried out by authorized personnel.

☐ IN ☐ OUT

5.8.4 Disposal of Physical Media

Please provide the formal written procedures the agency has for the secure disposal or destruction of physical media, and if these procedures are witnessed or carried out by authorized personnel.

☐ IN ☐ OUT

5.9 Physical Protection

The agency's facility, area, room, or group of rooms shall have physical and personnel security controls sufficient to protect CJI. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

☐ Does the agency keep a list of personnel with authorized access ?
Does the agency control physical access to information system distribution and transmission lines within the physically secure location?
Does the agency control physical access to information system devices that display CJI and position information system devices in such a way to prevent unauthorized individuals from accessing and viewing CJI?
Does the agency control information system-related items entering and exiting the physically secure location?

If the agency cannot meet all the controls required for establishing a physically secure location, does the agency meet at a minimum:

☐ Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency?
Lock the area, room, or storage container when unattended?
Position information system devices and documents containing CJI in such a way as to prevent unauthorized access or viewing?
Follow the encryption requirements found in section 5.10.1.2 for electronic storage of CJI?

☐ IN ☐ OUT

5.10 System and Communications Protection and Information Integrity

Does the agency encrypt all CJI data before it leaves the secure location? Do you have the FIPS certificate?

☐ IN ☐ OUT

5.10.1.1 Boundary Protection

Does the agency have a boundary protection device (firewall) implemented to protect computers and access devices from non-CJI networks including Internet access?

☐ IN ☐ OUT

5.10.1.1 Network Monitoring

List the tools and describe techniques to monitor network events, detect attacks, and provide identification of unauthorized use.

____ IN ____OUT

5.10.1.1, 5.10.1.2 CJI Segmentation

How is the criminal justice agency segmented from other non criminal justice agency's networks?

____ IN ____OUT

5.10.1.4 VOIP

Is Voice over IP (VoIP) services segmented from data traffic?

____ IN ____OUT

5.10.1.5 Cloud Computing

Who provides Cloud Computing services for the agency and does the vendor meet all CJIS Security requirements? Does the contract prohibit scanning any email or data files for the purpose of data mining, advertising, etc ?

____ IN ____OUT

5.10.3.2 Virtual Environment

If the agency maintains CJI in a virtual environment, what controls are implemented?

☐ IN ☐ OUT

5.10.4.1 Security Updates

When were the last Windows updates applied? When was the last update for interfaced software?

NOTE: Do not update the Java version on functional systems as this could impair Omnixx functionality.

☐ IN ☐ OUT

5.10.4.2 & 5.10.4.3 Antivirus

Are all IT systems (workstations, servers, mobile computing devices, and critical information system entry points, including terminals and MDTs without Internet access) with CJIS connectivity protected with anti-virus, anti-spam and spyware protection? Are automatic updates enabled on all systems that have Internet access or please describe the update process?

☐ IN ☐ OUT

5.10.4.4 Laptop Firewalls

Are personal/software based firewalls enabled on all wireless laptop devices and do they meet current CJIS Security Policy requirements?

☐ IN ☐ OUT

5.10.4.5 Security Alerts

Does the agency receive Security Alerts and Advisories? From what organization(s)?

☐ IN ☐ OUT

5.12 Personnel Security

All Personnel who access CJIS Data either physically, logically, or remotely must be fingerprint based background checked. Has this been completed for everyone?

☐ IN ☐ OUT