CJIS Security Audit

CJIS Security Policy Version 5.5

This is a sample and subject to change without notice.

Auditor: Staff Select

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 ☐ NA ☐

NOTES

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

IN ☐ OUT ☐ NA ☐

NOTES

5.2 Security Awareness*

Have all personnel (Dispatchers, Law Enforcement, IT, Contractors) received Security Awareness training? Describe methods used, (ie; Omnixx Trainer, CJIS Online, PDF,etc.) provide documentation.

(Discuss new level guidelines and topics for Level One, Two, Three, and Four as baselines.)

IN ☐ OUT ☐ NA ☐

NOTES

5.3 Incident Response*

Provide a documented incident plan detailing incident handling, collection of evidence, incident response training, and incident monitoring. (Ensure DPS OIC contact information is included.)

IN ☐ OUT ☐ NA ☐

NOTES

5.4 Auditing and Accountability

5.4.1.1 Events

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

- Successful and unsuccessful system log-on attempts.
- Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
- Successful and unsuccessful attempts to change account passwords.
- Successful and unsuccessful actions by privileged accounts.
- 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?

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

IN ☐ OUT ☐ NA ☐

NOTES

5.5 Access Control

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

IN ☐ OUT ☐ NA ☐

NOTES

5.5.1 Account Management*

Provide a documented process for creating, activating, disabling and removing accounts with CJI access.

IN ☐ OUT ☐ NA ☐

NOTES

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 ☐ NA ☐

NOTES

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 ☐ NA ☐

NOTES

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?

Note Exemptions; MDTs (Patrol Vehicles), Dispatch, and Receive Only Terminals (ROT).

IN ☐ OUT ☐ NA ☐

NOTES

5.5.6 Remote Access

Explain the agencies process for allowing remote support: agency personnel, IT support, vendors. Does the agency authorize, monitor, and control all methods of remote access to the information system to include Virtual Escorting?

IN ☐ OUT ☐ NA ☐

NOTES

Are encryption requirements met for connection(s) outside of secure location? Provide details and FIPS certificates (Numbers).*

IN ☐ OUT ☐ NA ☐

NOTES

Are AA (Advanced Authentication) requirements met for connection(s) outside of secure location? Provide details.

IN ☐ OUT ☐ NA ☐

NOTES

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 ☐ NA ☐

NOTES

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 ☐ NA ☐

NOTES

5.6.2.1.1 Standard Authenticators

Do passwords (and PINs, if applicable) meet CJIS Policy requirements?

IN ☐ OUT ☐ NA ☐

NOTES

5.6.2.2 Advanced Authentication

A. BYOD (Bring Your Own Device)

Is agency using BYOD devices; Smart Phones, Tablets, Etc. to process CJI data?
Provide details below:

If YES to above, AA is required.

IN ☐ OUT ☐ NA ☐

NOTES

B. Laptop

Is agency using Laptop devices to process CJI data?
Describe methods and policy agency has in place to meet requirements:

(If YES to above, AND no AA in place, devices must be limited to secure area(s) ONLY.)

IN ☐ OUT ☐ NA ☐

NOTES

C. Tablets / Smart Phones

Is agency using Tablet devices or Smart Phones to process CJI data?
Provide details below:

If YES to above, and AA is not present, devices must be controlled via MDM (Mobile Device Management), be agency issued, and have documented AA compensating control according to TX Security Policy Supplement. (Email to security.committee@dps.texas.gov).

IN ☐ OUT ☐ NA ☐

NOTES

5.7.1.2 Network Diagram*

Does the agency have a current Network Diagram which lists all communication paths, circuits, and relevant components and include “For Official Use Only”, Agency name and date?

IN ☐ OUT ☐ NA ☐

NOTES

5.8.1 Media Storage and Access

Does the Agency store any CJI outside of the Secure Location?
If YES to above, but data does not meet FIPS 140-2 encryption requirement, is the data encrypted AT REST to meet FIPS 197 certified, 256 bit as described on the National Security Agency (NSA) Suite B Cryptographic list of algorithms?

IN ☐ OUT ☐ NA ☐

NOTES

5.8.3 Digital 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 ☐ NA ☐

NOTES

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 ☐ NA ☐

NOTES

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.

Physically Secure Location:

- 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:

Controlled Area:

- 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 ☐ NA ☐

NOTES

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 ☐ NA ☐

NOTES

5.10.1.2 Encryption*

Does the agency encrypt all CJI data to meet FIPS 140-2 standards before it leaves the secure location? Provide Relevant Certificate numbers below:

IN ☐ OUT ☐ NA ☐

NOTES

Is CJI data segmented from other non-criminal justice agency's networks/data? Describe methods below:

IN ☐ OUT ☐ NA ☐

NOTES

5.10.1.5 Cloud Computing

Does agency utilize cloud services or ensure that all data is encrypted prior to being transmitted outside of secure area(s)?
If applicable, view the Security Addendum to ensure all security requirements are met; to include prohibiting scanning any email or data files for the purpose of data mining, advertising, etc.

IN ☐ OUT ☐ NA ☐

NOTES

5.10.2 Facsimile Transmission of CJI

Faxing over a standard telephone line is exempt from encryption requirements. Use of a server, application or email-like technology must meet encryption requirements as defined in Section 5.10. Describe the agencies use (if applicable) of fax services below. Does agency meet encryption requirements?

IN ☐ OUT ☐ NA ☐

NOTES

5.10.3 Partitioning and Virtualization

Partitioning 5.10.3.1
Are applications, services, or information services physically or logically separate? Separation may be accomplished through the use of one or more of the following:

- Different Computers
- Different Central Processing Units
- Different instances of the operating system
- Different network addresses
- Other methods approved by the FBI CJIS ISO

Virtualization 5.10.3.2
Are virtualized environments secured with the following additional controls in place?
Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.

- Maintain audit logs for all virtual machines and hosts and store the logs outside the host's virtual environment.
- Virtual machines which are internet facing (web servers, portal servers, etc.) shall be physically separate from virtual machines (VM) that process CJI internally or be separated by a virtual firewall.
- Drivers which serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.
- Additional Technical Security controls which MAY be implemented include:
- Encrypt CJI when in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
- Encrypt network traffic within the virtual environment.
- Implement IDS and/or IPS monitoring within the virtual environment.
- Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
- Segregate the administrative duties for the host.

IN ☐ OUT ☐ NA ☐

NOTES

5.10.4.1 Security Updates

Describe the agencies computer update processes. When were the last Windows updates applied? When was the last update for CAD/RMS (Version)?

IN ☐ OUT ☐ NA ☐

NOTES

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 ☐ NA ☐

NOTES

5.10.4.5 Security Alerts

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

IN ☐ OUT ☐ NA ☐

NOTES

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 ☐ NA ☐

NOTES

5.12.2 Personnel Termination and 5.12.3 Personnel Transfer

Are assignment changes updated within a timely manner and accounts disabled to meet CJIS Policy requirements?

IN ☐ OUT ☐ NA ☐

NOTES

5.12.4 Personnel Sanctions

Does the agency have a formal sanctions process for personnel failing to comply with established information security policies and procedures?

IN ☐ OUT ☐ NA ☐

NOTES

5.13 Mobile Devices*

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

IN ☐ OUT ☐ NA ☐

NOTES

5.13.1.1 All 802.XX Wireless Protocols

Does the agency maintain a complete inventory of all Access Points (Aps) and 802.XX wireless devices, and provide documentation of logging (if supported) and review on a recurring basis per local policy?
(Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA) cryptographic algorithms, used by all PRE-802.11i protocols, DO NOT meet the requirements for FIPS 140-2 and SHALL NOT be used.)

IN ☐ OUT ☐ NA ☐

NOTES

5.13.1.4 Mobile Hotspots

If agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot for connection, are they limited to agency controlled devices ONLY?

IN ☐ OUT ☐ NA ☐

NOTES

5.13.2 Mobile Device Management (MDM)

If Mobile Device Management (MDM) is in use, does it meet at least the following compensating controls:

- Remote locking of device
- Remote wiping of device
- Setting and locking device configuration
- Detection of “rooted” or “jailbroken” devices
- Enforce folder and/or disk level encryption
- Application of mandatory policy settings on the device
- Detection of unauthorized configurations or software/applications
- Ability to determine the location of agency controlled devices
- Prevention of unpatched devices from accessing CJI or CJI systems
- Automatic device wiping after a specified number of failed attempts

IN ☐ OUT ☐ NA ☐

NOTES

5.13.4.3 Personal Firewall

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

IN ☐ OUT ☐ NA ☐

NOTES

5.13.5 Incident Response (Mobile Devices)

In addition to the requirements in Section 5.3 Incident Response, agencies are responsible to meet additional reporting and handling procedures. Has the agency developed a written plan which includes the items listed below in the event of:

Loss of device control:

- Device known to be locked, minimal duration of loss
- Device lock state unknown, minimal duration of loss
- Device lock state unknown, extended duration of loss
- Device known to be unlocked, more than momentary duration of loss

Total Loss of device:

- CJI stored on device
- Lock state of device
- Capabilities for remote tracking or wiping of device
- Device compromise
- Device loss or compromise outside of United States

IN ☐ OUT ☐ NA ☐

NOTES

5.13.7.2.1 Compensating Controls for Advanced Authentication*

If Mobile Device Management (MDM) is in use, does it meet at least four of the following compensating controls: (NOTE: Compensating controls is not an option for mobile devices when deployed via a BYOD policy).

- Possession of the agency issued smartphone or tablet as an indication it is the authorized user
- Implemented password protection on the Mobile Device Management application and/or secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after predetermined number of failed authentication attempts
- Remote device location (GPS) tracking
- Require CJIS Security Policy compliant password to access the device
- Use of device certificates as per Section 5.13.7.3 Device Certificates

IN ☐ OUT ☐ NA ☐

NOTES

(* indicates documentation is required from agency)