Criminal Justice Information Technical Audit Preparation Guide

The objective of the FDLE CJIS technical audit to verify compliance to the polices and regulations of the Florida Crime Information Center (FCIC)/National Crime Information Center (NCIC), adherence to the FDLE Non-Criminal Justice User Agreement (NCJUA) as well as the FBI CJIS Security Policy, and to state and federal laws and administrative codes. The technical audits are conducted every three (3) years, or when necessary to ensure compliance standards are met. The audit consists of a questionnaire utilized to gain insight regarding the agency's network and systems and how it handles criminal justice information (CJI). The auditor will contact the agency contact person (LASO) to set up the on-site visit. The LASO, in return, may solicit other agency personnel to provide a cohesive audit response, such as IT personnel and/or other agency personnel familiar with the agency's information systems, policies, and procedures. The auditor will discuss the agency's process of criminal justice information (CJI) to determine the agency's security requirements and remedies. The following depicts, but is not limited to, what will be discussed as well as the type of documents that will be requested at the time of the on-site agency visit.

Documents that maybe requested during the On-site Visit:

- ☐ **Information Exchange Agreements** between the agency and other NCJA's that the agency receives or shares information, databases, services, etc. with.
- ☐ **Vendor/Contractor Contract/Agreement** (if applicable) between the agency and private contractor. This should include all vendors (CJI System, Fiber vendor, VoIP vendor, 911 Phones, etc.)
- ☐ **Security Addendums** (if applicable) between the agency and private contractor personnel
- ☐ **Spreadsheet of all Private Contractor Personnel with physical or logical access to the network**
- ☐ **Security Awareness Training List and Materials**
- ☐ **Spreadsheet or Documentation of User Account Verification**
- ☐ **Network Diagram** – High-level diagram that shows all forms of FBI CJIS data systems access [including wireless, dial-up, etc.] by system users and/or IT personnel.
- ☐ **Encryption Certificates** – see the NIST certificates section below regarding how to obtain these certificates
- ☐ **Agency Required Policies (see required policy checklist)**

ON-SITE VISIT TO THE AGENCY

LOCAL AGENCY SECURITY OFFICER - CSP 3.2.9

- The agency identified LASO should provide nexTEST certificate showing completion of LASO training to the FDLE auditor during the on-site visit.

- The LASO should verify that all personnel with access to criminal justice information/applications/systems/network have the proper personnel screening and security awareness training. This includes all agency personnel, IT personnel, and vendor personnel.

INFORMATION EXCHANGE AGREEMENTS / MCA's – CSP 5.1

- At the time of the audit, the agency should provide copies of interagency agreements between criminal justice agencies that outline the process of sharing, sending or receiving criminal justice information. The agreement should also indicate whether access is provided to either agency regarding the use of criminal justice information systems and services.

- At the time of the audit, the agency should provide copies of any management control agreements with non-criminal justice agencies that outline the scope of the relationship between the agencies. This should include any city or county IT support. The agreement should indicate that the control of the criminal justice function remains with the criminal justice agency. The agency should also provide proof of state and national fingerprint-based record checks, and appropriate level of security awareness training for governmental IT staff that may access the criminal justice information data or systems.

SECURITY ADDENDUM PROCESS – CSP 3.2.7 and 5.1.1.5, 5.12.1.2

- At the time of the audit, the agency should provide copies of any agreements with vendors and contractors. The agreement should indicate the purpose of the relationship, the scope of the exchange of services that authorize access to criminal justice information and limits the use of criminal justice information. The contract or agreement must identify access control (physical, logical or virtual) to the agency's information systems, applications, or servers and incorporate the FBI CSP Security Addendum. In addition, the agency should also provide proof of state and national fingerprint-based record checks, appropriate level of security awareness training, and signed security addendums for all vendor/contractor personnel that have access the criminal justice information data or systems.

- At the time of the audit, the agency should provide agreements which incorporate the CJIS Security Addendum, with all vendors (such as: IT Support, RMS, JMS, CAD Provider, Cable Company, Internet Company, Inmate Healthcare System Vendor, Dispatch Phone Provider, VoIP Provider, Commissary Vendor, Offsite Storage Vendor, Shredding Company, etc).

- The agency should provide a verification sheet to the auditor that shows the agency is maintaining up-to-date records of Contractor/Vendor employees who access the system, including name, date of birth, social security number, date fingerprinted/fingerprint cards submitted, date security clearance issued, and date initially trained, tested, certified, or recertified.

PERSONNEL SECURITY AND SECURITY AWARENESS TRAINING – CSP 5.2

- The auditor will review the retained print list report and verify that the prints on file are current and up-to-date.

- Security awareness training documentation (CJIS ONLINE or CJIS Certification) for all personnel with a criminal justice function that may access CJI (includes agency, city, county, or external vendor IT staff).

CRIMINAL JUSTICE INFORMATION (CJI) SYSTEMS AND ACCESS CONTROL – CSP 5.4

- The agency will provide a list of applications, services, and systems used to access, process, or store criminal justice information.

- The auditor will discuss and verify that the agency is utilizing an auditing tool that captures previously defined events and that the agency periodically reviews and updates the list of these events.

- The auditor will verify how the agency audits the information when there is an increased risk to agency operations, assets or risk to individuals.

- The auditor will verify the length of time the agency retains the audit logs. **(This section pertains to CJI systems: eAgent, SmartCop, New World, Spillman, Sungard, Elvis, TraCS, etc…)**

ACCESS CONTROL - CSP 5.5

- The auditor will verify documentation and management of access control accounts to information systems, applications and logs of access privilege changes. The auditor will verify how the agency controls access to the systems and the information.

- The auditor will verify that a system use notification message is enabled on all agency terminals and that it meets the minimum requirements of the CSP.

- The auditor will verify that a session lock is enabled on all agency terminals and verify the actions taken for the user to re-establish connection.

- The auditor will discuss how the agency utilizes remote access for access to agency systems and applications.

- In addition, the agency will need to provide the appropriate encryption certificates for secure remote access and verify that remote access is monitored and controlled by authorized agency personnel.

- The auditor will discuss the use of personally owned devices within a network containing CJI as well as publically accessible computers.

IDENTIFICATION AND AUTHENTICATION – CSP 5.6

- The auditor will discuss and verify that the agency is using secure and stringent password attributes to all systems and applications that store, process and access criminal justice information. At a minimum, the agency's password policy must meet the requirements of the CSP and the FDLE CJUA. **(Passwords for Windows Domain as well as each CJI system the agency accesses, advanced authentication, system use notification on all computers and session lock settings)**

- If the agency utilizes Personal Identification Numbers (PIN) or One-Time Passwords (OTP), the audit will review the setup of the passwords and verify that the agency is adhering to the CJIS Security Policy.

- The auditor will determine if the agency has the ability to query from mobile devices and ensure that if they do, Advanced Authentication is being utilized on the device.

CONFIGURATION MANAGEMENT (Agency Network Diagram) – CSP 5.7
The agency's network diagram should contain the following:

- Agency name and ORI number
- Date the diagram was created or updated
- "For Official Use Only" (FOUO) marking
- Annotation of the number of workstations, mobile devices, and clients on the network
- Complete and current system configuration that depicts the agency's interconnectivity to CJI systems and/or services
- Includes all communication paths, circuits and components beginning with the agency and traversing through all systems to the agency end-point
- Location of all components (firewalls, routers, switches, hubs, servers, encryption type/bit level and workstations).

MEDIA (ELECTRONIC AND PHYSICAL) PROTECTION – CSP 5.8

- The auditor will discuss and verify how the agency protects criminal justice information from unintentional viewing
- How the agency transports physical and electronic media
- How the agency securely disposes of physical and electronic media and hardware(includes leased devices)
- How the agency oversees the disposal and who at the agency level witnesses the destruction
- If the agency utilizes an outside agency to dispose of the media, the agency will need to provide an agreement with the agency to the auditor as well as fingerprint based records check and security awareness training for all employees of the agency that may have access to the criminal justice information.

PHYSICAL PROTECTION – CSP 5.9

- The auditor will confirm site security, physical and logical access to CJI, and verification of appropriate signage to network or server rooms, dispatch areas, or other areas as well as the location of CJNet / FCIC / FDLE equipment / router, CJI systems, servers.

SYSTEM AND COMMUNICATIONS PROTECTION AND INFORMATION INTEGRITY – CSP 5.10

- The auditor will discuss the type of network the agency is utilizing and the type of protection that is used for criminal justice information at rest or in transit. **(Show connections to other agencies via MDT's or shared resources)**
- The auditor will discuss network security to include boundary protection tools, firewalls, security alerts and advisories as well as the steps the agency takes during a network security event. **(Looking for types of intrusion detection, spyware, spam ware, virus protection).**
- The auditor will discuss and verify that the agency is utilizing encryption on all criminal justice information data that is stored at rest outside the boundary of the secure location, the data that is transmitted outside the secure location as well as encryption on all mobile device terminals.
- At the time of the audit, the agency will provide to the auditor copies of FIPS certificates for all encryption mechanisms being utilized by the agency. **(Need FIPS 140-2 certificates for all encryption – VPN, Firewalls, Back-up Storage, transmission, at rest)**
- The auditor will discuss if the agency is utilizing a cloud service provider for the storage of CJI and the requirements.
- The auditor will discuss any virtual machines that the agency is using to store or process criminal justice information. This will include any servers that are onsite at the agency or that are housed offsite. The process will identify how the information is stored, protected and kept separate from all non-criminal justice information. **(how VM's are set up, if they co-mingle CJI and non-CJI information, if they are partitioned or physically separate)**

MOBILE DEVICES – CSP 5.13

- The auditor will discuss wireless and cellular technology as it pertains to how the agency stores, accesses, processes and protects criminal justice information/systems utilizing wireless technology. This will include mobile devices, air cards, Mi-Fi boxes, agency wireless networks, etc. The auditor will also address the protection of the device include encryption certificates, advanced authentication, firewalls and boundary protection tools. **(MDT connection and wireless connection of computers within the agency)**

- LIMITED FEATURE OPERATING SYSTEMS (OS) (Ex: Android, IOS, Windows Tablets, Smart Phones, etc.) The auditor will discuss the agency's use of limited operating systems (tablets, smart phones, etc.) and how they are utilized in conjunction with criminal justice information, systems and applications. The agency will need to provide the type of mobile device management solution used to protect the devices.