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**
- ☐ **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 for the access or storage of CJI. The agreement should indicate the purpose of the relationship, the scope of the exchange of services that authorize access and limits the use of CJI. The contract or agreement must identify access control to the agency's physical media containing CJI 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 to the CJI.

- At the time of the audit, the agency should provide agreements which incorporate the CJIS Security Addendum, with all vendors (such as: a company that offers CJI storage resources).

- 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).

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.