

## **Information Technology Security Audit**

### **Audit Categories**

**Criminal Justice Audit** – an audit of a criminal justice agency’s access, use, storage, and destruction of any criminal justice information (CJI) received from FBI Criminal Justice Information Services (CJIS) Division systems via both direct and indirect access methods. These audits include both name-based and fingerprint-based queries over wired or wireless networks.

**Non-criminal Justice Audit** – an audit of a non-criminal justice agency’s access, use, storage, and destruction of any CJI received from FBI CJIS systems via direct and indirect access methods. These audits include both name-based and fingerprint-based queries over wired or wireless networks.

**Outsourcing/Channeling Audit** – an audit of an FBI approved contractor who submits fingerprints on behalf of an authorized recipient to the FBI and receives the results of such a submission for dissemination back to the authorized recipient. The scope of channeler audits focuses mainly on the storage, dissemination, and destruction of criminal history record information (CHRI).

These audits are comprised of an administrative interview to review administrative and technical controls implemented to protect CJI from both a physical and logical perspective. Additionally, most audits include a physical security and network inspection in which controls identified in the administrative interview are verified to be implemented and working correctly.

### **Audit Objective(s)/Scope**

The purpose of the audit is to assess the user community’s compliance with the FBI *CJIS Security Policy* requirements as approved by the Advisory Policy Board (APB) and National Crime Prevention and Privacy Compact (Compact) Council. The FBI *CJIS Security Policy* provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

The FBI *CJIS Security Policy* applies to all entities with access to, or who operate in support of, FBI CJIS Division’s services and information. The FBI *CJIS Security Policy* provides the minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, and/or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for non-criminal justice purposes are also governed by the standards and rules promulgated by the Compact Council to include the Outsourcing Standard for Channelers.

## **Overview of the Process**

### **Pre-audit Methodology**

Prior to the on-site audits, the CJIS Audit Unit (CAU) auditors contact the CJIS Systems Officer (CSO) or Information Security Officer (ISO) and local agency representatives to schedule the audit date and to give an overview of the audit process. They also gather basic audit information and discuss pre-audit responsibilities.

The CSA pre-audit questionnaire is used to assist the audit manager in gathering pertinent information prior to the on-site visit. Information gathered from the pre-audit questionnaire is used to formulate additional questions to be answered during the on-site visit and to assist in determining policy compliance. Additionally, the pre-audit questionnaire is used as a tool by audit managers to prepare information sheets for local auditors, outlining/summarizing the CSAs audit program and procedures.

The local pre-audit packet is used to assist local auditors in determining the agency's compliance with FBI *CJIS Security Policy* policies and procedures. This information is mailed prior to the audit and reviewed during the on-site visit.

### **Assessment**

During the CSA visit, the audit manager interviews the CSO/ISO and CSA personnel to determine the CSA's adherence to FBI *CJIS Security Policy* policies and procedures.

During local audits, auditors conduct interviews with local agency representatives to determine the agency's adherence to FBI *CJIS Security Policy* policies and procedures. Additionally, an on-site network inspection is conducted. Upon completion of the on-site interviews and network inspections, auditors determine compliance with FBI *CJIS Security Policy* policies and procedures.

After all interviews and network inspection assessments are completed, exit interviews with the CSO/ISO and local agency representatives are conducted to inform them of compliance issues and copies of the results are disseminated.

### **Post-audit**

After the audit, a draft FBI ITS Audit report is forwarded to the CSO/ISO for review and comment. The report includes findings from the interviews with the agency personnel, the network inspections, and required actions for agency compliance.

CSO/ISO's are requested to review the draft report and respond to required actions, if any, by indicating corrective actions.

The CSO/ISO's responses are appended to the report. Once the response is added to the report, a final report is prepared and sent to the CSO/ISO.

The CAU provides the Executive Summary of the final report, which includes the CSO's response to the recommendations, to the CJIS APB's Compliance Evaluation Subcommittee (CES) for review and appropriate action. The CES will continue to monitor the corrective actions until appropriate remedial action has been taken.