DOJ OCIO LESIS

Department of Justice | Office of the Chief Information Officer | Law Enforcement Services & Information Sharing

Department of Justice
Criminal Justice Information Network

Audit Policy

(Interim)

May 1, 2019

Law Enforcement Services & Information Sharing Office
Two Constitution Square (2CON)
145 N Street NE
Washington, DC 20002

Table of Contents

DOJ OCIO LESIS

Department of Justice | Office of the Chief Information Officer | Law Enforcement Services & Information Sharing

Section 1. Introduction

The Law Enforcement Services and Information Sharing (LESIS) Office of the United States Department of Justice (DOJ) Chief Information Officer (CIO) serves as the FBI Criminal Justice Information Services (CJIS) Systems Agency (CSA) for DOJ, as well as other Federal and Tribal agencies and entities. The DOJ CSA is responsible for establishing and administering an information and information technology security program across its User Agencies. A User Agency is the entity legally authorized by FBI CJIS to submit to or receive information from FBI CJIS systems, either as a Criminal Justice Agency (CJA) or a Non-Criminal Justice Agency (NCJA). The DOJ CSA provides its User Agencies access to the following national crime information systems through a mechanism referred to as the DOJ Criminal Justice Information Network (CJIN):

- National Crime Information Center (NCIC) and Interstate Identification Index (III)
- Next Generation Identification (NGI)
- National Instant Criminal Background Check System (NICS)
- National Data Exchange (N-DEx)
- International Justice and Public Safety Network (Nlets)

1.1 Purpose of the Policy

The purpose of the DOJ CJIN Audit Policy (hereinafter "Audit Policy") is to establish the DOJ CSA audit principles, processes, and procedures for verification of User Agency and individual user compliance with the following:

- Applicable laws, regulations, and requirements of the FBI CJIS Security Policy, all related FBI CJIS system-specific manuals, and the Nlets User Policy Manual
- Directives and decisions of the criminal justice community's Advisory Policy Board (APB), National Crime Prevention, and Privacy Compact Council
- All relevant DOJ-specific policies, orders, and regulations

The DOJ CJIN Audit Policy will:

- Maximize the value of FBI CJIS information to User Agencies by providing best use practices
- Leverage best business practices and technology to reduce the administrative cost of compliance activities
- Lower User Agency risk of inappropriate system use and handling of CJI
- Prepare User Agencies for potential FBI CJIS Audits, which are conducted of the DOJ CSA and its User Agencies; the FBI CJIS audit of the CSA consists of reviewing the CSA's CJI policies, procedures, practices, and data, as well as selecting a sample of User Agencies it has audited for compliance

1.2 Roles and Responsibilities

The following table sets out the various roles and responsibilities for the DOJ CSA Audit:

Role	Responsibilities
DOJ CJIS Systems Officer (CSO)	• Administers the triennial Audit • Provides the User Agency with the official DOJ CSA Audit Findings and Ratings Report • Reviews and approves the User Agency Corrective Action Plan
DOJ CSA Auditor (hereinafter "Auditor")	• Serves as the Audit point-of-contact for the User Agency • Assists and guides the User Agency in all phases of the Audit • Provides the User Agency all documentation necessary to complete the Audit • Performs the Onsite Verification • Reviews and assesses the User Agency and individual user compliance with all requirements
Terminal Agency Coordinator (TAC)	• Serves as the User Agency point-of-contact for the Audit • Supports and facilitates the Audit, including any Onsite Verification activities • Completes all DOJ CSA Audit-related documentation, and provides supporting evidence • Reviews and responds to the DOJ CSA Audit Report, including preparing a User Agency Corrective Action Plan if required

Training materials pertaining to the Audit and the responsibilities of the TAC are available on the DOJ CJIN Training and Learning Center.

Section 2. DOJ CSA Audit Policy

The DOJ CSA is responsible to ensure User Agency and individual user adherence to applicable statutes, regulations, and policies, as they pertain to the use of and access to CJI and Criminal History Record Information (CHRI) through DOJ CJIN. As previously noted, a User Agency is the entity legally authorized by FBI CJIS to submit to or receive information from FBI CJIS systems, either as a Criminal Justice Agency (CJA) or a Non-Criminal Justice Agency (NCJA). To verify User Agency and individual user compliance, the DOJ CSA will audit all User Agencies at least once every three years for the data and services to which the DOJ CSA authorizes access. The Audit consists of an Online Phase and a potential Onsite Verification Phase, a review of supporting evidence, and production of a DOJ CSA Audit Findings and Ratings Report. If there are findings of non-compliance, the User Agency must enact a User Agency Corrective Action Plan, completely addressing all issues.

Section 3. DOJ CSA Audit Policy Principles

3.1 Audit Data and Services

The DOJ CSA evaluates the following data and services-associated compliance areas during the audit:

Data and Services	Compliance Areas
National Crime Information Center (NCIC) – An information system which stores CJI concerning property and persons that can be queried and managed by appropriate Federal, Tribal, state, and local law enforcement and other CJAs, as well as limited types of NCJAs; this includes criminal history information accessible through both III and Nlets	• System Administration • Training • Record Validation • Hit Confirmation • Record Integrity • Secondary Dissemination • Interstate Identification Index (III) • Protection Order File • Wanted Person File • Missing Person File • Nlets
National Instant Criminal Background Check System (NICS) – A system utilized by CJAs in connection with the issuance of a firearm-related permit or license, and the disposing of firearms in the possession of a CJA, and by limited types of NCJAs for the purpose of entering information on prohibited persons	• Purpose Code Usage • Federal Denial Criteria • NICS Indices Submission Requirements • Training
National Data Exchange (N-DEx) - A national investigative information sharing system that provides investigators criminal justice data from state, local, Tribal, regional, and Federal agencies	• System Administration • System Usage • Training • Logging
National Identity Services (NIS) – An audit program that assesses compliance with III and National Fingerprint File (NFF) participation standards, Federal laws and regulations associated with the use, dissemination, and security of national CHRI, and National Crime Prevention and Private Compact rules and procedures	• Use and Dissemination of CHRI • Purpose for Disclosure of CHRI • Applicant Notification and Record Challenge • Training
National Sex Offender Registry (NSOR) – An NCIC file that contains records on individuals, who are required to register in a jurisdiction's sex offender registry	• Record Integrity, Maintenance, and Validation • Training
Justice Automated Booking System (JABS) – A system used for the query and electronic submission of biographic and biometric data for offender identity verification, criminal history record management (i.e. Identity History Summary, also known as the Rap Sheet), and sex offender registration	• System Administration • Use and Dissemination of CHRI • Training

Information Technology (IT) – A User Agency's technical environment that manages the controls within the information system infrastructure, which includes the safeguarding of assets, maintaining data integrity, and operating effectively to policies, and operations	CJAs • Authorized Access, Use, Retention, and Dissemination of CJI • System Administration • Administration of Criminal Justice Functions • Information Protection • Network Infrastructure • Training	NCJAs • Authorized Access, Use, Retention, and Dissemination of CJI • System Administration • Administration of Non-Criminal Justice Functions • Information Protection • Network Infrastructure • Training

3.2 Audit Methodology

The DOJ CSA takes a systems- and risk-based approach in conducting its audits. This approach seeks to identify risks in system use and User Agency data management to ensure CJI and CHRI reliability, confidentiality, completeness, and accuracy. To properly identify potential risks in data and services, the Audit occurs in two phases: the Online Phase and the Onsite Verification Phase. The table below details the Online and Onsite Verification Phases, as well as the responsibilities of the TAC. All User Agencies must participate in the Online Phase. User Agencies are selected for Onsite Verification based on a combination of risk factors (i.e. poor historical compliance, new User Agency status, unique system-use cases), as well as complex User Agency structure (e.g. geographical distribution and size).

Phase		Description	Responsibilities
1	Online Phase	The DOJ CSA provides the User Agency TACs with the Online Questionnaire to be completed for each service and data it accesses. The Online Questionnaire consists of questions related to the FBI CJIS Security Policy, the DOJ CJIN Policy, and other relevant system-specific policies	The TAC completes the Online Questionnaire, including the submission of required supporting evidence related to both the Online Questionnaire and system transactions performed by individual users
2	Onsite Verification Phase	The DOJ CSA performs in–person, onsite visit of selected User Agencies and selected regional administrative sub-units (e.g. Field Offices, Regional Offices, Judicial Districts, and Field Divisions) to confirm the Online Questionnaire responses, as well as review and collect additional evidence of compliance	The TAC completes the Online Questionnaire prior to the scheduled Onsite Verification, and facilitates the auditor's verification activities at the regional administrative sub-units

3.3 Audit Documentation

The table below sets out the documentation types required during the DOJ CSA Audit:

Audit Documentation Type	Description
Evidence of Compliance	The TAC is required to produce one of the three following types of compliance evidence as determined by the Auditor: • Artifact –evidence that shows agency compliance to required processes (such as a User Agency Standard Operating Procedure) • Metadata – structured information that describes, explains, or locates an artifact, for example the title of an artifact and time stamps (such the date of approval and approving official for User Agency Standard Operating Procedure) • Agency-Certification – affirmation of compliance from the TAC (such as the TAC's written assurance that the User Agency has a specific Standard Operating Procedure in place)
DOJ CSA Audit Findings and Rating Report	At the conclusion of the Online and Onsite Phases, the DOJ CSA sends the User Agency the Audit Findings and Rating Report, which contains: • Summary of the Audit • Findings of non-compliance • Rating based on the severity of non-compliance • Recommendations to improve compliance with statutes, regulations, and policy • Request for the User Agency to produce a Corrective Action Plan if there are any findings of non-compliance
User Agency Corrective Action Plan	If there are findings of non-compliance issued by the DOJ CSA, the User Agency must enact a DOJ CSA-approved User Agency Corrective Action Plan, completely addressing all findings. The User Agency shall notify the DOJ CSA of the completion of the User Agency Corrective Action Plan. If the User Agency believes that the DOJ CSA Audit Findings and Rating Report is fundamentally flawed, the User Agency may dispute specific findings in writing

3.4 Audit Cycle

The DOJ CSA's Audit Cycle is every three years and follows the Federal fiscal year, which begins on October 1 and ends on September 30. The chart below sets out the DOJ CSA's Audit Cycle:

DOJ CSA Audit Cycle
October 1, 2017 – September 30, 2020
October 1, 2020 – September 30, 2023

3.5 Sanctions

The failure to comply with the applicable laws, regulations, and policy requirements, to include those in the FBI CJIS Security Policy, all related FBI CJIS system-specific manuals, the Nlets User Policy Manual, directives and decisions of the criminal justice community’s Advisory Policy Board (APB), National Crime Prevention and Privacy Compact Council, and all relevant DOJ specific policies, orders, and regulations, may subject the User Agency, an individual user, or both, to DOJ CSA sanctions that range from suspension of access to termination of services.