

National Identity Services Audit

Audit Objective(s)/Scope

The FBI's CJIS Division has established audit programs for the purpose of evaluating compliance with policy requirements associated with access to CJIS systems and information. The National Identity Services (NIS) Audit assesses compliance with Interstate Identification Index (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 Privacy Compact (Compact) rules and procedures. The NIS Audit is conducted with state criminal history record repositories, federal agencies, FBI-approved channelers, and other entities authorized access to Next Generation Identification (NGI) and III, and includes reviews of local agency components within their applicable jurisdictions.

III Participation Minimum Requirements In order to participate in the III, a state must meet the minimum standards described in Chapter 3, Section 2 of the *III/NFF Operational and Technical Manual*. These standards include requirements for fingerprint identification, record content, record maintenance, record response, and accountability.

NFF Qualification Requirements In order to participate in the NFF Program, a state must meet the requirements described in Chapter 8, Section 2 of the *III/NFF Operational and Technical Manual*. These standards augment III participation requirements and include requirements for fingerprint identification, record content, record maintenance, record response, and accountability.

Access to CHRI for Non-criminal Justice Purposes Agencies which access criminal history records for non-criminal justice licensing and employment purposes must meet requirements established in federal laws and regulations, as well as requirements established by the Compact Council for such access. Specific policies include: Use of CHRI; Reason Fingerprinted Field and Purpose Code Usage; Dissemination of CHRI; Applicant Notification and Record Challenge; Name-Based III Access Using Purpose Codes I and X; User Fee; and Audit Program. Primary sources for these policy requirements include:

- Title 28, United States Code (U.S.C), Section 534 (a)(4) and (b)
- Title 42, U.S.C, Section 14616, Article IV (c) and Article V (a) and (c)
- Title 5, U.S.C., Section 552a, (e)(3)
- Title 28, Code of Federal Regulations (C.F.R.), Section 50.12, (b)
- Title 28, C.F.R., Section 20.33, (a)(3) and (d)
- Title 28, C.F.R., Section 901
- *III/NFF Operational and Technical Manual*, Chapter 2, Section 2
- *CJIS Security Policy*, Version 5.3, Section 5.11.2

Outsourcing of Functions Involving Access to CHRI Authorized recipients of CHRI for non-criminal justice purposes and private/governmental contractors which have access to CHRI on behalf of these authorized recipients must meet the requirements set forth in the *Security and*

Management Control Outsourcing Standard for Non-Channelers or the *Security and Management Control Outsourcing Standard for Channelers*, as applicable. These standards incorporate various responsibilities of authorized recipients and contractors regarding establishment of adequate safeguards for CHRI to include compliance with the *CJIS Security Policy*.

Overview of the Process

Pre-audit

Pre-audit activities provide a broad-based appraisal of the audit participant, as well as those activities necessary to coordinate the logistics of the audit. Pre-audit tasks are centered on the initial gathering of information required for successful execution of the audit. Primary pre-audit tasks include:

- Conducting internal research, which includes reviewing fingerprint submissions and NGI or III transactions/messages as well as applicable statutes used by the audit participant to access criminal history.
- Contacting the audit participant to schedule the audit, explain the audit process, and request documentation.
- Selection of local agencies and/or organizational subcomponents/offices for review.
- Preparing surveys, questionnaires, and requests for information and forwarding to the audit participant for completion, as applicable.
 - III Unsolicited Message Surveys (record consolidations, non-unique and missing SID numbers, and missed identifications)
 - III Usage Surveys (purpose codes I, X, and others as applicable)
 - Fingerprint Surveys (user fee and access to CHRI)
 - Information regarding access to CHRI by local agency components (authorities leveraged, fingerprint transactions, primary systems involved)
- Reviewing documentation and information received from the audit participant.

Local Agency/Record Selection

The NIS Audit includes procedures for selecting local agencies and/or organizational subcomponents in order to assess the primary audit participant's performance in administering access to CHRI for noncriminal justice purposes. Of principal importance is obtaining the best available representation of the primary audit participant's access to CHRI at key nodes of operation. A typical state audit includes selection of 10 to 16 local agencies. Factors used to prioritize selection include (in no specific order):

- Relative volume of access to CHRI over a period of time.
- Use of multiple statutory authorities and the number of applicant types.
- Leveraging of programs which authorize dissemination to non-governmental entities and the re-use of criminal history records.
- Compliance issues identified during past audits.
- Use of name-based III access.
- Number of times audits have been conducted in the past.

- Use of private and/or governmental contractors for administrative functions.
- Type and scale of systems used for distribution and storage of CHRI.
- Logistical and resource constraints

For each local agency, a sample of fingerprint transactions is selected for review (typically 25 to 50). If the local agency is also authorized access to name-based III checks, then a sample of III transactions is selected (typically 25 to 50). Transactions are generally selected based on trends, specific areas of interest, and potential anomalies identified during pre-audit analysis. However, in instances where the local agency's submissions appear to have no discernible differences, then a random selection of transactions may be made.

Assessment

The assessment phase centers on a comparison between policy requirements and the audit participant's processes associated with those policy requirements in order to determine compliance. There are a number of techniques or combinations of techniques employed:

- Interviews with audit participant personnel to include in-person and/or teleconference.
- Surveys and questionnaires completed by the audit participant.
- Review of policy and procedural documents to include: standard operating procedures; statutes; administrative rules; and forms.
- Review of case files and/or other documentation associated with system transactions or access.
- Demonstrations by the audit participant of administrative processes and information technology platforms.
- Exit briefings with audit participant personnel to provide tentative results and potential areas of concern.

Post-audit

Post-audit activities center on reporting the results of assessments as well as reconciliation of compliance issues. Draft audit results are prepared and forwarded to the audit participant. Applicable policy/reference material and additional supporting audit documentation may also be provided. The draft audit results include:

- Findings of compliance status relative to policy requirements, which could include varying degrees of compliance such as: in compliance; out of compliance; area of concern; and note of interest.
- Analysis describing why the conclusion regarding compliance status was made.
- High-level required actions needed for the audit participant to correct compliance issues or improve performance.
- Request for a formal response from the audit participant describing actions taken as a result of the audit findings and required actions.

Final audit results are published which incorporate the audit participant's response to the draft results. Applicable final audit results are forwarded to the Compact Council's Sanctions

Committee for review and disposition in accordance with the procedures set forth in Title 28, C.F.R., Section 907. As part of these procedures, the Compact Council or FBI may follow-up with the audit participant to request additional information in order to ensure compliance issues have been adequately resolved prior to formally closing the audit.