Next Generation Identification Audit

Audit Objectives/Scope

The FBI's Criminal Justice Information Services (CJIS) Division has established audit programs for the purpose of evaluating compliance with policy requirements associated with access to CJIS systems and information. The Next Generation Identification (NGI) audit primarily assesses compliance with: Interstate Identification Index (III) and National Fingerprint File (NFF) participation standards; federal laws and regulations associated with the use and dissemination of national Criminal History Record Information (CHRI); and National Crime Prevention and Privacy Compact (Compact) rules and procedures. The NGI audit is conducted with state criminal history record repositories, federal and federally-regulated agencies, and other entities with access to the NGI system, 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 2, Section 2.2 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 8.2 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 Noncriminal Justice Purposes Agencies which access criminal history records for noncriminal 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 policy areas include: Use of CHRI; Dissemination of CHRI; Purpose for Disclosure of CHRI; Applicant Notification and Record Challenge; Noncriminal Justice Agency Audits; and User Fee. Primary sources for these policy requirements include:

- Title 28, United States Code (U.S.C), Section 534 (a)(4) and (b)
- Title 34, U.S.C, Section 40316, 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 3, Section 3.2
- *CJIS Security Policy*
- Compact Council's Noncriminal Justice Online Policy Resources

Rap Back Participants in NGI Rap Back services must meet requirements published in the *NGI Program Rap Back Service Noncriminal Justice Policy and Implementation Guide* and the *NGI Program Rap Back Service Criminal Justice Policy and Implementation Guide*. These requirements include subscriber and submitter obligations for proper implementation of subscription management plans and associated privacy risk mitigation strategies.

Interstate Photo System (IPS) Agencies with access to IPS must meet participation requirements established by the *NGI Interstate Photo System Policy and Implementation Guide*. These requirements include baseline standards for enrollment of photos and authorized facial recognition searches.

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 statutory authorities used by the audit participant to access criminal history.
- Contacting the audit participant to schedule the audit, explain the audit process, and request documentation.
- Selecting 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. Examples include:
  - III Unsolicited Message Surveys (record consolidations, non-unique and missing SID numbers, and missed identifications)
  - III Usage Surveys (purpose codes A, H, 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.

Agency Selection

The NGI 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. Of principal importance is obtaining the best available representation of the primary audit participant's access to CHRI at key nodes of operation. Currently, a typical state audit includes on-site reviews of approximately seven local agencies. Factors used to prioritize selection include (in no specific order):

- Relative volume of access to CHRI over a period of time (e.g., fingerprint submissions).
- Use of multiple statutory authorities for access to CHRI and the number of applicant types.
- Use of multiple NGI services such as Rap Back and/or IPS.
- Leveraging of programs which authorize dissemination of CHRI to non-governmental entities and/or the re-use of CHRI for multiple purposes.
- Compliance issues identified during past audits.
- Use of name-based III access.
- Number of times audits have been conducted in the past.
- Submission of no-fee or reduced-fee fingerprints.
- Type and scale of systems used for distribution and storage of CHRI.
- Logistical and resource constraints such as geographical location and cost.

For each local agency, a sample of fingerprint and/or other types of transactions, such as name-based III queries, are typically selected for review. 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 primary 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 findings of noncompliance were made and causes.
- High-level recommendations capturing action required for the audit participant to correct compliance issues or improve performance.
- Requests for formal responses from the audit participant describing actions taken as a result of the audit findings.

Final audit results are published which incorporate the audit participant's response to the draft results. Applicable final audit results are forwarded to the CJIS Advisory Policy Board's (APB's) Compliance Evaluation Subcommittee and/or the Compact Council's Sanctions Committee for review and disposition in accordance with their respective shared management and oversight responsibilities. As part of these procedures, the CJIS APB, Compact Council, and/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.