National Data Exchange

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 Data Exchange (N-DEx) Audit is to assess compliance with appropriate policies which pertain to the system access, system usage, and training of the N-DEx system. Assessments are made based on policies set forth in the *CJIS Security Policy* as well as the *CJIS National Data Exchange Policy and Operating Manual*.

Overview of the Process

Pre-audit

Prior to the audits, the CAU auditors contact the CJIS Systems Officer (CSO) 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 CAU staff will provide agency personnel with an overview of the audit process and what they can expect during the audit.

The CAU staff will internally request a sample of N-DEx transactions that will be used to ensure the legal use and dissemination of the N-DEx information. Some agencies will receive a Transaction Survey to complete prior to the audit. The survey will be e-mailed to the N-DEx Agency Coordinator (NAC) with a response deadline for it to be e-mailed back to the audit Point of Contact (POC).

Assessment

CAU staff will conduct telephone interviews with agency personnel to discuss N-DEx policies and procedures and review the transaction survey, if applicable. Upon completion of the interviews, auditors will determine compliance with laws, policies, and regulations as they pertain to system access, system usage, and training of the N-DEx system.

After all interviews and policy assessments have been completed, the audit staff will conduct a briefing with agency representatives to present audit findings, including areas of compliance and non-compliance, and provide a policy compliance packet via e-mail. The auditors will advise agency representatives that the audit findings will be documented in an audit report.

Post-audit

Upon completion of N-DEx audits, auditors will enter all audit results into an in-house database which will be used to prepare the N-DEx audit report.

To ensure the accuracy of information entered into the database, all entries will be double-checked by another auditor. This information will be provided to the N-DEx audit manager who will perform a triple-check of the data. Both the double-check and triple-check will ensure that all policies were accurately and consistently assessed for all audited agencies**.**

The N-DEx audit manager will analyze the data collected to develop an audit report that summarizes non-compliance areas with the *CJIS Security Policy*, the CJIS National Data Exchange Policy and Operating Manual, as well as with appropriate laws, policies, and regulations that govern the CJIS systems.

The CSO will be requested to review the audit report and respond to the required actions, if any exist, regarding their corrective actions that will be implemented to achieve policy compliance. Their response will be incorporated into the Executive Summary of the N-DEx report.

Currently, N-DEx audit findings are informational only and are presented in aggregate totals of non-compliance areas to the Information Sharing Policy Board.