Preparing for a LEIN Audit

The FBI CJIS Security Policy, Version 5.4, Section 5.11.2, requires the CJIS Systems Agency (CSA) to audit all criminal justice agencies that have direct access to the state system triennially in order to ensure compliance with applicable statutes, regulations, and policies. The Michigan State Police (MSP) is the CSA for the State of Michigan, with the Criminal Justice Information Center (CJIC) designated as the executive agent within MSP that holds the responsibility for compliance auditing. The CSA has the mission of ensuring the security, integrity, and confidentiality of Criminal Justice Information (CJI) through compliance auditing of, assistance to, and as an essential resource for criminal justice agencies within the State of Michigan. Michigan adopted the FBI CJIS Security Policy as the security policy for the state, and in addition, has incorporated the Michigan Addendum to further clarify some policy requirements. This is the reason why agencies are audited by the MSP Law Enforcement Information Network (LEIN)/National Crime Information Center (NCIC) Auditors.

The audit process assists in ensuring the security, integrity, and confidentiality of CJI. The audit process consists of reviewing and evaluating agency physical and technical security, administrative policies, criminal history use, records entered into LEIN/NCIC, and other practices in order to identify the level of compliance by user agencies with state and federal law, along with other applicable requirements. The audit process not only assures compliance but identifies areas of concern and will assist in correcting and resolving the noncompliance issues.

So how does an agency prepare for the audit process? The agency designated terminal agency coordinator (TAC) is the main point of contact, responsible for preparation, and participating in the audit. The TAC will receive a phone call from the Auditor and a mutual date and time, approximately 30 days out, will be scheduled. During the scheduling conversation, the Auditor will review and discuss the areas of the audit: Technical Security Review, Administrative Review, Criminal History Review, the criminal history query log (QLOG) and if applicable, Data Quality or the Records to be reviewed, and what to expect on the day of the audit. The agency will receive a packet of information in the mail approximately 10-14 days after the phone conversation that provides the written audit preparation directions.

The Technical Security Review (TSR) questionnaire is mailed in the audit packet. This questionnaire needs to be completed by the TAC and the agency IT provider (City/County/Private/Agency IT). The questionnaire mentions policies and procedures that are required for technical security compliance. The TAC will need to have the agency's policies and procedures available for review by the Auditor. Sample required TSR policies and procedures are available on the MSP LEIN website (http://www.michigna.gov/LEIN). However, agencies are required to tailor the sample policies to reflect agency practice.

Part of the TSR includes ensuring that all personnel with unescorted access have been fingerprinted and background checked. In addition, anyone with unescorted access, including IT personnel, janitorial/maintenance personnel, city managers, contractual service providers, etc., must be trained in Security Awareness Training (SAT). Proof of SAT completion must be documented. MSP has a power point presentation that is available on the MSP LEIN website.

IT personnel that are not department employees (e.g., all City/County IT employees) must sign a Management Control Agreement (MCA). If your agency IT provider is a contractual agent, in addition to

executing a MCA with them, each employee of that agency must read and sign a CJIS Security Addendum. Both the MCA and the CJIS Security Addendum can be found on the MSP LEIN website.

Also included in the mailed packet is the Executive Level Training Supplement document. This document needs to be signed by the agency head. Locate your agency network diagram, the agency LEIN User Agreement with MSP, fire department or school access agreements (if applicable), Holder of the Record Agreements, Hit Confirmation Agreements, and ORI Agreements, if they pertain to your agency. All agreements will be reviewed by the Auditor.

Ensure your agency information is updated/correct in LEIN. Update the Certified Operator file in LEIN with the list of current operators and last date of certification. Copies of the most recent LEIN Certification tests should be available for the Auditor to review. Also have available documentation of the TACs most recent training or certificate.

A substantiation of criminal history inquiries will be completed the day of the audit. The Auditor will bring a QLOG with them. The QLOG is a random sampling of fifty criminal history inquiries that were made in the 90 days prior to the date of the QLOG. Substantiation may be through the agencies electronic records management system, written logs, etc.

If the agency enters records into the LEIN/NCIC system, the agency will need to prepare the requested number of Warrants, PPOs, Missing Persons, and/or Stolen Vehicles. Part of the audit is to assess the accuracy, completeness, and timeliness of records that are being entered into LEIN/NCIC.

The warrants can be taken from the most recent monthly validation lists or by randomly selecting the requested number from the agency's warrant drawer/file. Pull the number of requested warrants and for each warrant, run the System Identification Number (SYSIDNO) on the entry. Running by the SYSIDNO provides the most current entry information in LEIN. If you do not know or cannot find the SYSIDNO, query the person by name, locate the SYSIDNO, and then run by the SYSIDNO. Run a new person query and a criminal history inquiry on each of the warrants. Check the warrant entry for all available identifiers and verify that all current information is correct. If you should have to make corrections, modifications, or supplement the original entry be sure to print a new copy of the LEIN entry by the SYSIDNO. If the warrant was entered into NCIC, a copy of the NCIC entry must also be printed and included with the requested documentation. Paperclip all the information together in this order: the LEIN entry and NCIC entry if applicable, warrant (or copy of the warrant), the person query and criminal history information, and a copy of the complaint, ticket, or other originating documentation. Remember, this needs to be completed for each warrant being reviewed.

For Personal Protection Orders (PPOs), follow the same procedure as warrants, pulling the requested number from the drawer/file. There most likely will not be a complaint to accompany the preparation of PPOs.

With Stolen Vehicle entries, run each entry by the vehicle identification number (VIN). Along with the LEIN entry information, the Auditor will want to review the original police report (or a copy of it), the Secretary of State (SOS) response, and the NCIC response. This is to ensure the information is accurate and matches the report. If owner data has been entered be sure it is accurate. The SOS print out will indicate if the insurance company has paid. If this is the case, you may need to modify the owner information to reflect the insurance company information. Paperclip all the information together in this

order: the LEIN/SOS entry, the NCIC entry, and the original (copy) of the police report. This process needs to be completed for each of the Stolen Vehicle records being reviewed.

To prepare the Missing Person records, run the individual(s) in LEIN and print only the LEIN and NCIC missing person entry information. Place the LEIN/NCIC printouts with the investigation report(s).

The audit findings will be shared with the TAC at the close of the audit. The TAC will know all areas of noncompliance, what needs to be completed, and resources are provided. The Auditor will assure the TAC has a good understanding of everything and will provide contact information for questions and assistance that may be needed in the future.

The audit process assists in ensuring the security, integrity, and confidentiality of CJI. Audits are required and unavoidable. The Auditors want agencies to be successful. If you have questions, need assistance, or are interested in additional training opportunities, contact your Auditor.