Audit Highlights

Highlights of Legislative Auditor report on the Security and Integrity of the State's Criminal History Repository, issued on May 8, 2002.
Report # LA02-24.

Purpose of Audit

The purpose of this audit was to determine the security and integrity of the state's criminal history repository. The repository is managed by the Records and Identification Bureau within the Nevada Highway Patrol Division of the Department of Public Safety. Our audit included a review of controls over the criminal history records database, and data stored in the database as of March 30, 2001.

Audit Recommendations

This report contained 14 recommendations to improve the security and integrity of the criminal history repository. The Bureau should test the accuracy of the criminal history records database, implement the re-key function for disposition information, and standardize and file disposition forms to allow more effective entering and efficient retrieval. The Bureau should also re-enter missing criminal records and determine how records were deleted. In addition, it should retain fees for services performed. To provide greater security over criminal history records, the Bureau must provide password controls, lock users out after a specified period of inactivity, and ensure only current employees have system access. In addition, the Bureau should capture information and report on user activities and limit physical access to authorized individuals. Furthermore, the Bureau should update its disaster recovery plan and provide offsite backup storage. Finally, it should ensure each local criminal justice agency is audited biennially.

The Agency accepted all 14 audit recommendations.

Status of Recommendations

The Department of Public Safety filed its 60-day plan for corrective action on July 25, 2002. The plan indicates that good progress is being made to implement the 14 audit recommendations.

The six-month report on the status of audit recommendations is due February 3, 2003.

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.us/audit (775) 684-6815.

Security and Integrity of The State's Criminal History Repository

Results in Brief

Errors and missing data in the criminal history records database reduce the reliability of programs that rely on this information. Such programs include background checks for employment and gun purchases. In addition, thousands of criminal fingerprint cards have not been fully processed and others were not processed timely. These weaknesses have resulted from a lack of controls in entering and testing data, and allocating resources to other activities.

Computer security weaknesses place the criminal history repository at risk of unauthorized access to the system and data. This could result in sensitive and confidential information being viewed, altered, or destroyed deliberately or accidentally. In addition, controls over physical access to source documents and computer equipment need strengthening. Furthermore, the lack of a complete disaster recovery plan leaves the system vulnerable in the event of a disaster or tampering with data. Sustained management commitment is needed to ensure these weaknesses are addressed.

Principal Findings

The criminal history database contained inaccurate information and some records were missing. In one test, 31 of 945 (3%) data elements in the database contained errors. In another test, 56 of 155 (36%) data elements contained errors. These errors were caused by data entry, lack of a re-key function, and system design problems. Furthermore, the entire criminal histories for 47 individuals were no longer present in the database. The cause of these missing records is unknown. Having errors in records of criminal history will impact the accuracy of background checks for gun purchases and work-related background checks.

Nearly 70,000 criminal fingerprint cards have not been fully processed by the Records and Identification Services Bureau. Specifically, information from the cards has been entered into the criminal history records database, but the fingerprints have not been matched to existing records. In addition, the re-key function has not been performed for 40% of these cards which could reduce the accuracy of the information entered into the database.

Adequate password controls, designed to prevent unauthorized access to computer data, have not been implemented. We found 4,381 of 4,757 (92%) passwords tested for one computer system did not meet the criteria for strong passwords. In addition, we found passwords that had been in use for an extended period of time without a forced change. Furthermore, passwords are stored in plain text rather than encrypted.

Computer system access controls are not designed to limit or detect access to computer programs and data. These controls protect information from being viewed, altered, or destroyed by unauthorized individuals. Users are allowed unlimited login attempts, and are not locked out after a period of inactivity. In addition, the system is not designed to detect and prevent suspicious activities leading to unauthorized access.

Access to the computer system is not always terminated for ex-employees. One employee had access 3 months after leaving and another employee 11 months after leaving. By allowing access to ex-employees, there is increased risk of these employees or others gaining unauthorized access to sensitive criminal information.

Access to fingerprints cards was not adequately controlled thus increasing the risk of losing cards. The door to the fingerprint card room was open 39 of the 43 (91%) times we checked. In addition, nearly 4,000 criminal fingerprint cards were stored in open containers by the door to this storage room.

The Bureau's disaster recovery plan for the criminal history records database does not address all key components that are designed to ensure protection of assets. Specifically, the plan has not been tested, there is no specific assignment of responsibilities, and critical data has not been identified. In addition, the location used to store a backup copy of the criminal history database is not off-site.

Audit Division
Legislative Counsel Bureau