LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
Angie Grove

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Kent Rice, Information Systems Audit Manager

CC: Steve Bullock, Attorney General, Department of Justice
Tim Burton, Deputy Director, Department of Justice
Joe Chapman, CIO, Department of Justice
Mike Batista, Administrator, Department of Justice

DATE: October 2012

RE: Information Systems Audit Follow-up (12SP-38): Sexual or Violent Offender Registry (11DP-08)

ATTACHMENTS: Original Information Systems Audit Summary

Introduction

The *Sexual or Violent Offender Registry* (11DP-08) report was issued to the Committee in June 2011 and contains five recommendations to the Department of Justice (DOJ). In June 2012, we began gathering preliminary information from the DOJ regarding progress toward implementation of the report recommendations. This memorandum summarizes the results of our follow-up work.

Overview

The Sexual or Violent Offender Registry (SVOR) is the central listing of sexual and violent offenders residing in Montana who are required to register their location. This audit reviewed who has access to offender data, how changes to the system are controlled, how the systems are maintained, and what controls are in place to ensure data integrity. Of the five recommendations made in the report, one has been fully implemented and the other four are being implemented.

Background

The SVOR system is developed and maintained by DOJ and is comprised of three main components: 1) the registry, 2) the website, and 3) a repository for offender photographs. The registry is the primary database containing all active and inactive offender registration information. The website allows the public access to offender information. Offender photographs are stored on servers and matched with offender records for searches on the website. The website servers, along with the photographs, are hosted and maintained by the Department of Administration (DOA).

Follow-up Audit Findings

The following sections summarize progress towards implementing the report recommendations.

Room 160 · State Capitol Building · P.O. Box 201705 · Helena, MT · 59620-1705
Phone (406) 444-3122 · FAX (406) 444-9784 · E-Mail lad@mt.gov
http://leg.mt.gov/audit

Access Management

Access controls minimize the risk of unauthorized access to agency systems and data. Because there are various components within the SVOR system which are managed by two separate agencies, we reviewed access to information to ensure it was restricted to users with a business need. Our audit noted assigned access that either was not needed or DOJ was not aware of.

RECOMMENDATION #1

We recommend the Department of Justice strengthen system access controls for the Sexual or Violent Offender Registry by:

A. Developing, documenting, and executing a process to add, remove, or change system access.
B. Developing, documenting, and executing regular system access reviews.
C. Establishing a formal agreement with the Department of Administration outlining roles and responsibilities associated with hosted systems.

Implementation Status: Implemented

DOJ currently has two draft documents related to access. The first is DOJ policy on user and system access change control. According to this policy, the access request process is a four step procedure which includes the initial request, authorization, implementation, and sign-off. Authorization includes approval by the business owner, the requestor's supervisor, the security officer, and DOJ mid-tier supervisor. All four people must approve the request for it to be implemented. The second document is an internal procedure which provides details on the steps to follow. This policy and associated procedure are applicable to all systems maintained by DOJ, not just SVOR.

DOJ conducted a review of access in July 2012. They reviewed access for both DOJ and DOA. The review resulted in removal of access for three DOJ employees. Numerous DOA employees have access to the data, and according to DOJ, this is because DOA does not assign employees to specific systems. In addition, all DOA employees with access to DOJ systems and data are required to go through background checks. This is included in a memorandum of understanding DOJ developed with the State Information Technology Services Division (SITSD), DOA. The purpose of the agreement is to "define the process and roles and responsibilities regarding DOA SITSD access to DOJ systems and data that are hosted by DOA SITSD."

RECOMMENDATION #2

We recommend the Department of Justice strengthen user access reviews for the Sexual or Violent Offender Registry by ensuring the Information Security Officer:

A. Develops, implements, distributes, and maintains user access review policies and procedures.
B. Performs and documents ongoing user access reviews.

Implementation Status: Being Implemented

As noted under Recommendation #1, DOJ has drafted policy and procedures related to user and system access change control and has completed a review of user access. The policy is currently awaiting signature by the Attorney General. Once signed, this recommendation will be fully implemented.

Change Management

In order to reflect the changing needs of an organization or to remediate flaws, system data and programming code needs to be modified and updated. Because there are risks associated with any programming or data changes, an organization should try to mitigate risks by controlling changes. This occurs through a process called change control which manages changes from the initial request to full

implementation. Our audit noted a change management process was in place, but documentation was incomplete and there was no change management policy.

RECOMMENDATION #3

We recommend the Department of Justice follow state policy for change management processes.

Implementation Status: Being Implemented

DOJ plans to implement policy and procedures related to change management. DOJ is currently reviewing their processes and has formed a working group to review incident management. This working group will also review change management and configuration management. The policies and procedures developed in this area will also be for all DOJ systems.

RECOMMENDATION #4

We recommend the Department of Justice develop and implement formal access control policies which address segregation of duties.

Implementation Status: Being Implemented

DOJ plans to develop and implement policies which address segregation of duties; however, DOJ is currently changing its system architecture. According to DOJ personnel, most DOJ systems, including SVOR, are Oracle-based. DOJ has limited resources with expertise in this area and recently experienced turnover. In order to address this limitation, DOJ is planning to switch its systems to be SQL-based as DOJ has more personnel with expertise in this area.

Data Integrity

Data integrity gives users assurance that information is trustworthy. We reviewed data input, system processing, and data output for data integrity. While controls are in place to help ensure data integrity, we noted offenders who are overdue on verifying their location are not flagged in SVOR, and deceased offenders are not routinely removed from the registry.

RECOMMENDATION #5

We recommend the Department of Justice strengthen the integrity of offender data in the Sexual or Violent Offender Registry by:

A. Flagging an offender when they fail to verify their address.
B. Developing a routine process to compare active offenders against death records.
C. Inactivating offenders who match deceased records.

Implementation Status: Being Implemented

DOJ updated SVOR to flag offenders who fail to return their address verification letters or fail to keep their registration current as required by law as “noncompliant”. This designation is noted on the SVOR website.

DOJ personnel are currently working with personnel from the Department of Public Health and Human Services to develop an automated process for comparing the death registry to the SVOR database. They plan to run the comparison twice per year. In addition, according to DOJ personnel, as part of training, DOJ personnel remind local law enforcement of the need to notify DOJ of deceased offenders.