A Report
to the
Montana
Legislature

Information Systems Audit

Sexual or Violent Offender Registry

Department of Justice

June 2011

Legislative Audit
Division

11DP-08

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting, education, computer science, mathematics, political science, and public administration.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705
(406) 444-3122

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor

Deputy Legislative Auditors
Cindy Jorgenson
Angie Grove

June 2011

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit of the Sexual or Violent Offender Registry System maintained and operated by the Department of Justice to assist in the administration of offender registration records. The focus of the audit was to ensure specific controls are in place and processes are working as intended.

This report contains five recommendations for strengthening controls over user access, change management processes, and data integrity.

We wish to express our appreciation to department personnel for their cooperation and assistance.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

Table of Contents

Figures and Tables

Figures

Tables

Appointed and Administrative Officials

Department of Justice	Steve Bullock, Attorney General
	Tim Burton, Deputy Director
	Mike Batista, Administrator, Division of Criminal Investigation
	Joe Chapman, CIO, Administrator, Justice Information Technology Services Division
	John Strandell, Chief, Investigations Bureau
	Jack Marks, Chief, Application Services Bureau

Montana Legislative Audit Division

Information Systems Audit

Sexual or Violent Offender Registry

Department of Justice

June 2011 11DP-08 Report Summary

The Sexual or Violent Offender Registry (SVOR) system plays a key role in the tracking and management of sexual and violent offenders in Montana. Given its important role in public safety and informing law enforcement and the public on the whereabouts of offenders, data integrity is critical. We determined nearly 26 percent of the total registered active offender addresses are not verified and not flagged in the system.

Context

The registry is the primary database which houses all offender registration information in Montana. As of April 2011 there were nearly 5,000 registered sexual or violent offenders in the registry. The registry is used by the public to identify the location of registered offenders and by law enforcement for queries of criminal history and offender information. There were over 120,000 public searches and 100,000 law enforcement queries during November 2010.

Results

Overall, SVOR has controls in place in the areas we tested. However, we identified areas where controls over the SVOR system can be strengthened including: user access, change management, and data integrity.

The Department of Administration hosts two components of the SVOR system. DOA users have excessive access to SVOR systems. The Department of Justice (DOJ) was not aware of DOA access to offender photographs, the website program code, or the website database. Additionally, they did not participate in, or review, determination of DOA user access.

We reviewed change management documentation for evidence the department's change management processes were being followed. Our review of these records identified weaknesses in the documentation process including: lack of management approval, no indication of user acceptance testing, and inconsistent indication of reasons for changes. Lack of an effective change management process can lead to unauthorized changes to the system or the inability to quickly identify and correct programming errors.

According to §46-23-507, MCA, offenders who fail to register, verify registration, or keep registration current are subject to potential incarceration, a fine, or both. However, offenders who fail to submit their annual verification letter within 15 days are not automatically flagged in SVOR in such a way that makes their overdue status available to law enforcement or the public. We determined nearly 26 percent of the total registered active offender population are

(continued on back)

overdue and not flagged. As a result, when members of the public access the website or law enforcement queries data, they will not be aware of the offender's failure to verify their registration.

Recommendation Concurrence	
Concur	5
Partially Concur	0
Do Not Concur	0

Source: Agency audit response included in final report.

For a complete copy of the report (11DP-08) or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to **lad@mt.gov**; or check the web site at **http://leg.mt.gov/audit**
Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
Call toll-free 1-800-222-4446, or e-mail **lad@mt.gov.**

Chapter I – Introduction

Introduction

The Division of Criminal Investigation within the Montana Department of Justice (DOJ), in cooperation with local and federal criminal justice agencies, maintains a state registry of offenders convicted of sexual or violent crimes. Based on an assessment of risk and in the interest of public safety, the Legislative Audit Division conducted an Information Systems audit of the Sexual or Violent Offender Registry (SVOR) system.

Audit Objectives

We audited SVOR to identify and test key controls to ensure system access is limited, changes are controlled, and data integrity maintained. Our objectives were to:

1. Determine if SVOR system access is limited to users with a legitimate business need.
2. Determine if changes to the system are controlled.
3. Determine if an agreement is in place outlining responsibility for maintaining and restoring hosted SVOR systems.
4. Determine if controls are in place to ensure data integrity including automatic monitoring of offender status, web server updating, and complete and up-to-date data.

Audit Scope and Methodology

Offenders complete registration forms at either Department of Corrections facilities or their local registering entity (either the county sheriff or city police department). The forms are submitted to DOJ and manually entered into SVOR. County and city entities are outside of our jurisdiction, and therefore, were not part of our audit. As a result, our audit scope focused on a review of data once it arrives at DOJ. Our work also included a review of controls in place over the SVOR system and business processes at DOJ.

Work included interviewing DOJ and Department of Administration (DOA) personnel, querying the SVOR system, observing business processes, reviewing agency information, and comparing hard copy data entry records against system data. Additionally, we observed reconciliations of county registries performed by DOJ personnel and used to update SVOR data.

Management Memorandum

During the course of our audit, we identified an area warranting management attention. The version of the underlying Oracle application software currently in use for the SVOR application is an out of date, unsupported version and should be updated. Although not included as a recommendation in this report, our suggestion was presented to DOJ for its consideration.

Chapter II – Background

Introduction

In an effort to assist law enforcement and help protect the public, Congress and individual states required registries which track the whereabouts of sexual offenders, and in some cases, violent offenders. The Division of Criminal Investigation within the Montana Department of Justice (DOJ), in cooperation with the Department of Corrections (DOC) and local and federal criminal justice system agencies, maintains a state registry of offenders convicted of sexual or violent crimes.

Background

In 1994, Congress passed legislation addressing registration of sexual offenders. Provisions required states to create sexual offender registries, but gave states discretion to determine what types of sexual offender information was made available to the public.

In 1996, Congress required creation of a national database for tracking the location and movements of persons who commit certain sexual crimes or crimes against children. The National Sexual Offender Registry is a database maintained by the National Crime Information Center, a national repository for criminal justice information within the Federal Bureau of Investigation.

Public access to information available on offender registries varies among states. Some states provide extensive offender information, including pictures, address information, nature of offense(s), characteristics of an offender's victim(s), and other biographical information. Some provide limited information such as the general location of offenders, while others consider this information confidential and make it available for law enforcement purposes only.

In 2006, Congress passed legislation standardizing offender information contained in state registries and information made available to the public, creating additional crimes requiring registration, and standardizing the designation of sexual offender tier levels.

History of the Montana Registry

In 1989, the Montana Legislature first enacted a registration law for sexual offenders which required a central registry maintained by DOC; delineated qualifying offenses; required only sexual offenders to register for a period of 10 years; and made the penalty for failing to register a misdemeanor. Under this legislation there were no provisions for making registry information available to the public. Since initiation, laws governing the registry have been expanded and strengthened.

In 1995, lawmakers strengthened the registration statute, which became known as the "Sexual or Violent Offender Registration Act" (§§ 46-23-501 through 520 and § 46-18-255, MCA) and redefined the offenses requiring registration. Montana became one of only a few states to register violent offenders in addition to sexual offenders. Specific changes included: requiring certain violent offenders to register; requiring registrants to be fingerprinted and photographed for registration purposes; and lengthening the duration of registration to life. Additionally, the penalty for failure to register was increased to a felony and certain registration information was made available to the public, including the name of any registered sexual offender and any additional information deemed appropriate by the district court for public distribution.

In 1997, the Legislature moved the Sexual or Violent Offender Registry (SVOR) Program from DOC to DOJ. The revised statute also added tier levels to sexual offenders which are currently assigned by the sentencing court based on the likelihood the offender would commit additional crimes. The type of information released to the public varied according to the offender's tier level, and law enforcement agencies were given authority to release additional offender information if safety of the community was at risk.

Additional changes have been made to the registration process in subsequent legislative sessions including:

- 2002: requiring offenders to register within 10 days of entering a Montana county for the purpose of setting up a home (even if temporary) for 10 days or more.
- 2005: requiring out of state and federal sexual offenders who move to Montana to be treated in the same manner as Montana offenders.
- 2007: requiring photos of all sexual offenders to be posted on the registry; in person verification of registration information; addition of special designations; increasing reporting frequency for certain offenders; and adding qualifying offenses.

Sexual or Violent Offender Registry System

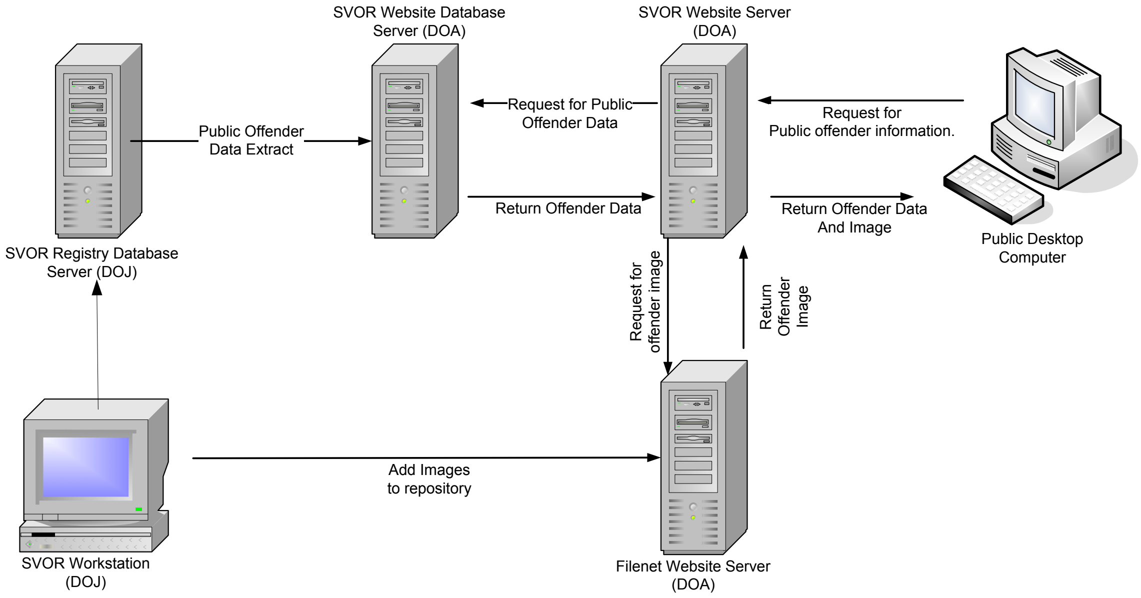
The SVOR system is developed and maintained by DOJ and is comprised of three main components:

- the Sexual or Violent Offender Registry (registry)
- the Sexual or Violent Offender Web (website)
- a repository for offender photographs (Filenet)

The following figure highlights the structure of the SVOR system.

Figure 1

SVOR System Overview


SVOR Website Database Server (DOA)
SVOR Website Server (DOA)
Request for Public Offender Data
Request for Public offender information.
Public Offender Data Extract
Return Offender Data
Return Offender Data And Image
Public Desktop Computer
SVOR Registry Database Server (DOJ)
Request for offender image
Return Offender Image
Add Images to repository
SVOR Workstation (DOJ)
Filenet Website Server (DOA)

Source: Compiled by the Legislative Audit Division from Department of Justice information.

The registry is the primary database containing all active and inactive offender registration information. Inactive offenders are those whose obligation to register has ended or who are deceased. As of April 18, 2011, there were 4,992 active registered sexual or violent offenders in the registry detailed in Table 1 below.

Table 1

Active SVOR Offender Types

Offender Type	Number of Registered Offenders
Violent	2,883
Sexual	2,028
Sexually Violent	81

Source: Compiled by the Legislative Audit Division from SVOR website information.

The registry is used by law enforcement for querying criminal history and offender information. Law enforcement queries are initiated through other systems such as the Criminal Justice Information Network, Montana Enhanced Registration and Licensing Information Network searches, and other law enforcement databases. During November 2010 there were over 100,000 law enforcement queries.

The website was developed and is maintained by DOJ and allows the public access to offender information. There were over 120,000 hits on the website in November 2010. The website servers, along with the Filenet, are hosted and maintained by the Department of Administration (DOA).

Offender photographs are stored on Filenet servers. The photos are matched with offender records when members of the public search for offenders on the website. As of April 2011 there were approximately 7,000 offender photographs stored on the server.

Chapter III – User Access

Introduction

State agencies often possess significant amounts of information; however, access to the information should be restricted to employees or customers with a business need. Access controls, including providing and removing access and regular access reviews, minimize the risk of unauthorized user access to agency information technology (IT) assets. This chapter addresses access controls for the Sexual or Violent Offender Registry (SVOR) systems and data.

System Access

The Department of Administration (DOA) manages two components of the SVOR system on its servers: Filenet (storage site for offender photographs) and the website (access point for public data). Server management requires use of administrator accounts allowing access to server specific settings and system data. The nature of administrator accounts is to allow access to an entire application or system, including data. Although DOA manages the servers, the Department of Justice (DOJ) owns the data on the servers. State policy requires access to data be restricted to users who need it to perform their job duties. Further, policy requires identification of authorized users.

We reviewed access to Filenet which stores offender photographs as required by §46-23-504, MCA. Once obtained by DOJ, the photographs are transferred to a DOA server through Filenet. As of April 2011, DOJ stored approximately 7,600 photographs on the server. Both agencies have assigned user access to Filenet. DOJ user access was limited to those with an identified business need. DOA access includes administrator accounts required to manage Filenet; however, these accounts also allow access to offender photographs.

The second system component hosted by DOA is the SVOR website. Although DOJ manages the website, both the program code and database are housed on servers managed by DOA. Again, both agencies have assigned user access to the website program code. However, DOJ has one user whose access was not needed. DOA access includes server administrator accounts required to manage the server; however, the accounts also allow access to the website program code.

We also reviewed access to the website database hosted by DOA. Access is managed by both agencies depending on where the user is employed. Although currently assigned DOA access is appropriate, the process does not ensure DOJ is informed if the access is changed. We also determined DOJ access to the database includes a contractor no longer needing the access and two former employees (one left in 2007 and the other in 2010).

DOJ management indicated they were not aware of DOA access to offender photographs, the website program code, or the website database. Additionally, they did not participate in, or review, determination of DOA user access. As a result, seven DOA administrators have access to add, remove, or change SVOR offender photographs; nine DOA administrators have access to the website program code, and one DOJ user has unnecessary access. User access reviews could have identified the unneeded access as well as the level of access for DOA employees. DOJ management stated user access reviews have not been a priority because of the limited number of staff with access to the database.

Service Level Agreement

State policy advises entities to:

- establish personnel security requirements including security roles and responsibilities for third-party providers.
- document personnel security requirements.
- monitor third-party compliance.

DOA is considered a third-party provider for DOJ since it provides servers and database support services.

Meeting the standard above typically involves the creation of formal, documented agreements, defining each agency's responsibilities. However, no formal agreement currently exists between DOJ and DOA outlining access to, and the roles and responsibilities for, SVOR system elements hosted by DOA. In 2005, there were two service level agreements (SLAs) in place; one for Filenet and one for website servers, but both SLAs expired in 2006. DOA extended the Filenet SLA to 2010; however, none of the extensions were signed by DOJ management as required by the 2005 SLA. DOJ stated they have been negotiating a website server SLA since 2006; however, no agreement has yet been made. The lack of valid SLAs has contributed to access control issues with SVOR components hosted by DOA. Additionally, without the SLAs in place, roles and responsibilities are not defined.

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.*

User Access

SVOR contains nonpublic data managed by DOJ. We queried SVOR to identify users with access to nonpublic data to determine if these individuals need the access to perform their job duties. DOJ management stated they perform nonpublic data access reviews on an annual basis and any users no longer requiring access are removed. However, we determined the most recent review did not result in the removal of users who no longer needed SVOR database access. Our review identified a total of seven individuals with unneeded access to nonpublic data. Three were missed by the review and four were identified for removal but removal never occurred.

The access review consists of a database administrator (DBA) running a query to determine who has access. The DBA will then ask DOJ staff responsible for approving the access if it is still needed, and adjust access based on the response. However, as noted above, this process is not effective in removing all unneeded access. Additionally, the access review is not documented, and there are no written policies and procedures.

State policy requires organizations to develop, document, and distribute user access policies and procedures as guidance for access control and management of user access accounts. Additionally, policy states the individual who administers security reviews should be separate from security personnel who administer access controls. Typically, access controls are part of an agency security plan. Section 2-15-114(2), MCA, requires an agency's information security manager to administer the agency security plan. Additionally, the position description for DOJ's information security officer (ISO) requires them to direct the development and implementation of DOJ system security, including access. However, the SVOR database administrator performs both security reviews and administration of the system's access controls.

DOJ IT management stated they are trying to refocus the ISO position on IT security policy and procedures. Documented user access policy and procedures providing guidance as well as ISO oversight would decrease the risk of excessive access.

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.*

Nonpublic Offender Data

The SVOR registry contains offender data considered nonpublic such as social security numbers. This information is not essential to informing the public. We reviewed system controls in place to determine if nonpublic offender data could be viewed by unauthorized individuals.

The extract process updates the website data from the registry and transfers it directly to the website database. We reviewed the program code for the extract process and did not identify any nonpublic offender data. Additionally, we reviewed the process in place for law enforcement to access nonpublic offender data to ensure no unauthorized users have access and determined controls are working as described. Finally, the SVOR website uses offender addresses to obtain geographic location codes from Google Maps to show the approximate location of an address. We reviewed the process used to obtain geographic location codes and determined no nonpublic offender data is exchanged with Google.

Conclusion

Aside from the previously noted unneeded access, we conclude the controls over nonpublic offender data are working as intended.

Chapter IV – Change Management Processes

Introduction

Information systems are generally a dynamic, changing environment. Data can be modified and programming code updated to reflect the changing needs of an organization or to remediate flaws. However, 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. We reviewed procedures in place for the Sexual or Violent Offender Registry (SVOR) to ensure the Department of Justice (DOJ) controls changes to SVOR.

Change Management Processes Should Be Better Documented

DOJ management stated requests for programming changes to the SVOR system are entered into a computer application. The request is assigned to a developer who, in concert with the individual or group requesting the change, evaluates the work needed. After initial evaluation the developer conducts a design analysis and submits it to the requestor for approval.

The approved design is then submitted to a DOJ programmer who develops the new program code. The change is tested in the development environment and, once it appears to be working, is moved to the test database by a database administrator. There it is tested by the developers to ensure the new code does not interfere with other aspects of the SVOR system. Once the change passes development testing, it is submitted to the requestor for user acceptance testing. After the requester has tested and approved the change, it is moved to the production environment.

Database Changes

Requests for database changes are initially handled in a different manner. Requests are managed through the use of an Implementation Plan Checklist (IPC). This document identifies the data to be changed, the process used to change it, migration procedures, and the personnel who will conduct the change. Once the IPC has been developed, the change process is similar to that for programming changes.

Change Documentation Is Incomplete

State policy provides guidance with regard to the documentation needed for change control. Overall, state policy recommends that an organization should:

- Approve changes to the system.
- Document approved changes to the system.
- Retain and review records of changes to the system.
- Audit activities associated with changes to the system.
- Coordinate and provide oversight for change control activities.

Effective documentation provides evidence of these objectives being met by the organization.

We extracted all available change documentation from the current change management application and obtained copies of the IPC's for 2009 and 2010. Our review of these records identified weaknesses in the documentation process:

- **No indication of management approval for requested programming changes**: any system change should be approved by management; however, programming requests all appeared to go directly from the requestor to the programmer.
- **No indication of user acceptance testing**: programming and data changes should all be tested prior to introduction into the production environment; however, department documentation did not indicate this was occurring.
- **Inconsistent indication of reason(s) for a requested change**: change documentation should include a reason for the requested change; however, department documentation did not always include reasons for requested changes.

Lack of an effective change management process can lead to unauthorized changes to the system or the inability to quickly identify and correct programming errors. Since SVOR is designed to inform the public and law enforcement of the whereabouts of offenders such errors could have serious consequences including compromising public safety.

DOJ management acknowledged that its process for documenting changes to the SVOR system is lacking. The department stated its intention is to upgrade to a new change management application.

No Change Management Policy

We inquired about any formal department change management policies and were informed that no such policies existed. State policy provides that a formal, documented change control policy is essential to effectively managing changes to an information system.

The lack of formal, documented change control policies can result in changes being made to the system without formal approval, user acceptance, and management awareness. Agency management indicated the processes in place have been there for some time and no policies have ever been developed. Management also stated they were considering a review of change management processes but had not yet completed a review.

Recommendation #3

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

Change Management Lacks Segregation of Duties

One of the most important tools for prevention of unauthorized changes to an information system is segregation of duties among users. Segregation of duties is the process of assigning responsibilities for various steps in system changes among a number of separate users. Such segregation allows for the verification of completion of each step in the change control process and prevents a single user from making undetected changes to the system.

Conflicting Duties Assigned to Users

The SVOR database employs the use of delivered generic user accounts. These accounts are essentially superuser accounts which the department uses to perform key functions such as systems maintenance. However, DOJ database administrators (DBAs) have access to these accounts through the use of a single, shared password. The use of generic accounts with a single, shared login decreases accountability. DOJ employs compensating controls, including database auditing tools which record all data and structural changes, to ensure the superuser accounts are not used improperly. However, the lead SVOR DBA is the primary user of these accounts and is responsible for monitoring results through the auditing tool.

In addition, we noted the lead programmer for the SVOR system is also the person responsible for moving all programming changes to the SVOR production environment. The lead programmer also has the responsibility to monitor such changes to the SVOR system.

Programmers and DBAs with access to move changes directly into the production environment could potentially make unauthorized changes. Additionally, such access could allow them to bypass user acceptance testing processes and insert changes into the production environment that could change or damage the system. Lastly, since these individuals are also tasked with monitoring changes, there is potential that a single individual could develop changes, insert them into the production environment, and strike or alter any record of the changes, thus making it difficult to determine what changes were made and by whom.

State policy requires organizations to separate duties of individuals, document segregation of duties, and implement segregation of duties. Additionally, organizations should ensure that users performing activities in the system are not the same individuals with access to the monitoring functions of the system.

The Department of Justice does not have a formal, documented policy for access control and monitoring. Management stated the current process has been in place for some time. While the department indicated it was exploring changes to its process for granting access, the department has not made the implementation of segregation of duties a priority.

Recommendation #4

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

Chapter V – Integrity of Offender Data

Introduction

Data integrity gives users assurance that information is trustworthy. The Sexual or Violent Offender Registry (SVOR) system plays a key role in the tracking and management of sexual and violent offenders. Given its important role in public safety and informing law enforcement and members of the public on the whereabouts of offenders, data integrity is critical. We reviewed data input, system processing, and data output for data integrity.

Registration Process

According to §46-23-504, MCA, offenders convicted of certain violent offenses and any sexual offenses are required to provide specific information to the Department of Justice (DOJ). Offenders who are initially incarcerated are not required to register until ten days prior to their release. Those who are not incarcerated must register within three days of sentencing at the local registering entity (city police department or county sheriff's office) where they reside. Registration forms are then forwarded to DOJ for entry into the registry.

SVOR Website

Information considered public is updated on the SVOR website five days per week. Each day the website is updated the system generates an extract of public offender information from the registry and transmits the data to the website. We reviewed the extract process to determine if controls are in place to ensure the extract occurs as scheduled and is secure. Our work did not identify any concerns with the extract process.

Conclusion

Based on our audit work, we conclude controls are in place to ensure the website update process occurs as scheduled and is secure.

Periodic Verification

After an offender initially registers, they are subject to periodic verification depending on their status. Sexual offenders are assigned a tier level based on their likelihood to reoffend. Violent and Tier I sexual offenders must verify their address annually, Tier II sexual offenders every 180 days, and Tier III sexual offenders every 90 days. We performed audit work to ensure the SVOR system automatically monitors the status of offenders once they enter the system to assure compliance with these requirements.

The SVOR system records the original registration date for each offender and their offender type and tier level (for sexual offenders). Using this information the system determines when an offender must verify their address through completion of an annual verification letter (AVL) regardless of verification period. When offenders are due for verification, the system notifies DOJ staff and identifies all offenders due to verify and generates AVLs to be sent to offenders and their local registering entity.

Conclusion

Based on our audit work, we conclude the SVOR system automatically identifies the registration status of offenders for internal users.

Annual Verification Monitoring

The system notes the date AVLs are sent. DOJ staff then monitors the system for the return of the AVL. Once an offender returns the AVL, it is noted in the system and the clock reset for the next update period. However, if the offender fails to return the AVL within 15 days, they are identified as overdue by the system. This information is provided to local law enforcement upon request; however, it is not routinely distributed.

Overdue Offenders Are Not Flagged

According to §46-23-507, MCA, a sexual or violent offender who knowingly fails to register, verify registration, or keep registration current may be sentenced to a term of imprisonment of not more than 5 years or may be fined not more than $10,000 or both. The process employed by DOJ for offenders to verify registration is the AVL process. However, department personnel stated that offenders who fail to submit their AVL within 15 days are not flagged in such a way that makes their nonverified status available to law enforcement or the public. The department stated they will only change status when they are asked to do so by local law enforcement. An option would be for the agency to add a "not verified" flag in the SVOR.

We queried the SVOR database to identify all active offenders who are 15 or more days overdue on returning their AVL. We identified any offender who had not verified their address and were not flagged in the registry. At the time of our query, there were 4,964 total offenders who were active in the registry. Of those, we identified 1,289 offenders who had not verified their address and were not flagged in SVOR. This represents nearly 26 percent of the total registered active offender population. Table 2 provides a breakdown between sexual and violent offenders who had nonverified addresses.

Table 2

Nonverified Sexual and Violent Offenders

As of March 2011

Category	Number Not Verified	% of Total Not Verified	% of Total Population
Violent	858	66.6	17.3
Sexual or Sexual/Violent	431	33.4	8.7

Source: Compiled by the Legislative Audit Division from Department Records.

Table 3

Nonverified Sexual Offenders by Tier Level

As of March 2011

Category	Number	% of Total Nonverified Offenders
No Tier*	266	20.6
Tier I	63	4.9
Tier II	77	6.0
Tier III	25	1.9

*Pre 1997 Convictions

Source: Compiled by the Legislative Audit Division from Department Records.

Table 4

Amount of Time Nonverified

As of March 2011

Category	Number	% of Total Nonverified Offenders
1 Month or Less	293	22.7
2 Months	205	15.9
3 Months	105	8.1
4 Months	79	6.1
5 Months	56	4.3
6 to 12 Months	460	35.7
13+ Months	91	7.1

Source: Compiled by the Legislative Audit Division from Department Records.

Because sexual offenders are categorized by their likelihood to reoffend, we further evaluated the 431 nonverified sexual offenders. Table 3 details our work based on tier level, including 25 Tier III offenders who are considered the most likely to reoffend.

Next, we evaluated all nonverified offenders based on the number of months overdue. Table 4 details our work, including 551 offenders who are six months or more overdue.

Of the 4,964 active offenders in SVOR, 11 percent are more than six months overdue in returning their AVL and not flagged as such in the SVOR system. When members of the public access the website or law enforcement queries data, they will not be aware of the offender's failure to verify their registration. Therefore, they may not be aware of the offenders actual location.

Agency management asserts flagging all nonverified offenders in the SVOR system would lead the public and law enforcement to question the data in the registry since such a large number have not verified their registration. Additionally, the department stated they are often aware the offender actually resides at the address recorded in SVOR regardless of whether or not the offender has returned the AVL. However, statute clearly states the offender must verify registration and state policy places responsibility for ensuring the accuracy of data in SVOR with the agency. This includes indicating when offenders have failed to verify their registration.

Deceased Offenders Still Active

As another test of the integrity of data, we queried the system to identify any offenders still listed as active who are deceased. We compared all active offenders in the registry against a list, provided by the Department of Public Health and Human Services, Office of Vital Statistics, of Montana residents who died from 2007 to 2010. Our results indicated there were seven active offenders in the system who are deceased.

Department personnel stated they do not perform any routine checks to identify deceased offenders in the registry. Generally these offenders are identified by family, friends, or local law enforcement. The department indicated it will inactivate the offender once they receive proof the offender is actually deceased.

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.*

Department of Justice

Department Response

ATTORNEY GENERAL
STATE OF MONTANA

Steve Bullock
Attorney General

Department of Justice
215 North Sanders
PO Box 201401
Helena, MT 59620-1401

June 6, 2011

Tori Hunthausen
Legislative Auditor
Legislative Audit Division
PO Box 201705
Helena MT 59620-1705

Dear Tori:

The Department of Justice thanks your audit team for their professionalism while conducting this Information Systems audit. The audit provides valuable and timely information for us to evaluate our Sexual or Violent Offender Registry and information systems.

Following are the responses to the audit recommendations presented in your audit report dated May 10, 2011:

Recommendation #1

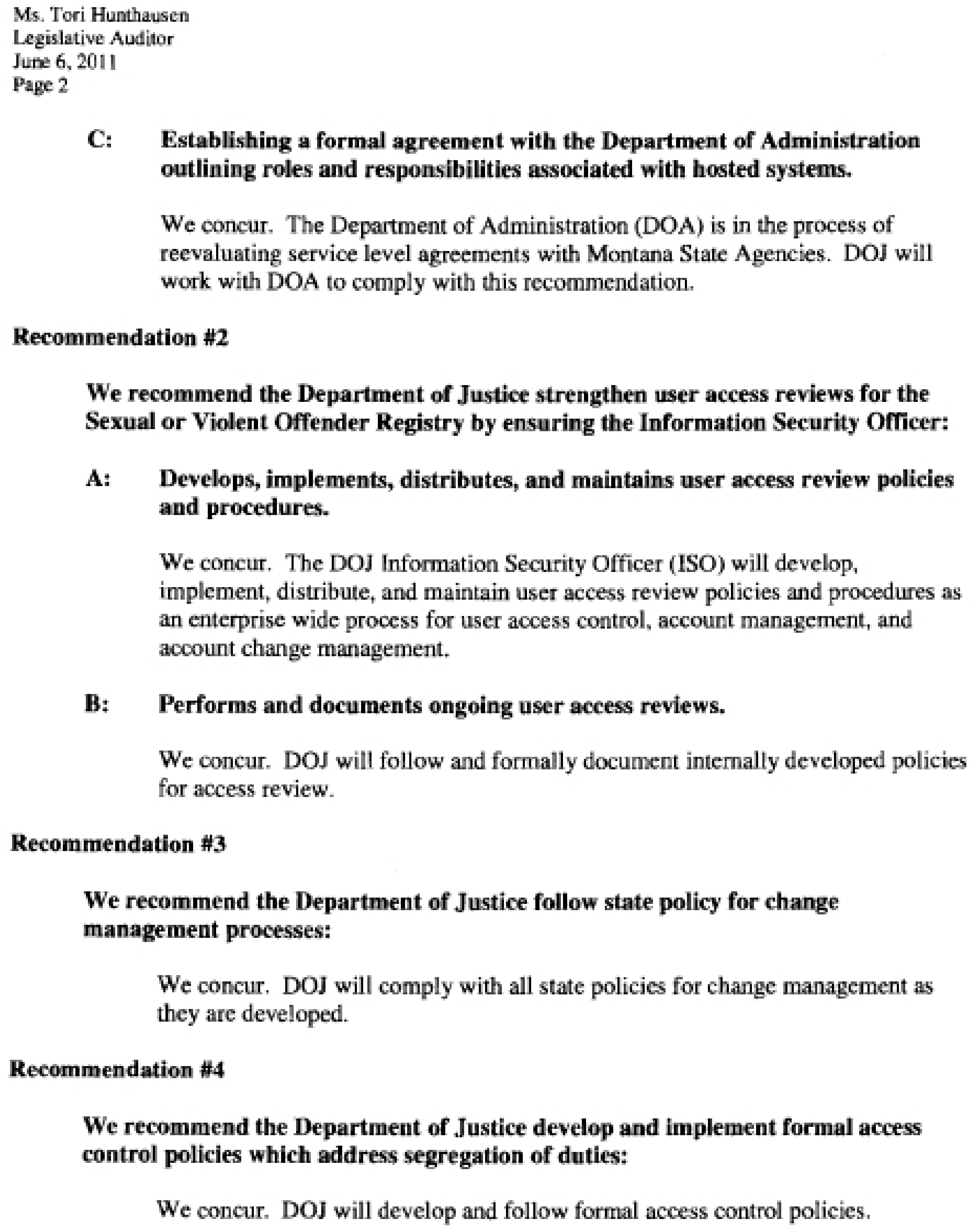
We recommend the Department of Justice strengthen system access controls for the Sexual or Violent Offender Registry by:

A: Developing, documenting, and executing a process to add, remove, or change system access.

We concur. The Department of Justice (DOJ) will develop, document, and execute internal processes to add, remove, or change system access on an enterprise level for all information systems, including SVOR, for the purpose of strengthening system access controls.

B: Developing, documenting, and executing regular system access reviews.

We concur. Following National Institute of Standards and Technology (NIST) guidelines, DOJ will work with information system owners to ensure, as part of a robust security plan, regular system access reviews are executed.



Ms. Tori Hunthausen
Legislative Auditor
June 6, 2011
Page 2

C: Establishing a formal agreement with the Department of Administration outlining roles and responsibilities associated with hosted systems.

We concur. The Department of Administration (DOA) is in the process of reevaluating service level agreements with Montana State Agencies. DOJ will work with DOA to comply with this recommendation.

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.

We concur. The DOJ Information Security Officer (ISO) will develop, implement, distribute, and maintain user access review policies and procedures as an enterprise wide process for user access control, account management, and account change management.

B: Performs and documents ongoing user access reviews.

We concur. DOJ will follow and formally document internally developed policies for access review.

Recommendation #3

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

We concur. DOJ will comply with all state policies for change management as they are developed.

Recommendation #4

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

We concur. DOJ will develop and follow formal access control policies.

Recommendation #5

We recommend that 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.

We concur. The Department of Justice (DOJ) will designate offenders who fail to verify their current address as non-compliant. The DOJ will also continue to work with local law enforcement and prosecutors to locate and prosecute non-compliant offenders.

B: Developing a routine process to compare active offenders against death records.

We concur. The DOJ will develop a process to compare active offenders against death records.

C: Inactivating offenders who match deceased records.

We concur. The DOJ will work with local law enforcement agencies to ensure that documentation of an offender's death is received, reviewed by the SVOR unit, and used to inactivate offender records.

Sincerely,

STEVE BULLOCK
Attorney General

SB:sj

c: File