A Report
to the
Montana
Legislature

Information Systems Audit

Security and Maintenance of Montana Election Systems

The Office of the Secretary of State

August 2020

Legislative Audit
Division

19DP-06

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.

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.

Audit Staff

Miki Cestnik
Amanda Sayler
T. Shane Somerville

Reports can be found in electronic format at:
https://leg.mt.gov/lad/audit-reports

LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
Joe Murray

August 2020

The Legislative Audit Committee
of the Montana State Legislature:

This is our information systems audit of the Security and Maintenance of Montana Election Systems managed by the Elections Division of the Office of the Secretary of State (SOS).

This report provides the Legislature information about the management of Montana's election process, election security, and the maintenance of the voter registration list. This report includes recommendations for defining and enhancing election security and developing quality assurance programs. A written response from SOS is included at the end of the report.

We wish to express our appreciation to SOS personnel for their cooperation and assistance during the audit.

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

Table of Contents

Figures and Tables iii
Elected, Appointed and Administrative Officials iv
Report Summary S-1

CHAPTER I – INTRODUCTION 1
Introduction 1
Voter and Election Day Process 1
Election Security 3
Resources and Funding for Election Management in Montana 4
Audit Objectives 4
Audit Scope 4
Audit Methodologies 5
Report Contents and Limitations on Reported Information 6

CHAPTER II – ELECTION SECURITY OVERSIGHT 7
Introduction 7
Multiple Guidelines and Best Practices Exist for Election Security 7
Montana Election Security Oversight and Management 8
Law Defines Authority and Responsibility for Election Security 9
Consistent Security Administration Is at Risk With Current Laws 9
Montana Law Needs to Further Define Security and Establish Consistent Assessments 10
Counties Need More Security Guidance Through Rule 10
Rule Needs to Be Consistent With Statute in Definition of Voting System 11
Election Security Improvements Require Consistency and Guidance Through Rule 11

CHAPTER III – ELECTION RESOURCE GRANT MANAGEMENT 13
Introduction 13
Success of All HAVA Grant Objectives Is Unclear 14
Grant Management Best Practices and Prior Federal Guidance Exist to Assist SOS 15
SOS Is at Risk for Not Meeting Future HAVA Goals and Desired Outcomes 15
Potential Legislative Oversight Opportunities 16

CHAPTER IV – SECURITY MANAGEMENT 19
Introduction 19
Agency-Wide Security Posture Is Important to Election Security 19
Security Oversight Is Not Assigned to a Single, Independent Management Position 20
Vacant Security Manager Position Should Be Filled 20
SOS Can Improve Managing Election Security Risks 20

CHAPTER V – VOTER REGISTRATION DATA ACCURACY AND MAINTENANCE 23
Introduction 23
Voter Registration Management and Responsibilities for Updating Voter Status 23
Voter Registration Status Changes 24
System Classifications and Tracking of Voter Status Changes 24
Voter Registration Analysis Identifies Delayed Status Changes 25
Voter Status Changes Need Follow-Up to Ensure Timeliness 26
NVRA Process Is Not a Primary Control for Updating Deceased Voter Records 27

Untimely Updates to Voter Registration Increases Risk of Inaccurate Statuses.....28
A State-Level Maintenance Program Is Needed for Increased Voter Registration Accuracy ...29

OFFICE RESPONSE
The Office of the Secretary of State A-1

Figures and Tables

Figures

Figure 1 Technology That Supports Montana Election Process 2

Tables

Table 1 States That Administer and Oversee HAVA Grant Dollars That Differ From Montana..... 17

Table 2 Number of Potentially Deceased Voters That Have Not Been Cancelled by Year of Death..... 26

Table 3 Time Elapsed for Status Cancellation of Deceased Voters 27

Elected, Appointed and Administrative Officials

Office of the Secretary of State	Corey Stapleton, Secretary of State
	Christi Jacobsen, Chief of Staff
	Dana Corson, Director of Elections and Voter Services
	Stuart Fuller, Election and Voter Services Manager
	Julie Lake, Chief Operations Manager
	Kellee English, IT Manager

Montana Legislative Audit Division

Security and Maintenance of Montana Election Systems

The Office of the Secretary of State

Background

Montana Elections are managed and administered by the Office of the Secretary of State (SOS) and local officials. Each of the counties administer elections differently, while SOS is required to advise and assist them. Additionally, the state and the counties receive resources and support from the federal government.

Agency:
The Office of the Secretary of State

Secretary of State:
Corey Stapleton

Division:
Elections

This information systems audit examined whether SOS is evaluating physical security and managing election risks, including the accuracy of the voter registration database. We found that, although SOS is making improvements to elections, further definitions are required to identify scope of election security and election security measurements. SOS can also improve success of future security initiatives by updating grant management practices, with potential oversight opportunities from the legislature. SOS provides counties the tools to manage the accuracy of voter registration and status changes, but our work found that SOS is not conducting state-level maintenance procedures where it is most efficient. These are needed to ensure changes are made in a timely manner and to identify potential training, system, or process improvements.

KEY FINDINGS:

Statute and rule do not define the scope of election security or align with best practices. Due to the decentralized management of elections, counties need a consistent definition of security and a formal security assessment process. Current law lacks clarification of election security and rule does not specify security measures.

Management of federal grants do not align with best practices. SOS does not have performance measurements in place as outlined in grant management best practices. SOS does not have any controls in place to ensure federal grant funding is being used to meet objectives and goals of the grant.

SOS does not have an Information Security Manager position to oversee all divisions within the department. Since 2017, SOS has had a vacant Information Security Manager position that is necessary to independently oversee all aspects of security within an agency, including election security.

The department does not have a state-level maintenance program in place to ensure accuracy and timeliness of voter registration statuses. SOS relies on the county election administrators to update their residents voter status. Although SOS provides the resources and information, they are not verifying that status updates have occurred within a timely manner.

(continued on back)

For the full report or more information, contact the Legislative Audit Division.

leg.mt.gov/lad

Room 160, State Capitol
PO Box 201705
Helena, Montana 59620
(406) 444-3122

The mission of the Legislative Audit Division is to increase public trust in state government by reporting timely and accurate information about agency operations, technology, and finances to the Legislature and the citizens of Montana.

To report fraud, waste, or abuse:

Online
www.Montanafraud.gov

Email
LADHotline@mt.gov

Call
(Statewide)
(800)-222-4446 or
(Helena)
(406)-444-4446

Text
(704) 430-3930

RECOMMENDATIONS:

In this report, we issued the following recommendations:
To the office: 4
To the legislature: 1

Recommendation #1 (page 10):
Using industry standards and best practices, the Montana Legislature should define the scope of election security and mandate assessments at the local levels.
Office response: Concur

Recommendation #2 (page 12):
SOS should align the definition of election security within rule with statute and provide further guidance on necessary security measurements.
Office response: Concur

Recommendation #3 (page 16):
SOS should enhance the grant management program, including implementing measurable objectives, goals, and timelines while ensuring ongoing evaluation is occurring to measure success.
Office response: Concur

Recommendation #4 (page 21):
SOS should fill the vacant Information Security Manager position to ensure both election security and agency-wide security have consistent, independent, and comprehensive oversight.
Office response: Concur

Recommendation #5 (page 30):
SOS should implement between a state-level maintenance program to address timeliness and verification of voter status updates in the voter registration database.
Office response: Concur

Chapter I – Introduction

Introduction

The administration of elections in Montana is decentralized and relies on cooperation and collaboration between state and local governments. At the state level, the Office of the Secretary of State (SOS) is responsible for maintaining the uniform application, operation, and interpretation of election laws. At the local level, counties are responsible for the execution of elections, including maintaining voter registration information, issuing ballots, running polling places, and ensuring voting systems are secure within their jurisdiction. In many counties, an elected official is responsible for elections administration. Each county is also required to provide voter accessibility and outreach.

The focus of this information systems audit is the administration and security of those aspects of elections and voting that depend on technology systems and processes. Security responsibilities for elections are managed at multiple levels, with various entities supporting SOS. For example, because the state's voter registration list is housed in the Montana Data Center, ensuring cybersecurity over registration data is a shared responsibility of the State Information Technology Services Division (SITSD) and SOS. Additionally, because of heightened federal involvement in issues relating to elections security, SOS works in conjunction with federal Department of Homeland Security (DHS), the Montana Department of Justice (DOJ), and the National Guard (NG) to ensure lines of communication remain open and incident responses are clear. DHS also performs various risk assessments, vulnerability testing, identifying issues and making recommendations regarding voter registration cybersecurity improvements.

Voter and Election Day Process

Since elections are conducted at the county level, elections can be administered differently depending on the population and resources of the county. Examples of these differences specific to the technology aspects of elections include:

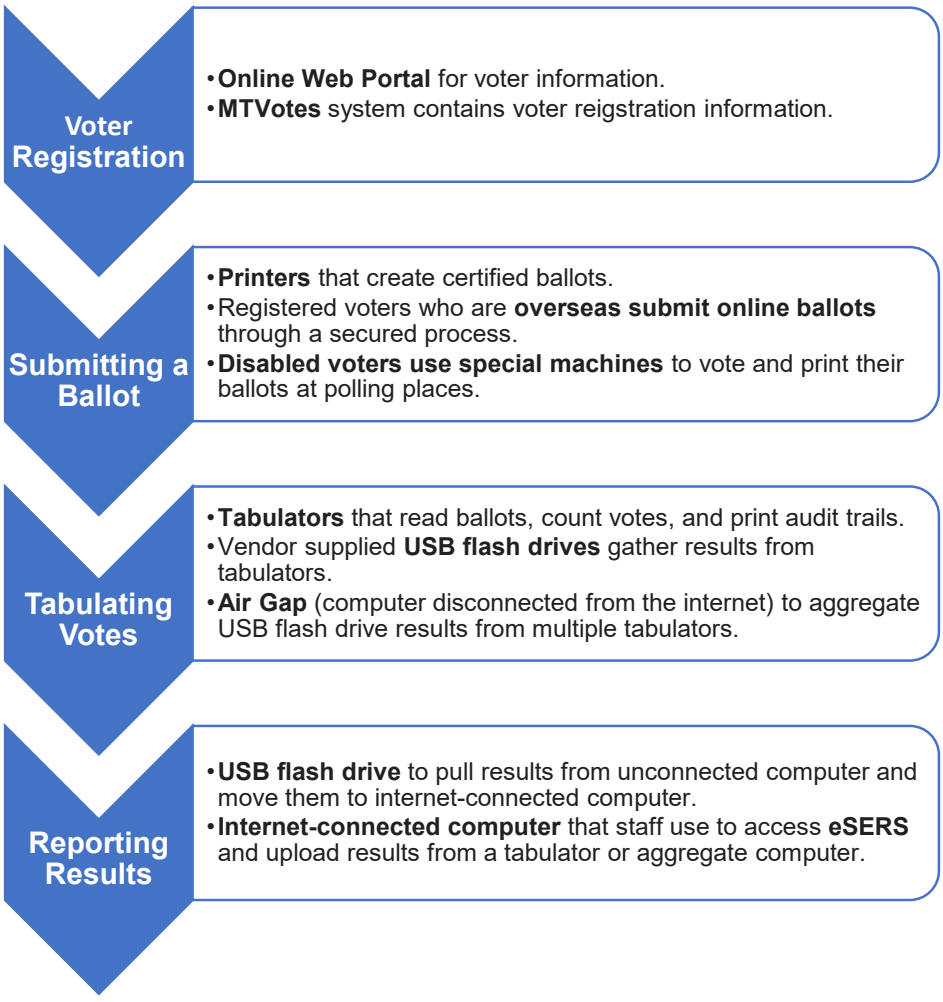
- More populous counties have an information technology (IT) office with dedicated staff, whereas less populous counties contract out for IT services.
- There are 11 counties that only use hand-counted paper ballots, which are considered the most secure form of voting. However, in counties with higher populations, this is not a viable option and voting tabulator machines and associated systems are used. These tabulators and associated components are provided and managed by an election systems vendor.

These differences can change details of the election process and the controls needed to ensure security. However, the overall election process remains the same.

The first step in the election process requires voters to register. The statewide voter registration list, or MTVotes, contains the record of every registered voter in the state. On election day, election administrators use voter registration data to prepare a precinct register for each precinct in the county. This list contains vital information on each voter to ensure that the correct ballots are given to the correct individuals. If there are issues that arise on election day, Montana allows for provisional ballots to be submitted.

Once voters are registered and election day preparedness is complete, counties execute election day process as outlined below.

Figure 1
Technology That Supports Montana Election Process



Compiled by the Legislative Audit Division.

Once the polls close on election day, votes are counted, aggregated, and uploaded to Electronic Statewide Election Reporting System (eSERS) by the counties for the published final counts. This is the system that collects all election results from each county and reports those results to the public.

The election process is dependent on technology, including tabulators that count individual ballots, USB flash drives that transfer counts between air gap computers and standard internet connected computers, specialized printers, and the election night reporting through eSERS. Based on the county size, some of these tools are used, and some are not. For example, the less populous counties hand count votes and therefore do not require the use of tabulator technology. Some counties only have one tabulator so they would not require the use of an air gap computer. However, each county is required to enter official results into eSERS.

Montana voters can also vote via absentee ballot if they request this type of ballot when registering. This allows a voter to receive a ballot via mail and was the official form of voting for the June 2020 primary elections. The voter fills out the ballot, puts it in a secrecy envelope, and puts the secrecy envelope in a return envelope. The voter signs the return envelope, which is sent to the county election office for processing. Although the absentee voting process differs in ballot distribution and collection, the use of election technology remains the same.

Election Security

In 2018, US elections were designated as critical infrastructure due to events of the 2016 election. According to the Department of Justice, "The Russian government interfered in the 2016 presidential election in a sweeping and systematic fashion." Given the vital role elections play in the country and the recent attacks, the Department of Homeland Security prioritized elections in order for states to receive the support and resources for defense of election infrastructure. DHS views election foreign interference as "malign actions taken by foreign governments or actors designated to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interest of the United States and its allies."

In recent years, election security standards have been reviewed and updated due to these events. Federal guidelines, best practices, industry standards, and election security controls all exist to assist and guide states in implementing election security controls. Federal guidelines, best practices, and industry standards related to election security controls align with NIST standards. These standards include all facets of security including physical security and governance of security risks. Federal guidance

and state law also clearly require security of election systems before, during, and after elections. A key component in maintaining security over election systems before, during, and after elections is physical security of election assets, like voting tabulators and ballots.

Resources and Funding for Election Management in Montana

Currently, Montana elections are funded through federal grants, fees, and services. SOS's total budget for the 2021 biennium is $12.8 million. SOS's Elections Division has a budget of $1.1 million. Revenue is received from fees charged to businesses, corporate filings, and registration for names and trademarks. Additionally, they collect fees from state agencies and users of administrative rules, storage and management of public documentation, election candidate filing, and citizens seeking to be notaries.

Audit Objectives

Our audit objectives were to:

- Determine if the Office of the Secretary of State is evaluating physical security and managing election security risks in accordance to state statute, industry standards, and federal guidelines.
- Determine if the Office of the Secretary of State is keeping voter registration information current and accurate according to statute.

Audit Scope

Audit scope was developed to address how SOS ensures the accuracy and security of elections held in Montana. This includes testing governance over voter registration accuracy, physical security of voting systems, and whether SOS is effectively managing risk at the county and state levels.

Based on our review of county security programs, we focused on assessing ten counties for physical security of election systems. The ten counties assessed represented low, medium, and highest populated counties prior to the June 2, 2020, primary election.

We also focused on Help America Vote Act (HAVA) county sub-grant expenditures. The primary objective of the federal grant is to increase election security, so we evaluated potential improvements to future HAVA expenditures that address the highest security risks at the counties.

Audit scope excluded responsibilities shared with State Information Technology Services Division, Department of Homeland Security, National Guard and other

federal and state stakeholders. A structure for communication and controls are in place to ensure MTVotes is protected. Finally, we excluded the impact of mail-in voting due to the COVID-19 pandemic because the technologies to support mail-in voting does not change.

We also analyzed the effectiveness of the maintenance of MTVotes by SOS. We collected the last five years (2015-2020) of status updates from MTVotes. We reviewed the status updates from one year prior to the most recent presidential election up through April 2020. We also took this data and matched it with data from external sources to determine how long it takes to update voter registration information.

Audit Methodologies

- Reviewed assessments, risk analyses, policies, and procedures regarding election security, and voter registration maintenance.
- Reviewed other state's administration of HAVA expenditures.
- Researched election administration methods and best practices used by other states and government entities.
- Conducted observations at county election offices.
- Defined criteria using:
    - ◊ National Institute of Standards and Technology (NIST): A nonregulatory government agency that develops commonly used security standards and controls for federal agencies. NIST standards are based on best practices from several security documents, organizations, and publications. Federal election security recommendations stem from NIST standards.
    - ◊ Federal election security best practices: These best practices were gathered from the Election Assistance Commission, Department of Homeland Security, Department of Justice, and Cybersecurity and Infrastructure Security Agency.
    - ◊ Montana statute and rule.
    - ◊ Federal statute and regulations.
- Conducted a comprehensive comparison between criteria and county observations of security programs at both the state and county levels.
- Compared and analyzed voter registration data with information provided from Department of Public Health and Human Services (DPHHS) and Department of Corrections.
- Conducted interviews with federal, state, and county officials.
- Assessed county administration of elections through a survey covering security resources, security awareness, voter registration management, and IT infrastructure, management, policies, and procedures. The survey was

sent to 47 counties, excluding those that hand count ballots. Thirty-three counties responded with a 64 percent completion rate.

- Assessed the SOS management of election and agency security risks.

Report Contents and Limitations on Reported Information

The remainder of this report contains findings, conclusions, and recommendations intended to assist SOS in improving election security and accuracy. Certain information regarding election security has been omitted from this report. The information could be used by malicious actors to undermine election security and voter confidence. Critical findings were discussed with SOS.

The report is organized into four additional chapters:

- Chapter II addresses improvements to election security administration.
- Chapter III addresses improvement to future HAVA spending, with an option for legislative oversight.
- Chapter IV explains the importance of having an Information Security Manager to oversee SOS security and provide a clear separation of duties between election security staff and the overall agency security posture.
- Chapter V discusses our analysis of voter registration statuses and the timeliness of status updates.

Chapter II – Election Security Oversight

Introduction

Democracy depends on the perception of accurate and secure elections. The physical security over elections needs to be in place because the risks of insider and external threats may impact the public's trust in elections. Additionally, without these protections in place, there is also risk of inaccurate counts that may not be detected but could still affect the outcome of the election.

Sound election security cannot be accomplished by any one entity acting alone. All stakeholders, including voters, need to work together to ensure democracies are protected. This includes sharing credible information, establishing best practices, and developing a coordinated effort to mitigate risks. In Montana, this means the Office of the Secretary of State (SOS) must be able to work with multiple federal, state, and local government entities to ensure the security of elections. This chapter reviews election security in regard to local government election processes.

Multiple Guidelines and Best Practices Exist for Election Security

Security can include, but is not limited to, information security, cybersecurity, and physical security. Multiple entities provide guidance for the general areas of security. We reviewed National Institute of Standards and Technology (NIST), Election Assistance Commission (EAC), Department of Homeland Security (DHS), Center for Internet Security (CIS), and Department of Defense (DOD) federal guidelines and best practices, as well as vendor material specific to voting systems used in Montana.

NIST Industry Standards: Within election resources provided by various areas of government and private sectors, the most referenced security framework to follow is NIST. For example, federal election grant language outlines NIST standards to be used in continuing review of election security. Although NIST does not discern the definition of information security, cybersecurity, or physical security, all three areas are included in the NIST cybersecurity framework. Therefore, the definition of security is not limited to only network and information security, but also includes physical security.

Federal Guidance and Best Practices: The EAC, CIS, DHS, DOD, and their subsidiary departments provide definitions and controls on what security of elections entails. They also provide recommendations for increasing security; however, states and

jurisdictions are not required to implement them. The EAC groups election security into several components:

- Election workers
- Election night reporting
- Contingency planning
- Voter registration
- Mail ballots
- Election equipment

CIS provides even more detail on what constitutes election security. They classified election assets and components into three classes:

- Network connected systems and components – These components are interconnected with other devices such as election night reporting and voter registration systems.
- Indirectly connected systems – These components are not connected to a network at any time and are not persistently connected to other devices. These components exchange information with other elections systems. The information exchanges are done through USB drives or a direct connection.
- Nondigital election components – These include paper-based voting and mail-in processes.

Election Vendor Guidance: The vendor that supplies the voting materials also highly recommends users to implement physical security procedures and measures that limit access to the equipment.

Each of these classes have detailed information on securing these voting systems and their technology assets. They are necessary in conducting elections and therefore require the same attention as other security areas, such as network security or information security.

Montana Election Security Oversight and Management

Currently, SOS examines and approves the voting system, which is defined as any machine, device, technology, or equipment used to automatically record, tabulate, or process the vote. Per statute, the examinations are only required for newly purchased systems and only ensure voter interface devices meet electronic security standards. SOS is required by statute to ensure that at least 10 percent of all voting systems have been randomly tested once per year. County election administrators are also required to publicly test voting systems used in an election at some point within 30 days of an election. Election day testing of voting systems is also required, as is a post-election audit of voting systems where tabulated results are compared with a randomly selected

hand recount of ballots. Although these measures ensure that votes are being counted correctly, they do not address the security of the entire voting system.

Law Defines Authority and Responsibility for Election Security

When evaluating Montana election security, we first identified the current statute defining responsibilities and authority. Sections 13-1-202 and 13-1-201, MCA, imply that security is the responsibility of SOS in order to maintain uniformity in the application and operation of election law. SOS has the authority to gather data from the counties that is necessary to:

- Evaluate the security, accuracy, and accessibility of elections.
- Assist in making recommendations to improve voter confidence in the integrity of the election process.

According to §§13-17-103 and 13-17-211, MCA, SOS is also required to develop rules that outline and require:

- Protections against fraudulent tampering of voting systems.
- Addressing security measures necessary to secure voting systems before, during, and after an election.

Consistent Security Administration Is at Risk With Current Laws

While requiring SOS to establish rule that identifies "the security measures necessary to secure the voting system before, during, and after an election," current law does not give enough direction to SOS on what areas of security these measures need to address. If the intent of the legislature is to ensure that security is maintained before, during, and after the election, the type of security required needs to be outlined in law. It is important to clarify this because not all technology assets require the same type of security or security standards. For example, some technologies are not connected to any network, so network security does not apply to these assets.

Consistent assessment of these technologies and risks also needs to be mandated. As technologies change and risks evolve, consistent assessment is important to ensure the security of all election assets are maintained at an acceptable level. Section 13-1-202, MCA, states that election administrators shall provide SOS information that SOS determines is necessary to evaluate the performance of voting systems and security, accuracy, and accessibility of elections. Giving SOS the ability to determine what information is necessary to assess security without defining what security is necessary has created risks in the administration of election security.

Our work reviewed physical security of elections and technology assets, such as tabulators, USB flash drives, the air gap computer (disconnected from the internet), and internet-connected computers. Our observations at various counties showed that these standards were not met consistently. While this indicates risks exist, it does not indicate where risks have been exploited. Our work identified physical security risks that are not addressed through any oversight procedure related to ensuring the security of elections.

Montana Law Needs to Further Define Security and Establish Consistent Assessments

While approvals and certifications of voting machines are described in law, there is no clear outline of the types of security needed for other important technology assets and their security outside of election day. If security risks are not addressed, tampering and interference in elections becomes easier, which ultimately undermines public trust in the election process.

Law can ensure there are clear definitions of election security scope based on industry standards and election security guidance. Law can also provide requirements ensuring the most critical form of election security protocols are in place and mandate a consistent assessment of these protocols to mitigate high risks at all levels of elections in Montana.

RECOMMENDATION #1

We recommend the Montana Legislature:

A. *Clearly define the scope of election security using federal election security best practices and National Institute of Standards and Technology security controls to ensure all aspects of elections are secure, and*

B. *Mandate the assessment of election security using defined security standards at the local and state levels.*

Counties Need More Security Guidance Through Rule

While the first recommendation suggests law define the type of security needed for elections and mandate the assessment of security, rule is needed to provide a more detailed look at how those types of security apply to the election process. Our review identified this as an additional cause contributing to security standards not being met at counties.

According to §13-17-211, MCA, SOS shall adopt rules that, at the minimum, must address security measures necessary to secure voting systems before, during, and after an election. ARM 44.3.1713 indicates that voting systems must apply security measures necessary to secure voting systems before, during, and after an election. The rule does not specify the security measures or provide guidance on what security entails.

Using federal guidelines and best practices discussed above, SOS can adopt rules clarifying election security measures. This should include physical security of voting technology assets, such as tabulators, USB flash drives, and various computers. This would assist counties in understanding what is necessary for securing voting systems before, during, and after an election.

Rule Needs to Be Consistent With Statute in Definition of Voting System

Section 13-1-101, MCA, defines voting system or systems as "any machine, device, technology, or equipment used to automatically record, tabulate, or process the vote of an elector cast on a paper ballot." Based on federal guidance and best practices, statute aligns with commonly accepted definitions. ARM 44.3.1701 provides the only relevant definition for voting machines and devices:

- ARM 44.3.1701(2)(h) "Marking device" means any approved device for marking a paper ballot with ink or other substance which will enable the ballot to be tabulated by means of automatic tabulating equipment.
- ARM 44.3.1701(2)(i) "System" includes a self-contained mechanical voting machine or an electronic voting device and the individual components of each.
- ARM 44.3.1701(2)(j) "Voting machine" means a mechanical apparatus on which to cast votes.

A voting system is based on the definition of the voting machine and its components. The voting machine only includes the machine used to mark the ballot, not tabulate and process the votes. Therefore, voting systems by ARM definition do not include all necessary assets and needs to be aligned with statute.

Election Security Improvements Require Consistency and Guidance Through Rule

SOS can further clarify through rule what security standards, requirements, reviews, and assessments should be used by counties. It is clear that definitions on voting systems are inconsistent and management of election security lacks guidance, specifically concerning physical security. Rule language does not provide enough detail to effectively secure election systems, including physical security over election assets.

SOS is required to ensure counties meet security measures. Due to the decentralized approach to election security measures, it is important to outline in rule the security measures necessary to secure voting systems before, during, and after an election that statute requires. When determining the security measures, SOS needs to consider the level of application in terms of county resources and size. For example, not every county requires security guards and surveillance cameras, but counties should have controls in place for surveillance of critical election assets. This level of guidance allows counties to determine the resource appropriate controls for their individual jurisdictions.

RECOMMENDATION #2

We recommend the Office of the Secretary of State develop rules that:

A. *Define voting system consistently with statute.*

B. *Include detailed security measures that align with statute, election best practices, National Institute of Standards and Technology security controls, and federal recommendations.*

Chapter III – Election Resource Grant Management

Introduction

Since 2018, Montana has received $6.1 million in Help America Vote Act (HAVA) grant funding with additional county matching of $775,596. The grant originated in 2002 to implement extensive reforms to the voting process across the US including creating a federal agency, Election Assistance Commission (EAC), serving as the clearinghouse for elections. The grant also requires states to follow minimum standards in several key areas of election administration, including certifying voting equipment and maintaining voter registration lists. The grant serves as a significant resource for state and local officials, so receiving grants requires states to submit a brief narrative to EAC on how the state intends to use the funds. The grant objectives established by EAC include:

1. Replacing voting equipment that only records a voter's intent electronically with equipment that utilizes a voter-verified paper record.
2. Implementing a post-election audit system that provides a high level of confidence in the accuracy of the final vote tally.
3. Upgrading election-related computer systems to address cyber vulnerabilities identified through Department of Homeland Security (or similar) scans, and assessments of existing election systems.
4. Facilitating cybersecurity training for the state chief election official's office and local election officials.
5. Implementing established cybersecurity best practices for election systems.
6. Funding other activities that will improve the security of elections for the federal office.

In 2018, the Office of the Secretary of State (SOS) and the counties determined implementing a new voter registration system would accomplish much needed technology and security improvements, as required by HAVA grant stipulations. Approximately $2.15 million of the grant was allocated for this new system. Other grant spending initiatives included:

- $250,000 for security services and personnel within SOS to manage aspects of elections security. This includes county security assessments and an Elections and Voter Services Manager position.
- $750,00 for counties to use at their discretion, as long as they provide a narrative on how the funds will be used and how much will be needed to achieve their objectives in that county.

During the fieldwork phase of this audit, SOS received additional federal funding as part of the 2020 HAVA grant. Decision-making regarding the use and distribution of the 2020 grant was still active while we were conducting fieldwork, so we did not analyze this funding, but SOS was able to provide the following description of anticipated uses:

- $1.9 million for counties to use at their discretion, as long as they provide a narrative on how the funds will be used and how much will be needed to achieve their objectives in that county.
- $200,000 to conduct security risk assessments through an agreement between SOS and the Montana National Guard.
- $1 million in administrative and indirect costs that include personnel costs associated with IT security and grant administration.
- $625,596 for election administration including IT system development and specific election and voter service division activities.

Success of All HAVA Grant Objectives Is Unclear

Although SOS has followed the HAVA requirements for managing and dispersing grant dollars, current HAVA grant requirements only align with minimum election security best practices. We identified several areas where it was unclear that the objectives of the grant funding were met. For example, 2018 HAVA funding indicated spending $150,000 for various election security assessments. This situation provides an example of where grant management best practices would provide a better structure to ensure grant objectives are achieved.

- **Measurable Objectives and Goals**: While SOS indicated how they would spend the money outlined in the brief narrative, they did not provide a way to measure the success of the spending on multiple initiatives.
- **Ongoing Evaluation**: Without a measurable, specific goal for the security assessments discussed above, it is unclear if SOS should evaluate completion of risk assessments, results of risk assessments, or the impact to overall security based on the risk assessments.
- **Timelines and Milestones**: In 2018, SOS completed two MTVotes security assessments and since then only three risks assessments have been conducted at the counties by the Montana National Guard. SOS has five years from the grant date to expend money with no timelines or milestones, so it is unclear if this is the expected rate of completion for the remaining three years of this grant, or if between expectation was to complete these objectives in the final years of the grant. It is also unclear if future security assessments will be conducted as these types of assessments should happen regularly.

Another example where best practice structure would be beneficial is security awareness training. Based on survey results from counties, 13 out of 27 counties responded they either have not received training or it has been more than a year since they have received

training. According to SOS, as of March 2020, security awareness training has not been taken in 25 counties. It is clear that close to half of the county election officials may not be aware of important security controls and the risks facing elections today. If goals, timelines, and milestones had been developed, more structure would be in place to ensure counties are receiving the training according to NIST industry standards.

Grant Management Best Practices and Prior Federal Guidance Exist to Assist SOS

Grant management best practices indicate that plans for spending and allocating funding should be comprehensive to ensure grant objectives are met. Applying these best practices to county subgrants would give counties more guidance and information on determining highest priorities for expending funds. Specific best practices for grant management plans include:

- Establishing measurable performance objectives.
- Outlining tangible timelines for achieving objectives.
- Detailing information and descriptions on the use of funds that can be easily tracked.
- Communication and authority definitions.

Original federal HAVA requirements included the development of a state plan that discusses some of these best practices as well, including:

- How the state will adopt performance goals and measurements to be used to determine its success at the state and local levels.
- Timetables for meeting objectives of the grant.
- How the state will distribute and monitor the distribution of payments to counties.
- Methods used to monitor the performance of the funding distributed to counties.
- Information on fund management based on the state's best estimates of cost.

State plans are no longer required for the use of HAVA funding for election security, but the practices can still be applied for developing goals, evaluation, and timelines. While SOS has implemented some of these practices, they can enhance the current program.

SOS Is at Risk for Not Meeting Future HAVA Goals and Desired Outcomes

States have the flexibility to determine the best processes and procedures for HAVA spending as long as it meets one of the six general objectives of the federal grant.

Montana addressed the highest security risks to elections by updating systems and machines through 2018 HAVA funding. However, in Montana, SOS is not meeting grant management best practices.

The grant is a significant resource for election officials and without performance metrics and monitoring as described in grant management best practices, SOS is at risk for not meeting the objectives and desired outcomes in future spending. By updating the grant management plan with requirements to ensure performance metrics are met, future allocations of grant funding can be used to address the next highest risks at the state and local levels. This could include a process of ongoing risk assessments to identify those highest priorities and physical security measures relevant to each county.

RECOMMENDATION #3

We recommend the Office of the Secretary of State implement a detailed grant management program to be applied to future allocated Help America Vote Act funding that includes:

A. *Measurable objectives and goals for grant spending.*

B. *Ongoing evaluation and tracking of objectives and goals to ensure success.*

C. *Clear timelines and milestones to ensure funding and expenditures meet objectives and goals of the grant.*

Potential Legislative Oversight Opportunities

As discussed above, states have broad discretion in how they allocate, manage, and track federal elections funds. In the 2018 round of HAVA grant funding, many states used an oversight body, such as state legislative approval or an independent council or board, to determine how HAVA allocations were spent and tracked. Table 1 (see page 17) shows the variety of means and methods states have used in terms of the approval, oversight, and tracking of HAVA funding.

Table 1

States That Administer and Oversee HAVA Grant Dollars That Differ From Montana

State	Brief Description of Oversight, Tracking, and Spending Authority
Arizona	Legislative Budget Committee approves and oversees expenditures.
Alaska	State of Alaska Elections Division works with the Election Policy Workgroup to approve and oversee expenditures.
Colorado	Colorado Department of State in conjunction with election and information technology personnel, bipartisan Election Advisory Committee, county clerks and community representatives, and citizens oversees spending. They have provided timelines and measurables for expenditures.
Florida	The Florida Governor's Office directs the Florida Department of State on HAVA expenditures.
Kentucky	The Kentucky State Board of Elections works with Kentucky Secretary of State and the Commonwealth of Kentucky HAVA Advisory Board to ensure appropriate allocation and use of funds.
Maine	Maine Secretary of State use of HAVA funds needs to be approved by Maine Legislative representatives.
Maryland	State Board of Elections shares equal responsibility with Maryland counties and conducts annual financial and performance reports on HAVA expenditures.
Michigan	Michigan Department of State is required to seek approval of all state matches through the Michigan State Legislature. They also use Department of Management and Budget to ensure timely completion of all planned activities.
Minnesota	Minnesota Secretary of State requires State legislative and governor approval to spend HAVA funds.
Mississippi	Mississippi Secretary of State is required to seek approval of all state matches through the Mississippi State Legislature.
New York	Requires approval from the State Board of Elections Commissioners.
North Dakota	Requires approval of state legislature to appropriate funds.
Oregon	HAVA grant spending must be approved by the state legislature.
Pennsylvania	Required to submit program narratives and progress reports to a state oversight body.
Rhode Island	Rhode Island Secretary of State works in conjunction with the state legislature for approval and to determine funding priorities.
South Dakota	Requires state legislature approval for state matching funds and has a HAVA board that oversees spending.
Utah	Provide tangible timelines and measurables for the use of HAVA funds.
Wyoming	A task force including Wyoming Secretary of State, state legislators, county clerks, and county commissions provide oversight of HAVA funding.

Compiled by Legislative Audit Division using data from Election Assistance Commission.

The narrative description for each of these states represents information as reported to the federal EAC. As shown, multiple states have put in place various mechanisms to provide for the approval, oversight, and tracking of how HAVA funds are being spent. By contrast, Montana SOS does not provide information to EAC on how they allocate, manage, and track funds. This is similar to approximately half of states nationally, which currently do not report any information to EAC on the approval, oversight, or tracking of HAVA funds to the EAC.

The scope of our audit did not allow for a full review of oversight mechanisms in all 50 states, so it is difficult to determine whether the information or lack of information reported to the EAC represents full disclosure of all oversight mechanisms. Some states may have robust oversight systems in place but choose not to report these to the federal government. However, our work reviewing other states generally shows there are a wide variety of potential oversight mechanisms available, including many that involve a more direct role for the legislature. Broad discretion in federal law and regulations means there is no definitive basis for implementing additional oversight, but Montana has used this approach in the past and it remains an option the legislature could consider for future federal funding opportunities.

Conclusion

Our review found that states are provided broad discretion under federal law and differ in how they manage HAVA funding. The legislature could consider developing expectations for future spending and creating an oversight body to ensure the management and tracking of HAVA funding is meeting those expectations. This may further contribute to ensuring Montana is meeting the goals and objectives outlined in federal grant agreements.

Chapter IV – Security Management

Introduction

Voter registration lists are another key asset in overall election security. The Office of the Secretary of State (SOS) manages the list and therefore has the responsibility to ensure security standards and state security policy are in place.

Agency-Wide Security Posture Is Important to Election Security

According to state statute, agencies are responsible for ensuring an adequate level of security for all data within their respective agency, including designating an information security manager. This statute also includes developing common security policies and procedures, like assessments, user management, software updates, and establishing security policy. Now that election security has been made high profile and is considered critical infrastructure, SOS needs to ensure these elements outlined in statute are addressed. It is critical that risks are assessed, mitigated, and communicated in the overall agency security program to establish groundwork for comprehensive election security.

During fieldwork, we found areas of SOS's security posture that can improve.

- SOS had not conducted the annual risk assessment since 2018.
- Required IT (Information Technology) policy and procedures were not developed to address internal security risks. An example is ensuring that user management and access control to the voter registration system are verified and corrected at the state and county levels.
- There was a lack of consistent communication between SOS and election stakeholders regarding security best practices and standards.

SOS relies on State Information Technology Services Division (SITSD) statewide procedure, such as user access and management procedures. However, relying on SITSD's statewide procedure is not enough to manage the specific scope of SOS responsibilities in all instances. For example, SOS relies on automated statewide user management to provision and manage users. However, county election administrators are responsible for managing user roles for their county users within the system. If a county user changes roles, access to the voter registration list may not be consistently adjusted to fit the person's new role.

Security Oversight Is Not Assigned to a Single, Independent Management Position

When reviewing responsibilities for managing these aspects of SOS's security posture, we found the duties are split between three staff members: the IT Director, Elections Director, and Voter Services Manager. Because two of these staff members also have some responsibilities within the election division, there is potential for conflicting interests, priorities, or expectations. National Institute of Standards and Technology industry standards dictate that to avoid abuse of privileges, key process responsibilities cannot be limited to individuals within the division. An example would be in user access management. If this responsibility is assigned to security positions within the SOS Elections Division, it is likely this user also has a role within the main voter registration system. The ability to review user access management needs to be independent of anyone who has access to the system themselves.

While reviewing the position descriptions for the individuals responsible for ensuring SOS's agency-wide IT security program aligns with state policy and industry standards, we also identified state policy requirements that have been overlooked, like the user access management issue discussed above and written internal policies and procedures. The internal documentation should include, but is not limited to, asset management, risk assessment, incident response, and disaster recovery.

Vacant Security Manager Position Should Be Filled

SOS currently has an FTE for an independent information security manager (ISM), but the position has been vacant since 2017. According to SOS they plan on using Help America Vote Act (HAVA) funding to hire a security specialist within the Elections Division instead of hiring an agency-wide security manager. While we agree with the decision of hiring for a security focused position, using HAVA funding to hire a security specialist for the election division would not address agency-wide security risks. The security specialist specific to elections may not meet the knowledge or skill level that an ISM would need, which could affect the overall implementation of a comprehensive security program.

SOS Can Improve Managing Election Security Risks

By keeping the ISM position vacant, SOS is at a disadvantage in managing election security risks. Without formal documentation and an independent security manager to oversee security in all divisions of SOS, election security will not have a strong security baseline to address election risks or a comprehensive understanding of the entire risk universe within SOS. Furthermore, due to inconsistent security at the counties, the position can serve as a resource for counties and independent oversight of how security is communicated to federal, state, and local election stakeholders.

RECOMMENDATION #4

We recommend the Office of the Secretary of State fill the Information Security Manager position to:

A. *Conduct all security requirements listed in statute,*

B. *Ensure internal policies and procedures are available and consistently reviewed to reduce election and agency risks,*

C. *Provide independent security oversight for election officials and election systems, and*

D. *Provide ongoing communication channels between election administrators, stakeholders, and agency personnel to address security risks.*

Chapter V – Voter Registration Data Accuracy and Maintenance

Introduction

According to federal requirements, each state requires a uniform voter registration list. In Montana, the voter registration list is referred to as MTVotes. MTVotes contains the record of every past and present registered voter in the state. MTVotes also allows for county election officials to enter and update voter information. Voter information includes name, address, county of residence, voter status history, election activity history, and if provided by the voter, social security numbers. MTVotes assists voters by providing:

- Initial registration,
- Personal information changes, and
- Reactivation of registration.

Montana does not permanently remove or delete voter records. If for any reason a voter is inactivated or cancelled in the system, the Office of the Secretary of State (SOS) keeps voter information in the system in perpetuity. However, other states such as Maryland, New Mexico, and Ohio remove voters from their lists after appropriate communications between state election officials and voters have occurred. As of the 2018 general election, there were over 700,000 active registrants with a total of 1.24 million voter records in MTVotes.

Voter Registration Management and Responsibilities for Updating Voter Status

Federal law mandates that states are responsible for creating and maintaining their own list of registered voters. In Montana, the Office of the Secretary of State is the chief election official and is responsible for developing rules for the maintenance of the voter registration list per §13-2-108, MCA. This law states that SOS is required to set the procedures for how the list shall be operated, maintained, and governed.

Due to the amount of records in MTVotes, it would be unrealistic to expect SOS to perform all the necessary maintenance on the voter file. Therefore, election administrators and their staffs from each county are given the responsibility to maintain their respective portions of the voter file. SOS provides some updated voter information to counties through facilitating voter information from other agencies such as Department of Public Health and Human Services (DPHHS) and Department of Corrections (DOC).

Voter Registration Status Changes

Once a person is registered in MTVotes, their information needs to be maintained, such as updating their physical address to ensure they are voting in the right jurisdiction. This is initiated by either the voter or the election administrator through procedures allowed in law. Their options for updating voter information include:

- **Address Changes**: Every odd year, SOS compares the absentee voter registration list to the National Change of Address (NCOA) list maintained by the US postal service to determine if voters' addresses have changed. Mailings are sent to voters identified in the comparison for verification of address changes. If the data comes back indicating change, the county staff have to then update the voter registration data.
- **Inactive Voters**: The National Voter Registration Act (NVRA) allows for voters to have an opportunity to reactivate their voter registration if they have not voted in a federal election. If voters did not vote in the preceding federal election, they receive mailings to try to confirm voter status. The first mailing can be forwardable or nonforwardable at the county's discretion. The notice is sent to active voters based on voting history to identify if the voter resides at the same address and chose not to vote. A second forwardable notice is sent to those who do not respond to the first notice to capture voters that may have moved and provided forwarding address. If there is no response after the two notices are mailed, county staff will manually change the voter status to inactive. After another two federal elections have passed without activity, the voter status is changed to cancel.
- **Voter Death**: A list of deceased individuals is provided to SOS by the Vital Statistics Unit at DPHHS monthly. This list is loaded into MTVotes and system calculations identify potential matches with voters that are not yet cancelled status. Counties can access this list of potential matches in MTVotes as part of their maintenance procedures. The counties also use information from local newspapers and word of mouth.
- **Voter Incarceration**: Updated incarcerated felon information is provided to SOS by DOC biweekly. This list is also uploaded to MTVotes and then compared to voters whose status is not yet cancelled.

System Classifications and Tracking of Voter Status Changes

As stated above, voter statuses can change for a variety of reasons. These changes and reasons for changes are tracked and documented within MTVotes. For example, a voter could be listed as inactive with the reason being that the voter moved to another county or cancelled with the reason that the voter is deceased.

A registered voter may have one of six statuses in MTVotes, three of which are the most common:

- **Active**: actively voting and able to vote in upcoming elections. Voters remain in an active status through the NVRA notifications; however, they

are flagged each time a notice is sent. Once notices have been sent without response, voters will change to inactive.

- **Inactive**: Inactivation occurs after no response to NVRA notifications or an undeliverable ballot is returned to the local election office.
- **Cancelled**: Cancelled reasons includes moving out of state, incarcerated felon, deceased, or duplication.

Other statuses are temporary and apply to unique situations such as same-day registration, pending voter information, and provisional ballots.

While SOS has created automation and consistency of comparing information to update voter status, it is still the responsibility of the county to review the information and update the individual voter statuses identified. Therefore, our work focused on the controls in place to ensure that the automated lists produced by DPHHS and DOC are being used to update statuses in a timely manner. Due to NVRA statute requirements and clear established procedures, NVRA status updates pose less of a risk to the accuracy of the MTVotes.

Voter Registration Analysis Identifies Delayed Status Changes

We reviewed voter status changes since 2015 through a system audit log, a death index file from DPHHS containing deceased individual information, and the most recent list comparison of DPHHS and DOC data to answer various questions about how timely voter status changes are under the current control structure. These questions were:

1. How many potential matches with DPHHS and DOC data have been identified by MTVotes and are still outstanding?
2. How long did it take to update deceased individuals voter statuses to cancelled?

There were 493 outstanding matches with deceased individuals based on the reports sent to the counties from SOS. The dates of death on the outstanding deceased list ranged from 2009 to 2020. Table 2 (see page 26) shows that most deaths have occurred within the past two to three years, but there is still roughly 10 percent or more of the list that have been outstanding for over three years or prior to 2017.

Table 2
Number of Potentially Deceased Voters That Have Not Been Cancelled by Year of Death

Year of Death	Potential Voters	Percentage
2009	1	0.2%
2010	1	0.2%
2014	6	1.2%
2015	6	1.2%
2016	35	7.1%
2017	26	5.3%
2018	82	16.6%
2019	250	50.7%
2020	86	17.5%
Grand Total	**493**	

Compiled by the Legislative Audit Division.

We are unable to provide the same summary for the potential felon list due to limited information. There is no start/end date of incarceration within the felon information provided by DOC for us to identify how timely these changes are. This process also varies from the potential deceased list because the county election official is required to get the status approved by the county attorney before any status changes can be made. This approval can impact the timeliness of the status changes. Reviewing the timeliness of these changes would need further information and coordination from other DOC systems as well as the county attorneys. However, we did discuss this report process and voter maintenance with county election officials.

We followed up with counties of various size that do not appear to be managing these reports in a timely manner. They expressed concerns over SOS's coordination and training and rely on other counties for support. Further work with the counties and other stakeholders could facilitate a more useful and efficient process. This can include additional system trainings that may be needed.

Voter Status Changes Need Follow-Up to Ensure Timeliness

While SOS is providing the reports to the counties, they are not following up to ensure the updates are accurate and timely. Reviewing these reports provides information about statuses that have not yet changed but does not provide a complete understanding of how long it takes to cancel a voter's status when no follow-up occurs. To review this, we identified cancelled voter statuses since 2015 and matched them with individuals from the death index provided by DPHHS. The match was limited to the data available,

which was exact matches only on first name, last name, date of birth, and last four of social security number. Our match identified over 13,000 voters that had a status change reason of deceased and have information from the death index. We were then able to compare the date of death to the date the voter status was cancelled.

The table below groups those results into time frames based on self-reported county update schedules, i.e. monthly, quarterly, and yearly. Almost 65 percent of the statuses were updated within 30 days. Over 14 percent of the statuses were updated between 90 days to one year after death, and roughly 1 percent were updated after one year.

Table 3
Time Elapsed for Status Cancellation of Deceased Voters

Time Elapsed for Status Update	Number of Voters	Percentage
30 Days	8,436	64.2%
30-90 Days	2,655	20.2%
90 Days-1 Year	1,863	14.2%
Over 1 year	188	1.4%
Total	**13,142**	

Compiled by the Legislative Audit Division.

While this indicates there are some delays in updating voter status based on data received from DPHHS, there are situations were DPHHS does not receive timely death information from coroner's office. We recognize that this impacts the timeliness of voter updates by county staff. Counties also expressed frustration that the reports provided by SOS were often late, inaccurate, or both. These instances need to be reviewed with counties to see if potential changes in the system or procedure can be made or if training needs to be updated for reviewing these comparisons.

NVRA Process Is Not a Primary Control for Updating Deceased Voter Records

We also reviewed this data to determine if counties were relying on the NVRA process to update voter data. NVRA does provide extra control to ensure status updates are made, but it should not be the main control. The NVRA process occurs every odd year where statuses are changed to inactive after the first missed federal election. After two additional missed federal elections, statuses are changed to cancelled. Because of the timeliness of the updates, this should not be the primary control for updating statuses.

Our review identified 74,642 voter records that had a status of inactive due to the NVRA process. Of these, we identified .0006 of a percent of voters were deceased. The

data show most changes are made within 90 days, indicating counties are manually updating these statuses as intended and they are not waiting on the NVRA updates to inactivate a voter.

Untimely Updates to Voter Registration Increases Risk of Inaccurate Statuses

While delayed updates can lead to wrong information being reported to state and federal stakeholders such as federal surveys, outdated voter registration information also increases the need for counties to verify ballots. Controls exist to detect invalid ballots including signature verification and usage of ballot barcodes. However, if controls, such as status maintenance, to prevent the acceptance of invalid ballots are inefficient, more reliance is then placed on detecting invalid ballots after the ballot is cast.

After discussing with SOS the gaps in cancelling voter statuses, they provided the voter history file to identify if ballots were accepted after the date of death. We matched names, dates of births and social security numbers of deceased individuals with only ballots that had been accepted in the last ten years. We were able to identify voter ID's for 22,000 of the 95,000 deceased individuals on the death index provided by DPHHS. We then compared the date of death for these matches to the date any ballots were sent to that individual. Date sent was used due to statute indicating a voter can submit a valid ballot if the voter dies between the date the ballot was sent to them and the election date.

There were 4.6 million accepted ballots since 2010. Through our analysis we identified two distinct situations from different counties where voter IDs had accepted ballots after the date of death. Between the two IDs, 26 ballots had been accepted. These two voter IDs represent .00009 of a percent of the 22,000 deceased individuals we were able to identify voter IDs for.

For the first instance, seven different ballots for federal elections, primaries, and municipal elections were accepted. When reviewing the situation, the county verified the issue as a father and son of the same name living at the same address. The father had died, and the son continued to submit his father's absentee ballots unintentionally. He did not appear to submit his own ballots in addition.

For the second, 19 different ballots for various elections were accepted. In this instance, an election official merged two people incorrectly in 2013. One of the merged voters died, so the incorrect merge was unnoticed. There were no actual invalid ballots submitted; it only appears that way in the system because the history of two separate voters appear under the deceased voter's ID.

A State-Level Maintenance Program Is Needed for Increased Voter Registration Accuracy

Federal law requires chief state election officials to uniformly define, maintain, and administer a centralized computerized voter registration list at the state-level. It also requires the chief state election official conduct a general program that makes a reasonable effort to inactivate ineligible voters. State statute requires SOS to adopt rules addressing list maintenance, but these rules do not dictate procedures for timely updates based on deceased and felon lists. Currently SOS does not have any verification in place to ensure the maintenance is being performed in a timely manner, or at all. Our analysis does not indicate a widespread problem; however, SOS has the ability to identify these instances and delayed status updates in order to address them with the counties consistently.

According to industry standards, maintenance programs address root causes of failure in a system. The standards recommend:

- Creating and integrating procedures and practices for key areas,
- Performing program monitoring, and
- Conducting consistent reviews.

All of these areas also include consistent communication with stakeholders. This enforces proactive reviews in coordination with counties, which in turns provides timeliness and accuracy to the voter data.

While there may be various, valid reasons for delayed status updates, such as external sources preventing updated voter records, SOS can provide direction and training to counties to ensure the data they provide is being reviewed and updated timely.

SOS is currently in the process of developing and implementing a new registration system as well. This system will include various systematic controls that can prevent some issues from occurring. However, a state-level maintenance program still needs to be implemented to alleviate potential user errors in updating voter status. The improved communication within the maintenance program will also assist in identifying potential system issues, timing issues when comparing reports from other agencies, and other procedural improvements.

RECOMMENDATION #5

We recommend the Office of the Secretary of State implement a state-level maintenance program that addresses issues identified including:

A. *Developing a regular maintenance, communication, and follow-up schedule for the state and counties to follow to ensure timeliness of updates.*

B. *Implementing periodic voter registration data analysis to review controls that ensure voter statuses are current, accurate, and prevent invalid ballots.*

The Office of the Secretary of State

Office Response

COREY STAPLETON
SECRETARY OF STATE
STATE OF MONTANA

RECEIVED
August 05, 2020
LEGISLATIVE AUDIT DIV.

Mr. Angus Maciver, Legislative Auditor
Legislative Auditor
Legislative Audit Division
PO Box 201705
Helena, MT 59620-1705

Re: Response to Information System Audit

Dear Mr. Maciver,

Thank you for the opportunity to respond to the Information System Audit report for the Office of the Secretary of State. The five recommendations included in the audit report were reviewed with responses provided below.

Recommendation #1

SOS Response: Concur

The Secretary of State would recommend setting the standard in statute that election information security and physical security must follow NIST standards and guidelines along with any security standards promulgated by the US Election Assistance Commission.

Recommendation #2

SOS Response: Concur

Using federal guidelines and best practices, the Secretary of State's office will consider adopting rules clarifying election security measures to assist counties in understanding what is necessary for securing voting systems, including physical security.

Recommendation #3

SOS Response: Concur

As stated in this report, the Office of the Secretary of State follows HAVA requirements for managing and dispersing grant dollars. HAVA grant award recipients and sub-recipients must also follow the U.S. Election Assistance Commission guidance and adhere to all applicable federal requirements including Office of Management and Budget (OMB) guidance: Title 2 C.F.R. Subtitle A, Chapter II, Part 200-

Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. § 200). The Office of the Secretary of State's existing Policies and Procedures for Administration and Monitoring of Federal Programs manual will be updated by September 1, 2020 to include additional best practices noted in this recommendation. Reviewing SOS's internal federal programs policies and procedures manual will be a business improvement process that will occur on a continuous and ongoing basis. The CFO will complete an additional 40-hour training in grant administration.

Recommendation #4

SOS Response: Concur

The IT Security Analyst duties have been divided amongst three existing positions. Going forward, the duties will be consolidated into one IT Security Analyst position. The position is currently posted.

Recommendation #5

SOS Response: Concur

The Secretary of State will implement a state-level maintenance and data analysis program.

Thank you to you and your staff for the professional work and interactions with our staff during this audit process and the willingness of the auditors to discuss recommendations and responds to our questions. The Office of the Secretary of State regards the audit process as an opportunity to improve the agency's operations and performance.

Sincerely,

Corey Stapleton
Secretary of State