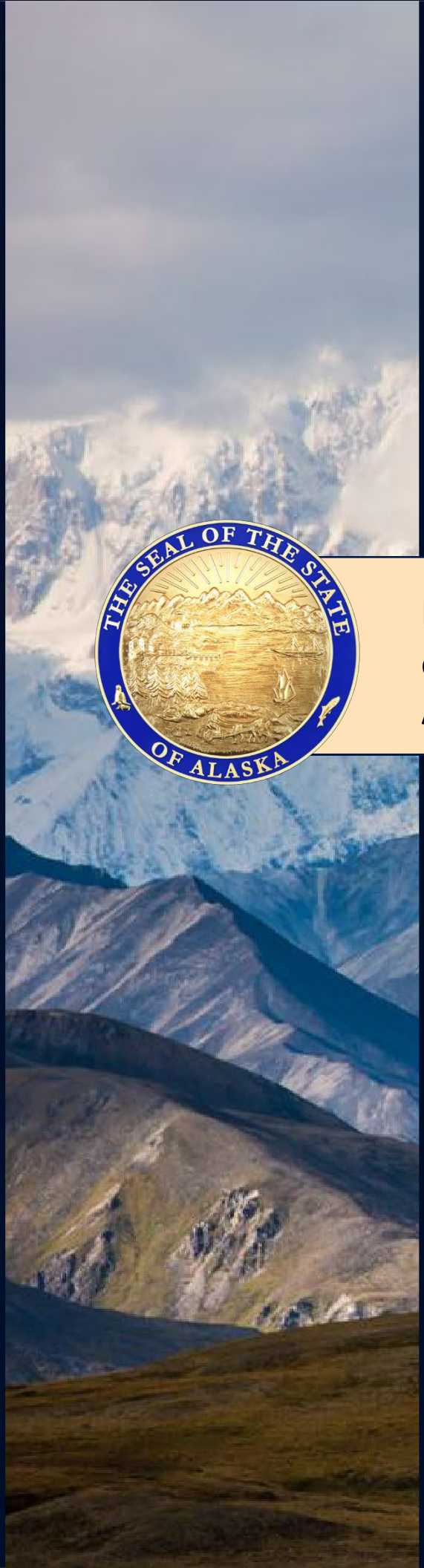


DEPARTMENT OF ADMINISTRATION

Oversight and Review Unit

Review of the Effectiveness and Security of the Division of Elections in Administering Alaska's Elections

July 13, 2020

Executive Summary

Review of the Effectiveness and Security of the Division of Elections in Administering Elections

RESULTS IN BRIEF

Lieutenant Governor Meyer requested a review of the Division of Elections (DOE) to assess how efficiently and effectively the DOE is operating.

We found that the DOE adequately complies with state and federal election laws. We determined the DOE effectively fulfills its duty to provide adequate access for all voters, with necessary accommodations made for voters with disabilities.

However, the DOE faces challenges preventing the voter registration of felons and other ineligible voters caused primarily by the PFD automatic registration law.

We identified voting discrepancy and security issues in several precincts during the 2018 elections, but, the DOE only conducted an audit in one of these precincts. While precincts are only eligible for audits if their votes are counted by optical scan and if they account for at least 5% of the vote in each respective district, the DOE can audit the ballots in any precinct in which there is an unexplained discrepancy.

We found the DOE has limited written policies or procedures on voter fraud response. Instead, the DOE relies on employees' instincts for identifying, handling, and referring potential voter fraud.

We also found the DOE made changes since the 2018 elections that provides for a more secure and effective election process for voters.

We identified long-existing challenges in administering elections in rural areas, including inability to retain consistent and reliable election officials to staff the polling locations and having significant technical issues with the voting machines.

The Permanent Fund Dividend Automatic Voter Registration law (PFD/AVR) has created significant challenges for the DOE to manage with little return on investment. The implementation of this law is neither the fault nor responsibility of the DOE, but it has a significant impact on the effectiveness of its operations.

One way to improve the DOE's effectiveness is by increasing cybersecurity audits. After the DOE was targeted by Russia in 2016 for election tampering, the Department of Homeland Security offered to perform at no cost a Risk and Vulnerability Assessment on the DOE's IT system. However, we found the DOE declined this offer.

We found the DOE has emphasized other aspects of cybersecurity, working to create a secure voting process. But the DOE does not have an Election Security Preparedness Plan. It also lacks collaboration with other cybersecurity stakeholders in the state, but instead has taken a siloed approach to its cybersecurity efforts. Very recently, DOE has started meeting monthly with the Office of Information Technology's Chief Information Security Officer, which is a positive step towards collaboration for greater elections cybersecurity.

We made 18 recommendations to improve the efficiency and effectiveness of the DOE, including:

- Consider Implementing Signature Comparison Software
- Continue to Monitor and Improve the Process to Ensure Voter Rolls are Current and Accurate
- Audit Precincts in which Discrepancies Occur
- Consider Implementing Hand Count Verification Process of All Precincts Using Optical Scan
- Repeal or Amend the PFD Automatic Voter Registration Program
- Conduct DHS Security Risk and Vulnerability Assessment Testing
- Give OIT Authority Over the DOE's Cybersecurity
- Create an Incident Response Plan

TABLE OF CONTENTS

INTRODUCTION

The State of Alaska is committed to administering accessible and secure voting to all citizens across the state. The Department of Administration (DOA) Oversight & Review Unit (O&R) initiated this review at the request of the Lieutenant Governor to assess how efficiently and effectively the DOE is operating, evaluate DOE management and processes, determine the DOE's level of security preparedness, evaluate DOE's efforts to administer fair and safe elections, and make recommendations for improvement where practicable.

Background

The DOE is responsible for planning, implementing, and conducting all statewide and federal elections. It also is responsible for statewide voter registration activities and maintenance of Alaska's voter registration database. Over the last 20 years, the DOE has relied on a precinct-level voting system made up of a complex network of voting equipment and processes. This system is intended to allow all Alaskans eligible to vote to do so without interference.

The Lieutenant Governor appoints the Director of the DOE, who is responsible for implementing all laws and regulations governing the elections process.[1] The DOE is divided into four geographically based election regions managed by Election Supervisors. The Election Supervisors are responsible for voter registration and election management activities for all elections within their region, as designated by the Director. In addition to the four regional offices located in Juneau, Anchorage, Fairbanks and Nome, the DOE has opened a satellite office of the Region II Elections Office in the fastest growing municipality in Alaska, the Matanuska-Susitna Borough.

The state is divided into 40 house districts with a total of 441 precinct polling places across the state and over 150 absentee/early locations serving a total of 575,049 eligible voters in 2018. The DOE also maintains an Absentee and Petition Office (APO) in Anchorage to facilitate and improve absentee voting by mail and by fax. In addition, the APO ensures the DOE's absentee voting programs comply with the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) and the Military and Overseas Voter Empowerment Act (MOVE Act), and it provides improved access to voting for military and overseas voters.

In early 2019, Lieutenant Governor Kevin Meyer met with Commissioner Tshibaka regarding concerns that during the 2018 election, many voters expressed verbally that they distrusted Alaska's elections process and the DOE. The Lieutenant Governor requested a review of the DOE, seeking to improve the DOE and increase Alaskans' trust in the elections process.

[1] Alaska Statutes Title 15 and Title 6 of the Alaska Administrative Code (AAC) govern the federal and state election process. Alaska falls under Section 5 of the Voting Rights Act (VRA) of 1965. Alaska also falls under the minority language assistance requirements of Sections 4(f)(4) and 203 of the VRA.

Prior Coverage of the DOE

In 2015, Lieutenant Governor Mallott convened an Election Policy Work Group (EPWG) to evaluate Alaska's elections. His goal was to maximize effectiveness, cost efficiency, and responsiveness to the needs of Alaskan voters. In response to the EPWG, the DOE produced two reports: the "2017 Fiscal & Policy Challenges" and "Improving Alaskan Elections: 2019 and Beyond." The DOE's 2017 report outlined various issues facing the DOE and Alaska's elections, and directed the EPWG to provide advice regarding solutions to those issues. The latter report served as both a descriptive and aspirational document detailing the EPWG's conclusions and urged the EPWG to maintain its momentum throughout the 2018 election cycle.

The EPWG determined the most important issues facing Alaska's elections, included: (1) modernization of Alaska's elections, (2) Permanent Fund Dividend (PFD) automatic voter registration, and (3) voter trust in elections. This report will address numbers two and three in addition to other findings. Issue one will not be our focus due to the DOE's purchase of new voting equipment in 2019.

The DOE resolved to take actionable steps in 2018 to address issues facing Alaska's elections. In July of 2018, DOE recruited the help of the University of Alaska Anchorage (UAA) Institute of Social and Economic Research (ISER) in creating a new report: "Perceptions of Universal Ballot Delivery System." This report considered alternative voting methods for state and federal elections by conducting a survey of 412 individuals registered in Region IV of Alaska. The EPWG recommended exploring a hybrid or universal system that includes early in-person voting and vote-by-mail (VBM).[2]

Survey respondents heard a description of three voting methods being considered: 1) keep voting the way it is now; 2) mail out and mail back; or 3) receive a ballot in the mail and have different ways to return it. Of the three methods, "keep voting the way it is now" was the first choice by 49% of respondents, followed by 36% for option 3, and 14% for option 2. Respondents had little experience with voting methods other than in-person.

Scope and Methodology

This review attempts to provide some transparency into the DOE and its process for administering elections. We examined areas of concern in administering the 2018 elections, and the changes the DOE made as a result. We evaluated challenges in administering elections in rural areas, the DOE's process for conducting post-election audits, and the Permanent Fund Dividend (PFD) Automatic Voter Registration program.

[2] VBM is regarded by many as more likely to be affected by malfeasance. Integrity problems with mail voting include: a) mail voting lacks the high level of proof of identity and eligibility standards that can be applied at in-person voting stations; b) there is no opportunity for party or candidate representatives to observe voting by mail; c) it is not feasible to provide complete security for all voting material as it moves through postal systems; d) there can be no guarantee that the voter who completed the ballot was not subject to influence or intimidation.

We also examined the DOE's compliance with Alaska election law, federal election law, and internal processes. Finally, this review examines the DOE's cyber security, coordination with the State Security Office (SSO), and efforts to improve the administration and security of elections.

To perform this review, we conducted interviews with DOE staff members, including IT professionals, Region Supervisors, the Director of the DOE, and the State Chief Information Security Officer. In addition, we interviewed Department of Homeland Security (DHS) representatives. We reviewed applicable statutes including the automatic PFD registration laws. We also examined the DOE's standard operating procedures, manuals, and training materials used in administering elections. Finally, we made recommendations for improvement.

O&R's authority derives from a February 26, 2019, memorandum from Governor Dunleavy to Commissioner Tshibaka stating his "intent and expectation that [her] expertise be utilized to review, investigate, and provide policy direction, not only as it relates to the Department of Administration, but as it applies statewide in the areas of management, audit, and government efficiency, as directed, on my behalf." (Appendix A) Commissioner Tshibaka established O&R to promote efficiency and effectiveness, in the programs and operations of the State of Alaska, and to detect and deter waste, fraud, and abuse.

This review was conducted in accordance with the Quality Standards for Inspection and Evaluation established by the Federal Council of the Inspectors General on Integrity and Efficiency.

This report provides findings about the DOE's current processes and offers insights to Alaska's voting procedures and cyber security efforts. It includes recommendations for policy, process, or procedural revisions that will increase DOE's effective administration of elections in Alaska. While this report is being issued during the COVID-19 worldwide health pandemic, all the fieldwork for this review was conducted prior to the pandemic. So, the findings and recommendations made herein are independent of the current health crisis, health mandates, and community limitations that could affect how the DOE administers elections.

We are grateful to the Office of the Lieutenant Governor for initiating this review and DOE assistance in getting this project accomplished.

FINDINGS OF THE REVIEW

The DOE's Process for Conducting Elections

DOE's efficient administration of elections in Alaskan communities (rural and urban alike) is largely dependent upon a continuous chain of relationships between DOE officials and community members tapped to participate in administering elections. Regional offices recruit election workers between February and May in even numbered years, often attempting to retain previous election officials. DOE has had difficulty finding election officials to administer elections, particularly in rural areas.

In compliance with AS 15.10.120, each precinct is staffed with a minimum of three workers or election officials, including the chair and co-chair. However, despite great effort, we found that in rural areas DOE has not always been able to staff each precinct with three workers. Language assistance is provided in areas of the state as identified in Section 203 of the Voting Rights Act.[3] In these areas, bilingual election workers are available in person or telephonically.

Election officials who agree to administer elections are requested to report for training in advance of election day. In compliance with AS 15.10.107, DOE mandates that the Chair and Co-Chair of each voting precinct attend training, and their attendance is tracked via a pen and paper sign-in sheet. However, there is no formal method of tracking whether other election workers have attended training.

Elections in Alaska are hand marked ballots that are either hand counted or scanned using voting equipment at the precincts. In compliance with AS 15.20.900(b), 6 AAC 25.030(e) and 6 AAC 25.045, the voting machines are tested before election day to assess logic and accuracy of the counting program. This process, and the election itself, is overseen by a regional board of 2-8 members (no more than 2 of whom may belong to the same political party). Before the opening of polls on election day, the election board must verify that the machine produces a "zero totals report." The same process is used if a machine is being used to count absentee or questioned ballots.

The DOE uses troubleshooters/field workers who are available on election day for technical and administrative support for voting machines. These troubleshooters receive additional training for this role. Each troubleshooter has a DOE-issued cellphone for effective communication.

The field workers also remain on standby to address complaints regarding election workers or mismanagement in their assigned precincts (5-8 precincts are assigned per fieldworker). DOE Director Gail Fenumiai noted that the DOE does not keep formal records of complaints received by fieldworkers, mismanagement in their precincts, or of corrective measures taken. This is attributed to the "fast pace of election day" and the fact that most complaints are

[3] https://www.census.gov/content/dam/Census/newsroom/press-kits/2017/esri/esri_uc2017_voting_rights_act.pdf

delivered verbally via telephone. The current Director was not with the Division during the 2018 elections and has no knowledge of complaints against DOE personnel related to the 2018 election cycle.

The significant difficulties DOE has encountered in identifying election officials to administer elections has, in some cases – most notably House Districts 06, 37, 39 – involved certain individuals being taken on as election workers who subsequently failed to properly administer the election. However, election officials are occasionally held accountable for misconduct or poor performance. For example, one election worker was not permitted to serve as an election worker after she became sleepy and belligerent while serving as an election worker during a primary election. We found, however, that DOE does not often dismiss election officials because of the difficulty it has in finding replacements.

Accessibility for All Alaskans

The DOE is responsible for making voting accessible to all Alaskans, including those of differing abilities and for whom English is not their first or preferred language. The DOE has compiled these standards in election worker handbooks and training curricula.

Ballots (written and audio), posters, glossaries, etc., are provided in multiple Native Alaskan languages, Tagalog, and Spanish. Interpreters may be reached via a toll-free phone number if bilingual election workers are not available. Special needs or disabled voters that may require assistance are entitled to it. Non-compliance is generally reported by individual voters who observe or are affected by precincts' failure to meet accessibility standards.

If voters are unable to vote at their assigned polling place due to age, illness, or disability, any voter may assign a personal representative to obtain ballots or other voting material available to each voter. The representative returns the voted ballot to the election official. Special Needs voting also is available at the polls on Election Day or through any absentee voting official.

Any voter who does not have identification and is not personally known by the election official, or whose name does not appear on the precinct register at the polling place where the voter is attempting to vote, can still vote by using a Questioned Ballot. After the election, Questioned Ballots are delivered to regional election offices for verification of voter eligibility in the statewide voter registration database.

Voters can also vote by mail through absentee voting. Any voter can request an absentee ballot and will receive their ballot by mail. Beginning 45 days prior to each election, ballots are mailed to active military members, their spouses, and dependents; U.S. citizens temporarily or permanently living overseas; voters who requested absentee ballots due to living, working, or traveling in remote Alaska; and voters who requested absentee ballots due to traveling internationally at the time of the election. All other absentee ballots are mailed to voters approximately 25 days prior to each election.

Methods for Counting Votes in Each District

Alaska's 441 precinct polling places have unique considerations that can affect how they count votes on election day:

- 304 of Alaska's 441 precincts use a single optical scanner throughout Election Day for scanning/tabulating the paper ballots.
- 137 of Alaska's 441 precincts are considered hand-count precincts, meaning election workers count the ballots by hand when the polls close and call their assigned Regional Office to report the election results.

Alaska's ballot tabulation system has had a paper trail of every ballot cast. Each precinct has received paper ballots that are either hand-counted when the polls close or counted using an optical scan unit. In addition, as part of the division's compliance with the Help America Vote Act (HAVA), each precinct has a touchscreen voting unit equipped with a voter-verifiable paper trail that allows the voter to verify the printed version of the ballot prior to casting the ballot. Alaska law considers the "printed" version to be the official ballot. In Alaska, 99% of all voters cast a paper ballot. The touchscreen voting units have been used by approximately 1% of voters, usually those who are physically unable to cast a paper ballot.

The optical scan voting machines provided by the DOE to the districts were significantly outdated, creating problems for election administrators and voters alike. The optical scan voting machines were purchased in 1998 and given a 20-year life expectancy. While most are still operational (although, some failed mechanically during the 2016 and 2018 election cycles), the machines are expensive and difficult to maintain because key components, such as memory cards, are no longer manufactured. Additionally, the method of reporting vote totals relies on outdated infrastructure, such as analog phone lines.

To address these issues, in March 2019, the DOE solicited proposals for the implementation, installation, testing, maintenance, support, and training for a comprehensive statewide voting and ballot tabulation system. This system will be used to support all aspects of creating, casting and tabulating ballots, and reporting election results. The expected life of the new election management system is at least 15 years. The system will support statewide elections, and the State intends to allow local jurisdictions to use the system and equipment where feasible. It was confirmed that the DOE has been actively working with the equipment vendor (Dominion) on training and implementation of the new voting system. The new system will be used in the 2020 elections, and Dominion will provide technical support in Alaska during the elections.

Areas of Concern Identified During the 2018 Elections

Alaska's 2018 elections resulted in public concerns about voting processes, the DOE, and unusual, improper or fraudulent voting, which were reported by local news media.[4] These

[4] See, e.g., https://www.adn.com/politics/alaska-legislature/2018/11/27/alaska-division-of-elections-certifies-tie-in-critical-fairbanks-house-race/ (comments section); "Voters at West Anchorage polling station briefly without paper ballots after election worker forgot them," Michelle

concerns included, but were not limited to, the DOE being biased towards Democrats, counting missing or disqualified ballots as legitimate votes, registered voters at the precinct not matching the number of votes counted, voters not having ballots in time on election day, absentee ballots being miscounted, and trouble with the voting machines. In one situation involving suspicious Absentee Ballots in House District 15, the DOE Director contacted the Alaska State Troopers (AST) and the State of Alaska Department of Law to report suspected voter fraud and possible violations of criminal provisions of the Election Code. This issue had been detected and appropriately reported by DOE staff.

With respect to the DOE's investigations or inquiries concerning suspected improper or fraudulent voting in any Alaska voting district during the 2018 primary and general elections, the DOE provided the following information:

1) Duplicate Voting

2018 Primary Election

There was an initial list of 39 potential duplicate voters out of 115,727 total voters. After research, there were 23 voters who submitted two ballots. Four of these voters had both ballots counted. For the other 19 voters, the DOE was able to find and reject the second ballot before it was counted. DOE staff interviewed these individuals and found that voters were confused, went to incorrect voting locations, and then attempted to make corrections.

2018 General Election

There was an initial list of 88 duplicate voters. After research, there were 54 voters out of 285,009 total voters who submitted two ballots. Thirteen of these voters had both ballots counted. For the other 41 voters, the DOE was able to find and reject the second ballot before it was counted.

2) Felony Voting

2018 Primary Election

A voter recognized the name on a precinct register of someone who was a convicted felon. The DOE contacted the court system to receive verification of the conviction status and the voter's record was inactivated. As a result of this, the DOE was asked to do a complete review of the statewide voter registration list to ensure there were no voters who had been convicted of a felony involving moral turpitude. However, the DOE did not have time to conduct this research before the 2018 general election.

In addition to the request for the statewide review, the DOE received the names of 256 individuals who indicated on their Permanent Fund Dividend (PFD) application they had been convicted of a felony. However, the DOE did not have time to adequately perform the

Theriault Boots, *Anchorage Daily News*, November 6, 2018; "Letter: Separate early Walker votes," Randall Burns, *Anchorage Daily News*, November 5, 2018; "Citing absentee ballot concerns, petitioners call for recount in close Kenai Peninsula primary," Devin Kelly, *Anchorage Daily News*, September 6, 2018; "Southern Southeast votes still trickling in: Trouble with voting machines leads to delays," James Brooks, *Juneau Empire*, November 8, 2018.

required research for all these records. An administrative decision was made to inactivate the voter registrations of the 256 individuals in question until such research could be conducted.

To address this problem, the DOE now receives a list from the Alaska Court System containing all convictions from the prior week. The DOE staff then sorts the list according to the conviction and uses it to eliminate those who have been convicted of any crimes involving moral turpitude.

2018 General Election

In the 2018 General Election, one voter submitted a Questioned Ballot which was rejected due to felony status. The DOE processed the information from the voter's ballot envelope to update his registration. Because he was in felony conviction status, the DOE contacted the probation office and was informed he was unconditionally discharged before the election.[5] The voter's registration was updated, but his ballot eligibility was not changed. It was not until the standard review of reject ballots that the DOE noticed this ballot should have been counted in full. During the DOE's follow-up review, this voter's inactive status was researched; it was confirmed he was eligible to be registered, and he had done so through the PFD application.

The DOE has implemented an ongoing comparison of the statewide registration lists to the court list of individuals convicted of felonies since 1976. The DOE advised that this is, "a work in progress."

3) DOE Lacks Voter Fraud Policies or Training

The DOE does not have written policies or procedures on voter fraud response. The Director of the DOE explained that she relies on her employees' "instincts" for finding cases of fraud. During the investigation into 2018 primary election voter fraud allegations, the DOE staff said they responded to the situation based on their experience and expertise. After reviewing the DOE's response to possible voter fraud during the 2018 primary election, we found the DOE responded appropriately by isolating the potential fraudulent ballots and monitoring for any additional fraudulent ballots.

The DOE does not have investigative authority or formal expertise in detecting fraud; the DOE involves the Department of Law when irregularities are identified. The DOE indicated it is "difficult to come up with a comprehensive list of potential fraud items." While not comprehensive, the following list covers most voter fraud schemes on which DOE staff could be trained to identify by using skill, rather than instinct:[6]

- Impersonation fraud at the polls
- False registrations
- Duplicate voting

[5] If a voter is unconditionally discharged, they must then take the step to re-register to vote.
[6] See https://ballotpedia.org/Electoral_fraud.

- Absentee ballot fraud
- Buying votes
- Illegal "assistance" at the polls
- Ineligible voting (felons, deceased, non-registered)
- Altering the vote count
- Ballot petition fraud

Changes Made After the 2018 Elections

1) Duplicate Voting

The DOE has revised its process for dealing with duplicate voting by adding to the precinct registers a notation for citizens who have "applied for an absentee ballot." This is in addition to the notations for those citizens who have "already voted," which appears for those voters who voted early or whose absentee ballot may have already been received.

In addition, each day following the date the precinct registers are printed, the DOE will produce supplemental lists that contain the names of new voters who have voted early or whose absentee ballot has been received. These lists will be provided to precinct chairpersons to notate next to the voter's name on the precinct register. The DOE will ensure printing of supplemental lists be done up to the day before Election Day.

No absentee ballots (by-mail, by fax, online or in-person) will be counted until *after* voter history has been completed for an entire house district and the duplicate voter report has been cleared.

Early vote (EV) ballots cast beginning the Friday before Election Day will no longer be commingled with other ballots. The EV ballots will be placed in an envelope with the EV certificate attached. The EV ballots cast on the Friday, Saturday, Sunday, or Monday preceding Election Day and on Election Day will not be counted until after an entire district's voter history is complete and the duplicate vote report is cleared.

If the name of a voter is marked on the precinct register as "already voted" and the voter appears to vote at a precinct, the voter will be required to vote a questioned ballot. If the name of a voter is marked on the precinct register as having applied for an absentee ballot and the voter appears to vote at the precinct, the voter will be required to vote a questioned ballot.

The DOE will publicize the changes in counting procedures by Public Service Announcements, social media, etc. The ballot counting schedule also will be published on the DOE's website.

2) Felony Voting

The DOE is researching other ways to identify and prevent illegal voting by ineligible felons.

The Division has explained that felony voter inactivation will never be perfect—there are too many moving parts within the judicial system. Felonies involving moral turpitude change as laws get changed by the legislature; individuals convicted with such crimes often have charges reduced.

3) DOE Efforts to Ensure Accuracy of Voter Rolls

The DOE reported that it currently follows the provisions for list maintenance found in the National Voter Registration Act (NVRA). The DOE is also working on tracking felony convictions more efficiently. The DOE also provides for online registration, including registrations at the Division of Motor Vehicles (required by NVRA), participation in the Electronic Registration Information Center (ERIC) with cross-state match and in-state move notices to voters, PFD match, vital stats death lists, court system lists for felon inactivation, flagging undeliverable addresses and updating mailing address with forwarding addresses, etc.

Challenges in Administering Elections in Rural Areas During the 2018 Elections

Alaska has approximately 150 rural communities with precincts that are isolated from connecting road systems. Typically, the only way to access these communities is by airplane or boat. At 663,300 square miles, Alaska is over twice the size of Texas. These geographic realities present many unique challenges for the DOE in administering elections. Below, we identify difficulties encountered during the 2018 election cycle, based on documentation provided by the DOE cataloging the incidents and any corrective action taken. Most of these difficulties occurred in isolated precincts.

Due to the overwhelming number of reported mechanical problems with the TSX (touchscreen voting) machines identified in various precincts below, we questioned whether voting machines were adequately tested before election day and if the testing was overseen and verified by the regional election board (as required by AS 15.20.900(b), 6 AAC 25.030(e), and 6 AAC 25.04).

In response to an information request, the DOE provided documentation verifying the required functionality testing and logic and accuracy testing had been done. The DOE also qualified that voting machines require shipping to the precinct and back to the division four times during an election cycle and that damage can and does occur during shipping. In our recommendations listed at the end of this report, we suggested that the DOE seek out possible solutions to this problem by exploring the possibility of securing remote storage facilities located near Regional or Local Precincts.

In the DOE's additional responses to information requests, it also qualified that loss of use of the TSX machines would not have affected the outcome of any election since all precincts have paper ballots as backups. It also was explained that there are sample ballots in Alaska Native languages for the bilingual election workers to use when language assistance is requested. The issues regarding the hand counting verification process in cases of machine malfunctions are addressed in the recommendations listed at the end of this report.

Region I Primary Elections - Juneau

Bear Creek,[7] Pelican/Elfin Cove: Election officials reported they could not get the touch screen voting (TSX) units set-up. The Bear Creek unit had a blank LCD screen and the Pelican/Elfin Cove leg brackets were bent, making it unable to stand. Documentation provided by the DOE did not clarify if these voting problems compromised the election in any way.

Region III Primary Elections – Fairbanks

Stevens Village:[8] Two people were scheduled to work the election, but neither of them came or could be found by DOE representatives. AST were requested to assist, but did not do so. Neither the Village Chief nor anyone in the community were willing or able to access the building and return the election materials. According to information provided by DOE, when a voter called to complain about not being able to vote, DOE asked if the voter would serve as the election worker and he agreed to conduct the election. DOE sent the election materials via airplane to Stevens Village, but according to DOE records, no votes were counted for this precinct.

Region IV Primary Elections - Nome

Aleknagik:[9] The TSX machine fell over election morning. After several attempts to get it back up and functioning, it did not work. Documentation provided by the DOE did not clarify if this issue was resolved or if a hand count was subsequently performed for this precinct.

Pedro Bay:[10] The election board reported issues with the TSX machine set-up. Region IV staff provided advice, but they did not get the machine working. Documentation provided by the DOE did not clarify if this issue was resolved or if a hand count was subsequently performed for this precinct.

St. George Island:[11] Post-election attempts to locate "red and green bags filled with voter materials" were unsuccessful for several weeks. The DOE finally contacted the chairperson on September 10th, and she said she would mail bags that day. The DOE did not indicate whether the election materials were ever received or if it compromised the election in any way.

St. Paul Island:[12] The chairperson reported TSX machine set-up problems during the primary election. Region VI staff provided advice, but they were still unable to set-up the TSX. Documentation provided by the DOE did not clarify if the issue was resolved or whether these problems compromised the primary election in any way. DOE reported votes were cast on the TSX machine in the general election.

Russian Mission:[13] The election board reported TSX machine set-up problems during the

[7] Bear Creek had 1742 registered voters during the 2018 elections.
[8] Stevens Village had 78 registered voters during the 2018 elections.
[9] Aleknagik had 164 registered voters during the 2018 elections.
[10] Pedro Bay had 39 registered voters during the 2018 elections.
[11] St. George Island had 48 registered voters during the 2018 elections.
[12] St. Paul Island had 303 registered voters during the 2018 elections.
[13] Russian Mission had 226 registered voters during the 2018 elections.

primary election. DOE staff offered advice, but set-up was still unsuccessful. Documentation provided by the DOE did not clarify if the issue was resolved or whether these problems compromised the election in any way. DOE reported votes were cast on the TSX machine in the general election.

Shishmaref:[14] The chairperson reported the TSX machine encoder was not working. Region IV staff provided advise to assist voters without use of the encoder. Documentation provided by the DOE did not clarify if the issue was resolved or whether these problems compromised the election in any way.

St. Mary's:[15] The chairperson reported the TSX machine had broken parts and was missing a paper spool, so the TSX was not used during the primary election. Documentation provided by the DOE did not clarify if the issue was resolved or whether these problems compromised the election in any way. DOE reported votes were cast on the TSX machine in the general election.

Teller: Region IV staff attempted to contact the chair-persons numerous times to check status of mailing of election results materials.[16] A co-chairperson returned the call on September 17 stating bags were mailed that day. Documentation provided by the DOE did not clarify if the bags were ever received or whether these problems compromised the election in any way.

Region IV General Elections - Nome

Kwethluk:[17] The TSX memory card said, "no election loaded." Documentation provided by the DOE did not clarify if the issue was resolved or whether these problems compromised the election in any way.

Emmonak:[18] The TSX machine memory card malfunctioned during the primary election. Documentation provided by the DOE did not clarify if the issue was resolved or whether these problems compromised the election in any way. DOE reported votes were cast on the TSX machine in the general election.

Kotlik:[19] After a phone consultation, the printer was not able to be set-up correctly. Documentation provided by the DOE did not clarify if the issue was resolved or whether these problems compromised the election in any way.

Kaktovik:[20] The keys for the Optical Scan Ballot Tabulator were missing from the materials. Documentation provided by the DOE did not clarify if the issue was resolved or whether these problems compromised the election in any way.

[14] Shishmaref had 375 registered voters during the 2018 elections.
[15] St. Mary's had 439 registered voters during the 2018 elections.
[16] Red bags contained: voted questioned ballots; voted special needs ballots; and all remaining voter materials and were sent to the Election Supervisors. Green bags contained: precinct registers; results tapes; voted ballot envelopes, and memory card envelopes.
[17] Kwethluk had 484 registered voters during the 2018 elections.
[18] Emmonak had 505 registered voters during the 2018 elections.
[19] Kotlik had 365 registered voters during the 2018 elections.
[20] Kaktovik had 197 registered voters during the 2018 elections.

Post-Election Audits

Alaska's post-election audits are conducted for the entire ballot by the State Review Board (SRB), which is a bi-partisan review board that is responsible for testing the ballot count programming (prior to the election) as well as performing the post-election audit.[21] The SRB reviews all precinct registers, absentee site documentation, absentee and questioned voter registers, summary sheets, and ballot tabulation tapes. According to DOE, the SRB compares the number of ballots cast to the number of actual voters. They will do further review if they find a discrepancy and rescan ballots when required.

The audit process involves a hand count of all ballots from one randomly selected precinct in each of the state's 40 house districts. A precinct is eligible for a hand count if the precinct accounts for at least 5% of the ballots cast in that district. [22] Audit results are binding on official results, but do not lead to a full recount. Races that are uncontested do not need to be hand counted.

According to AS 15.15.430, 6 AAC 25.068, and 6 AAC 25.203, the hand count verification process occurs after every statewide election to verify that the voting machines counted ballots accurately and that there was not a discrepancy of more than one percent between the machine tally and the hand count tally.

In the 2018 election, we identified 15 precincts (described above) with unresolved election issues that may have affected the outcome of the election. Of the 15 precincts, only one of them had a post-election audit. The DOE told us 13 of the 15 precincts were ineligible for an audit because they received hand-counts of the votes immediately following the election; precincts are only eligible for audits if their votes are counted by optical scan and if they account for at least 5% of the vote in each respective district.

However, AS 15.15.430(c) allows the DOE to audit the ballots in any precinct in which there is an unexplained discrepancy, regardless of whether it represents 5% of the vote for the district. We also found that even though several voting irregularities were reported to the DOE in other districts, the DOE followed the minimum statutory requirements in determining which precincts to audit and did not audit all of the precincts in which irregularities were reported.

With respect to post-election audits in general, the DOE clarified that the Alaska State Review board performs post-election audits of all precincts, however, the hand count verification process (HCVP) only applies to precincts that use optical scan. Of the 15 precincts addressed above, only two of them used the optical scan for counting ballots. And those two either did not meet the 5% requirement or if they did, they were not randomly drawn for the hand count verification. The other 13 precincts are hand count precincts and are not included in the HCVP process. We concluded that the HCVP should be required for any precinct where

[21] For the 2018 primary election, the SRB was comprised of 13 members, 6 teams of 2 people, which included 3 Republicans, 3 Democrats, 1 Libertarian, 4 Non-Partisan and 2 Undeclared Alaskan voters. For the 2018 general election, the SRB also comprised of 13 members, again 6 teams of 2 people, which included 4 Republicans, 3 Democrats, one Libertarian, 3 Non-Partisan and 2 Undeclared Alaskan voters.
[22] AS 15.15.430.

reported problematic issues could have any possible impact on the number of votes counted.

Risk-Limiting Audits Emerge as Best Practice

In recent years, researchers have developed statistically based audit techniques, referred to as risk-limiting audits. Risk-limiting audits are designed to limit an audit to a statistically predetermined level of confidence that the reported result is correct. If the margin of an election is wide, very few ballots must be reviewed. If the race is close, more ballots will be reviewed until statistical evidence confirms the declared election result. This method reduces the number of ballots that require auditing, while also providing statistical confidence that an incorrect election result is not certified (i.e., made official). This method also is both effective and efficient, allowing for a statistically accurate recount and not requiring more work than necessary. Typically, however, risk-limiting audits are used in jurisdictions that have a different election structure than Alaska. Use in Alaska would require adaptation to a method that would work for how ballots are counted in Alaska and possibly statutory revisions, which could be challenging.

According to a 2018 U.S. Senate Intelligence Committee report on Russian targeting of election infrastructure in 2016: "States should consider implementing more widespread, statistically sound audits of election results. Risk-limiting audits, in particular, can be a cost-effective way to ensure that votes cast are votes counted."[23] The Committee recommended that audits, "must be conducted after each election, as part of a comprehensive audit program," and specifically endorsed risk-limiting audits, writing, "Risk-limiting audits are a best practice to mitigate risk."[24] Similarly, the National Academies of Science, Engineering, and Medicine's 2018 consensus study report on election security advocated for using risk-limiting audits.[25] Again, Alaska's statutorily directed regional vote counting system would require a hybrid adapting of any risk-limiting audit implementation.

Permanent Fund Dividend (PFD) Automatic Voter Registration

In 2016, Alaska voters approved Ballot Measure 1 (15PFVR), which either automatically registers eligible applicants to vote or updates voter registration information for those voters who are currently registered to vote using the information provided when applying for a PFD, unless the applicant opts out.

After the March 31 PFD application deadline, the DOE sends a notice to all applicants who will either become a newly registered voter or who will have their Alaska residence address updated from the information provided on their PFD application. To opt-out, applicants must respond to the notice within 30 days. Once the 30-day deadline passes, new applicants are registered to vote and applicants with a change of address are updated. New voter cards are then mailed to those voters who are newly registered or have a change of address.

[23] https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.
[24] *Id.*
[25] https://www.nap.edu/read/25120/chapter/7#95.

The law creating the PFD automatic voter registration program went into effect on March 1, 2017, and the PFD application period ended on March 31, 2017. For this period, approximately 158,000 Alaskans applied—roughly 76,000 of whom received a mailer informing them that their voter records were changed.[26] Applicants who listed an undeliverable address were still registered, and many were sent a mailer; however, applicants who were ineligible to register were not sent a mailer. Because of the way some applicants provided information on the PFD application (e.g., incorrectly spelling a street name), the new voter records were not always easy to add to the DOE's database.

During our review, we found the PFD automatic voter registration program has caused a myriad of unforeseen problems. To begin, the DOE did not receive any budget to implement or continue the new process; however, as seen in the figure below, the DOE has spent a considerable amount of staff time and funds implementing the initiative. The total cost of the program has been approximately $1.5 Million dollars, with only 4,639 new voters added who have voted. The DOE reported excessive costs and other challenges with the Automatic Voter Registration Program. During the 2020 legislative session, the DOE proposed amendments to the program, specifically allowing an opt-out at the front end of the process versus the back end; however, they were not implemented.

Figure 1. PFD Automatic Voter Registration Numbers

By the Numbers – Statistics Since 2017	
317,743	Opt-out notices mailed to potential new applicants and existing voters with a change to residence and/or name information
61,183	Opt-out notices returned requesting to opt-out of program (20,095 from new applicants/41,088 existing voters)
64,583	New voters added (Since 2017)
4,639	Number of new voters added who have voted
$683,457	Costs for printing, mailing notices and personnel time ($343,205 printing and mailing/$340,252 personnel)
$800,00	Approximate cost for initial programming
$319	Approximate cost to the state per new vote
Total Cost to Date: $1,483,457	

One of the reasons the program is so resource-intensive is because it relies heavily on manual procedures, even though the law is referred to as "Automatic Voter Registration." After the online registration is complete, DOE must spend time processing many voter registrations

[26] Alaska's Election Policy Work Group; "Improving Alaskan Elections: 2018 and Beyond" January 2018.

using manual procedures. For example, in 2017 close to 27,300 records required manual processing, representing about 17% of the automatic registrations.[27]

Another problem occurs when voters enter an address on their PFD registration application that is different than their current physical address. A local registrant experienced this issue when he entered his business address instead of his home address on his PFD application. This automatically switched him to a district he should not have been qualified to vote in. He only discovered this after it was too late to change his voting district and therefore was not able to cast his vote.[28]

An additional problem with the program is that felons and non-US citizens have been automatically registered to vote after they file for their PFD. This issue was not identified until 2018. DOE said that it is difficult to catch these ineligible voters in the data because DOE does not receive the PFD data until July. In an election year, that does not allow the DOE much time to compare voluminous records and notify voters in advance of the election. The DOE is aware of this problem and is working with the Department of Revenue to solve this problem.

The Department of Revenue (DOR) added "US National" to their application to assist with accurately identifying US Citizens. The DOE said it also requested that a felony voter question be added; however, DOR did not want it added to their pages.

The DOE created a voter registration page and added a question related to felony conviction for purposes of registering to vote. However, this new page is voluntary and not required to be completed as part of the PFD-AVR process. A reporting requirement mandated by statute might be necessary to resolve this problem.

The DOE mentioned that an online "opt out" option for automatic voter registration should be included at the beginning PFD application instead of at the end of the process in the form of a mailer. This could help eliminate unnecessary redundancies and mistakes in voter registration. The "opt out" could include a statement warning non-eligible individuals against failure to "opt out."

DOE interviewees expressed concern that the State has expended substantial effort and expense on the PFD Automatic Voter Registration program for marginal results with only a small increase in voter participation.

Voter Trust in Elections Starts with Cybersecurity

Due to attempted attacks on U.S. elections in 2016 by foreign sources, Alaskans and all Americans have raised concerns over security of the election process. It is critically important to promote voter confidence in Alaska's elections while maintaining adequate access for voters. Election security is not a partisan issue, as noted by the chairman of the U.S. Senate

[27] *Id*.

[28] The voter failed to respond to the mailer from DOE.

Select Committee on Intelligence, Senator Richard Burr: "Russian activities during the 2016 election may have been aimed at one party's candidate, but in 2018 and 2020, it could be aimed at anyone, at home or abroad."[29]

On November 8, 2016, the SOA Chief Security Officer at the time, Chris Letterman, reported that at 5:37am his office was notified via an alert that an unknown individual (@CyberZeist twitter handle) had posted a screen shot from what appeared to be a compromised Alaska Division of Elections reporting system.[30] Although the unknown individual claimed to have accessed the election management system, there is evidence they only accessed the public facing unofficial results section.

Letterman further reported, in pertinent part:

1. The individual successfully executed an exploit to PHP (a computer scripting language used heavily in web presentation)

2. The individual was able to use privilege escalation to access the server' s underlying file system.

3. The individual posted to their Twitter account a screen shot from the GEMS Election Results System as proof they were capable of accessing administrative areas of the server.

4. Along with the screen shot, the following message was posted "#USElections2016 Alaska Election Division online #ballot administrator access #pwned waiting for people to start voting"

The DOE subsequently admitted that "CyberZeist" successfully accessed an elections web server during the 2016 election. Regardless of any distinction between scanning versus an actual attack or hacking attempts, the State of Alaska and DOE has recognized that a successful attack was made on the SOA Election web server. Nationally, there is growing concern that foreign powers are increasingly interested in compromising US election processes and undermining voter confidence.[31]

On 09/22/17, the Anchorage Daily News published that Russian "cyber actors" made an unsuccessful attempt to access Alaska's voter registration database last year, state officials said Friday, citing information they received from federal officials. Alaska was one of 21 states possibly targeted, said Josie Bahnke, the state elections director, in a prepared statement. She added that Alaska's election systems were not "compromised," according to information her office received from the U.S. Department of Homeland Security.[32]

[29] https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/.
[30] Email from Chris Letterman to Jim Steele dated 11/08/16.
[31] https://www.adn.com/politics/2018/05/07/hackers-broke-partway-into-alaskas-election-system-in-2016-officials-say-no-damage-was-done/
[32] www.ktuu.com/content/news/Alaska-was-unsuccessfully-targeted-by-Russian-Cyber-Actors-in-2016-election-446954033.html

DHS Makes Cybersecurity Findings and Offers to Conduct Security Risk Assessment

On September 22, 2017, the U.S. Department of Homeland Security (DHS) notified 21 states they were targeted by foreign hackers during the 2016 election: Alabama, Alaska, Colorado, Connecticut, Delaware, Florida, Illinois, Maryland, Minnesota, Ohio, Oklahoma, Oregon, North Dakota, Pennsylvania, Virginia, and Washington.[33] Ultimately, hackers only reportedly succeeded in breaching the voter registration system of one state: Illinois. While DHS did not name those responsible for the attempted hacks, many believe the culprits can be traced back to Russia. Experts have warned that a future attack on United States' election infrastructure, by Russia or other malicious actors, is all but guaranteed.[34]

After determining Alaska's election system was scanned by a foreign entity, DHS offered multiple times to conduct a Risk and Vulnerability Assessment at no charge to the State. Such a review would assess potential vulnerabilities in the DOE's voting system that could be exploited by a foreign nation-state seeking to infiltrate and manipulate it.[35] However, the DOE declined DHS's offer. When we inquired about why, the DOE expressed concern that conducting any assessment would have a detrimental effect on staff time and would require multiple layers of authorization, including from OIT. DHS, on the other hand, requires an invitation from the DOE to conduct such an assessment. To date, the assessment has not been done, and the DOE has not provided a timeframe for when they will allow the such a comprehensive risk assessment to be conducted.[36] However, the DOE allowed DHS to assist in conducting a Cyber Hygiene survey in 2016, and it participated in two "Tabletop the Vote" national election security tabletop exercises with DHS. Aside from these activities, no further cyber security assessments have been accepted or performed by DHS or by the SSO.[37]

Based on foreign actor activity regarding elections, DHS offered multiple services to assist Alaska Elections. According to the DHS Alaska website: "The goal of the Cyber Security Assessment is to improve the overall security of critical cyber infrastructure throughout the State of Alaska in all 18 Critical Infrastructure and Key Resource (CIKR) Sectors. The assessment process is a non-regulatory review of cyber security management practices within the organization to build a risk matrix, threat indicators, maturity model, prioritized recommendations, and is overall designed to build the relationships necessary to foster cooperative arrangements during both normal operations and in times of crisis. The Cyber Security Assessment is not an examination of all the IT business operations or a technical assessment. It does not satisfy compliance towards any specific regulatory authority nor does it force an organization to take corrective action based on the results."[38]

[33] Arizona, California, Iowa, Texas, and Wisconsin were also among those states originally contacted by DHS. However, those states have denied that their election systems were attacked.

[34] Ibid.

[35] A Risk and Vulnerability Assessment allows selecting from a menu of several network security services, including network mapping and vulnerability scanning, phishing engagements, web application or database evaluations, and full penetration tests.

[36] Information provided by the SOA OIT on 06/09/20 with supporting documents.

[37] Ibid.

[38] https://www.ready.alaska.gov/Plans/CSVA

In a July 2019 discussion with the DOA Commissioner, the CISO suggested engaging DHS as a neutral 3rd party to conduct a security review of the DOE systems in advance of the election. The SSO reached out via email to DHS on July 11, 2019 to seek engagement to perform the review. Via a phone conversation, DHS later informed the CISO that the SSO/CISO had no authority to approve/engage them in a cybersecurity review of the DOE since it is under the purview of the Lt. Governor. As a result, DHS could only provide "observations for consideration" and wait to be invited by the DOE/Lt. Governor's office to conduct any engagements.[39]

In March of 2019, OIT provided testimony during Legislative session regarding questions about Election security. OIT responded to questions about support, indicating that support was provided at an Enterprise level, while DOE-specific applications and systems were managed by DOE internal staff. Following that testimony, the SSO informed us it contacted the DOE in the interest of conducting a security review and was informed, again, that the DOE manages its own security independent from the SSO. The SSO was further informed that the SSO had no authority with DOE or the Governor's Office IT systems.

With respect to the DHS Risk and Vulnerability Assessment availability, the DOE provided the following information or explanation as to the reasons it has not been performed:

"A DHS assessment has a lot of technical matters that consume staff time and also due to our interconnectivity with OIT, it requires them to be on board with it and being able to allocate appropriate staff and resources as well. It involves multiple layers of staff and coordination of time and resources. The division has no reluctance to entering into agreements to have services provided by DHS. These do require a signed authorization by the CISO."[40]

Contrary to the comments made by the DOE that an assessment "requires a signed authorization from the CISO or SSO," we found this is incorrect. There is no such policy/statute or Administrative Order that enforces or requires the DOE or the Lt. Governor's Office to obtain approval from the CISO or SSO.[41] We also found the CISO was interested in pursuing and fully recommended to the DOE that such an assessment be performed. However, the DOE never followed-up with the recommendation.

At the time we were concluding this review, the DOE was working with DHS on a more limited-scope Phishing Campaign Assessment.[42] A Phishing Campaign Assessment only measures DOE staff's propensity to click on e-mail phishing lures. Phishing is commonly used to breach an organization's network. The assessment results can be used to provide guidance for anti-phishing training and awareness.

We found that OIT was on board and had the resources for the DHS assessments it was advocating. We also found the CISO not only would have authorized the assessments, but was

[39] Ibid.
[40] 05/20/20 comment made by the DOE on O&R's draft report.
[41] Information provided by CISO/SSO with supporting email communications.
[42] While interviewing Gail Fenumiai, she stated she had spoken with DHS prior to our discussion.

initiating them by contacting DHS himself. An evaluation of the evidence indicates the DHS Risk and Vulnerability Assessment or other in-depth DHS cybersecurity assessments did not occur because they were declined or otherwise not authorized by the DOE, seemingly because conducting any assessment would have a detrimental effect on DOE staff time.

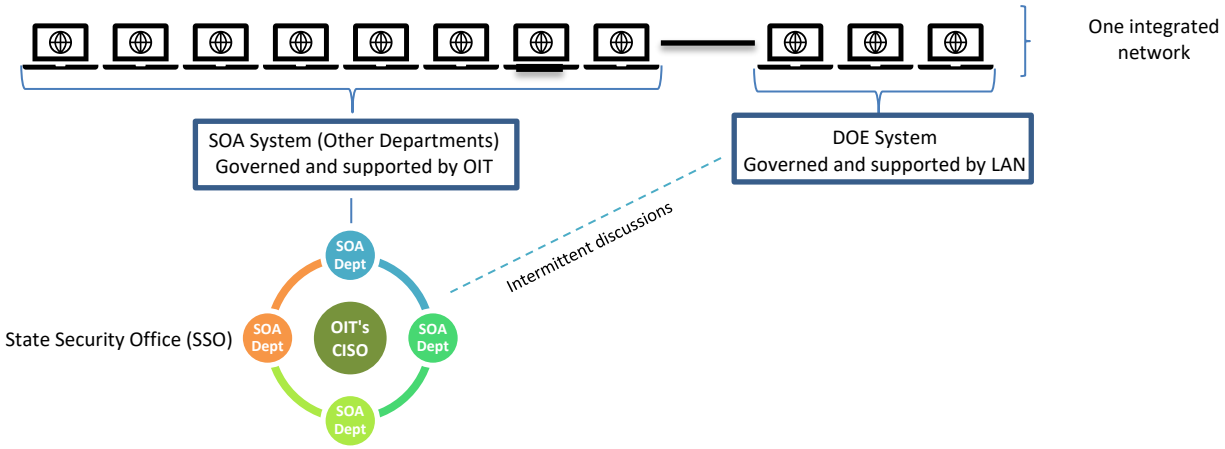
The DOE's Cybersecurity Governance and Coordination with the State Security Office (SSO)

The DOE is housed in the Lieutenant Governor's Office, but the SSO is housed in the DOA's OIT. Broadly, the SSO oversees State of Alaska security policies and implements standards and procedures in support of those policies. The SSO works through the Chief Information Security Officer (CISO), who oversees and facilitates statewide security management programs to ensure government information is adequately protected.

While DOE exists on the State's physical network, in reality, DOE's system is functionally segmented so the SSO has no visibility or access to the Elections environment or systems and no authority to audit or scan for security compliance. The DOE's cybersecurity decisions are not ultimately governed by the SSO or facilitated by the CISO, but made by the Governor's Office's Local Area Network (LAN) Administrator. The LAN has the authority whether or not to implement SSO security software or recommendations, or to find other ways to be compliant with SSO standards.

Below is a diagram of the governance structure for the DOE's IT system.

Cybersecurity Decisions for IT Systems in the State of Alaska



When we asked the DOE about its understanding of its coordination with the SSO and cybersecurity governance, DOE provided the following information: "Ultimately all of DOE systems fall under the CISO. For example, that is why we have things like CyberReason. It is [the LAN's] job to keep us compliant with the SSO/CISO. We believe that per AO 284, OIT is responsible for security at the statewide level."

In response to the DOE's comment above, the SSO provided the following information:

"*This statement reveals the heart of the issue... This statement, and variations of the same has been made many times as a mechanism to transfer risk and accountability while maintaining departmental control and authority…*

In April 2017, AO 284 was issued to consolidate IT functions and services throughout the state. The primary focus and language were to centralize all telecommunication and information technology services and consolidate them under the authority of a single Office of Information Technology (OIT) headed by the Chief Information Officer (CIO). As written, AO 284 places cybersecurity under the purview and management of OIT and explicitly the CIO. Article 9 identifies a position of Chief Information Security Officer (CISO) to, "assist the CIO in carrying out the CIO's duties; while not codifying the role nor delegating any authority.

In 2018, the inaugural Cybersecurity Report was delivered to the Governor. The report summarized the five key issues:

> *1. **Statute Updates** - Update Alaska's statutes to emphasize cybersecurity as a public interest to lessen chance of bureaucratic recidivism and provide an important complement to policies and standards developed by the OIT.*
> *2. **CISO Role Codified** - Codify the role of the Office of the Chief Information Security Officer (OCISO), and management of privacy and data security, as a significant step toward mitigating potential loss of focus on the Governor's policy direction to deliver assured cybersecurity outcomes.*
> *3. **Quarterly Meetings** - CIO to meet with the Governor quarterly to review cybersecurity status.*
> *4. **Governance and Compliance** - Implement robust, cabinet driven cybersecurity governance and compliance. Meet with OIT quarterly to review progress and needs.*
> *5. **Reorganization and Investment** - Support reorganization of existing funding, assets, and personnel resources to accomplish investment in cybersecurity priorities.*

To date, none of these key initiatives have been realized or resolved. Thus, the actual condition of cybersecurity at the State is:

- *The CISO/SSO is accountable for security and compliance throughout the state but has no authority or ability to fulfill the role or responsibilities. No statute or AO exists that empowers, codifies, or establishes the CISO/SSO.*
- *Under AO 284, the CIO is functionally the CISO/SSO (see CIO Responsibilities on Appendix B). Due to the major challenges of centralizing and consolidating IT systems and services, there is a lack of focus on cybersecurity. Additionally, a conflict of interest exists as OIT should not serve as both the owner/manager of state IT systems, as well as the auditor/certifier of compliance for the services and systems within its purview.*
- *There is no compliance, Internal Audit, or enforcement organization within the state. As a result, departments independently pursue cybersecurity compliance goals and objectives with no oversight or accountability.*

- *There is a lack of dedicated funding for cybersecurity. No formal budget exists for the CISO/SSO and existing funding is at the discretion of the CIO/OIT. This has led to the continued erosion of the CISO/SSO group, while simultaneously departments are hiring cybersecurity staff out of necessity and in alignment with their own specific departmental goals and objectives.*

…In short, the DOE and the LAN Administrator make their own independent decisions concerning cybersecurity. The DOE does not coordinate with OIT on cybersecurity until after it has chosen a product or made a security decision. This has often resulted in the SSO having to alter or accept waivers for non-standard applications or configurations. It also means that at the time of our review, the DOE did not have a written plan for future security improvements for its election system."

The CISO for Alaska explained that the DOE's lack of involvement and coordination with the SSO promotes an atmosphere of non-standardization and independence from the SSO and the statewide approved cybersecurity standards. As a result, the SSO has no visibility into the DOE, but the SSO is called upon to testify before the legislature regarding the adequacy of DOE elections cybersecurity and how the SSO is supporting DOE's systems.

For example, historically, DOE and the Governor's Office have procured solutions prior to communicating with the SSO. This also has resulted in instances of non-standard/non-compliant systems being implemented. However, the SSO reported that, in general, there now is agreement that communication and coordination with DOE and the SSO should improve over time. The DOE and SSO/CISO recently started meeting monthly to discuss statewide security and elections security.[43]

We also found the SSO does not have monitoring software installed on DOE machines, although DOE believed the SSO did. The SSO stated that it only provides antivirus (Cybereason) and anti-malicious Internet protection software (Zscalar).[44] We also found the SSO does not perform monitoring of the DOE's election systems, even though the DOE mistakenly assumes the SSO is monitoring the systems.[45]

We identified a best practice for elections security is to have the State CISO integrated into oversight of the elections system. The CISO for Alaska told us other states integrate their CISOs into their election security, and the Center for Internet Security (CIS) suggests that CISOs should be utilized in assisting to secure elections.[46] From our research, it appears anomalous to have a state election system's information security governance and practices completely segregated and disunified from those established and facilitated by the CISO.

[43] In March of 2019, the CISO/SSO attempted to establish a State Security Council to create a statewide cybersecurity governance group and foster statewide communication and collaboration of cybersecurity concerns and interests. Per management directive from the former CIO, the group was disbanded in 2019. A smaller, informal group within the state organization currently meets every two weeks.

[44] Information provided by the SSO in response to DOE's comments submitted to O&R.

[45] Information provided by the SSO in response to DOE's comments submitted to O&R.

[46] CISA Handbook for Elections Infrastructure Security (2018)

We found that while the DOE believes the CISO/SSO "has the final authority for any IT system," the DOE systems are not monitored by the SSO, DOE procures IT systems or software without first ensuring with the CISO that it complied with cybersecurity standards, the DOE had not implemented security recommendations strongly made by the CISO, and the SSO/CISO currently has no authority or control over any Elections systems.

Allegations of IT Vulnerabilities in DOE Systems

During this review, we received allegations from a private company that while conducting scans of electoral systems in the United States, they found access points an attacker could leverage to access Alaskans' personally identifiable information (PII).

We worked with the SSO to conduct a review of the alleged vulnerable access points and determined the firewall on the identified IP address was blocking penetrations. We also found the sites allegedly leading to Alaskans' information did not connect to any databases containing PII. Prior to this event, the SSO was working with the DOE to schedule a credentialled vulnerability scan. That scan found that in general, the system is secure, but it has a few vulnerabilities. The SSO will follow up with the DOE to remediate issues and ensure other controls are in place.

Allegations of Elections Fraud and Misconduct from the 2010 General Election

In 2010, Joe Miller won the primary election race against incumbent candidate Lisa Murkowski for U.S. Senate. However, Lisa Murkowski ran for U.S. Senate in the general election as a write-in candidate, and she prevailed over Joe Miller. Joe Miller challenged the results of the election in a lawsuit, he filed against the DOE in the Alaska Superior Court. Superior Court Judge William B. Carey upheld the DOE's actions. Miller appealed, and Murkowski cross-appealed. The court ruled in favor of Murkowski and she won the general election—an event that fractured the Alaskan GOP in ways that have not reconciled to this day.[47]

While conducting this review, we received allegations against the DOE in the form of numerous affidavits signed by multiple poll workers that were filed with the Court in support of Mr. Miller's case. These affidavits alleged violations of DOE's policies and procedures, including improper or negligent oversight provided by the current DOE Director. Many of the witnesses who signed these affidavits appear to have been election workers helping Joe Miller with the post-election ballot reviews. We also received information that some of these issues were not addressed by the Court system during the Miller court cases, and they still persisted in the DOE system and processes today.

Specifically, most of the affidavits alleged fraud or misconduct may have occurred during the post-election ballot reviews through various methods, including, but not limited to:

- repeated similar signature styles on ballots
- ballot tampering by alterations

[47] https://mustreadalaska.com/pressure-builds-on-pivotal-decision-of-lisa-murkowski/

- ballot box stuffing
- improper ballot challenge approvals by the Director[48]
- inadequate security measures
- violations of DOE procedures

We examined these allegations, whether in fact they were addressed by the Court system, and whether internal controls are now in place at the DOE to protect against such election fraud or misconduct.

Background on the 2010 Post-Election Ballot Review

After the ballots were sorted during the post-election ballot reviews, the Director personally examined: 1) the ballots on which ovals had been filled in, but the handwritten name was a variation or misspelling of "Lisa Murkowski," and 2) other ballots challenged during the sorting process to determine voter intent.

Mr. Miller challenged ballots cast that contained misspellings of "Lisa Murkowski." The Director examined these ballots and permitted write-in ballots containing "minor misspellings and phonetic variations of `Murkowski' to be counted for Lisa Murkowski when [she] determined that the voter clearly intended to vote for that candidate."[49] The Director placed the ballots into one of two envelopes: "challenged counted" or "challenged not counted."

Director Fenumiai also examined ballots in which no oval was filled in for the U.S. Senate race, and those ballots were not counted for any candidate. This was true of ballots on which voters spelled "Lisa Murkowski" correctly but failed to fill in the oval. Murkowski argued that these votes should have been counted for her, but the court disagreed. Alaska Statute 15.15.360(a)(10) states that "[i]n order to vote for a write-in candidate, the voter must write in the candidate's name in the space provided and *fill in the oval* opposite the candidate's name." (Emphasis added.)

Director Fenumiai also examined "over-voted ballots" with more than one oval filled in to determine voter intent. As Director Fenumiai explained in an affidavit submitted to the court:

> "I did not count ballots that had no oval filled in for the U.S. Senate race, even if a name was written in. If a ballot had two ovals filled in for the U.S. Senate race, I examined the ballot to see where the ovals appeared. If the voter had filled in the oval by the name of a candidate printed on the ballot and by the write-in choice, I counted the ballot if the voter wrote in the name of the same candidate. This is how Joe Miller received many of his 20 write-in votes. I also counted ballots with two ovals marked when it was clear that the voter crossed out one of the ovals. I did this regardless of whether the voter expresses an intent to vote for a write-in candidate or for a candidate whose name was printed on the ballot. Otherwise, I did not add the ballot to

[48] Gail Fenumiai was the Director of the DOE at the time of the 2010 election.
[49] Miller v. Treadwell, 245 P. 3rd 867 (2010).

the count. The candidates' observers were able to challenge all of these determinations."

Joe Miller also sought from the court an interpretation of election statute AS 15.15.360 that would disqualify any write-in votes that misspelled the candidate's name. However, the court held that its prior decisions clearly show that a voter's intention is paramount. Therefore, the court held that abbreviations, misspellings, or other minor variations in the form of the name of a candidate would be disregarded in determining the validity of the ballot, so long as the intention of the voter could be ascertained.[50]

Court Rulings on Allegations Presented in Affidavits[51]

Through the Superior and Supreme Court cases, we found that concerns raised in the affidavits were addressed, and the court ruled in favor of the DOE. Also, we found that the Superior Court ruled the affidavits inadmissible as hearsay.

The Superior Court denied Miller's request for discovery and granted the State's motion for summary judgment, noting that the admissible portions of Miller's evidence did not create a genuine issue of material fact regarding misconduct by anyone, and that it was not even sufficient circumstantial evidence to warrant discovery before ruling on the summary judgment motion.

The court explained that AS 15.15.240 allows any qualified voter to ask for assistance, including assistance in writing in the name of a write-in candidate. No reasonable inference of misconduct can arise from the mere fact that the handwriting on multiple ballots appears to be similar or coming from a small number of people.

Miller argued that the court's interpretation of AS 15.15.360 would lead to elections being decided by the discretion of election officials in determining voters' intent through visual inspection of write-in ballots. However, the court noted that other states use the same standard for counting write-in ballots, and that Congress has mandated that standard.

The court also saw no validity in Miller's argument that the application of the standard in the election violated equal protection under either the state or federal constitutions. The court clarified in its decision that only one person, the Division's Director, made the initial determinations whether write-in ballots demonstrated voter intent for a candidate. This avoids any constitutional infirmities that might arise from different reviewers applying the standard differently. Second, the initial election results were subject to the Director's review during a recount. Finally, the Director's final determinations are subject to judicial review.

[50] The federal Uniformed and Overseas Citizens Absentee Voting Act also provides that in counting the ballot of a uniformed services voter or other voter who is overseas, "[a]ny abbreviation, misspelling, or other minor variation in the form of the name of a candidate or a political party shall be disregarded in determining the validity of the ballot, if the intention of the voter can be ascertained."

[51] Miller v. Treadwell 245 P.3d 867 (2010).

For the reasons set out above and for other reasons beyond the scope of this report, the Alaska Supreme Court affirmed the decision of the Superior Court in all respects. It also concluded that there were no remaining issues raised by Miller that prevented the 2010 election from being certified.

Findings Regarding 2010 General Election Allegations

We determined that the allegations in the affidavits within the scope of this review either: a) were addressed by the courts, or were b) no longer are of concern because of internal controls and procedures now in place within the DOE. We requested documents related to the 2010 election dispute, but the DOE said it did not have any because retention policies required the destruction of records after 7 years. So, we were unable to review any records that would have been in possession of the DOE regarding these allegations.

Recent and Ongoing Changes within the DOE

The DOE has finalized the purchase and replacement of its existing, outdated voting equipment. This new system is a federally certified voting and ballot tabulation system for the 2020 election cycle. The August 18, 2020, State Primary Election will be the first election in which this new equipment is used.

The DOE recently implemented reCAPTCHA[52] to protect the online voter information system from automated abuse. The DOE also created a new spoiled ballot log to assist with better tracking of ballots at voting locations. In addition, the DOE has adopted regulations raising election worker pay; the most recent previous pay raise was in 2009.

The DOE also indicated it is in the process of making the following improvements:

- Adding two-factor authentication for the Voter Registration System users.
- Replacing aging hardware and software in the voter registration system. Including firewalls, servers, etc.
- Developing an online absentee ballot application system.
- Purchasing a new online ballot delivery system.
- Improving the chain of custody procedures for voted ballots.
- Returning all unused ballots to the Director's office following each election.
- Conducting a DHS Physical Security Assessment.
- Performing voter outreach regarding trusted source for election information.
- Conducting information integrity operations.
- Improving election worker training materials and videos.
- Providing staff election security training (both federal and state trainings, as well as private sector trainings).
- Introducing an Adopt-A-Precinct program in the hopes it will help with election worker recruitment.

[52] reCAPTCHA is a free service from Google that helps protect websites from spam and abuse. A "CAPTCHA" is a truing test to distinguish between humans and bots.

- Reviewing procedures and revisions as needed due to implementation of new voting and ballot tabulation system.
- Improving the felony conviction monitoring system.
- Enhancing network monitoring tools for voter information systems.

In addition, the DOE continues to focus on:

- Verification of voter identity when processing voter registration, absentee ballot applications, voted absentee and questioned ballots.
- Monitoring and contacting voters regarding returned undeliverable ballots.
- Conducting extensive training for all temporary staff who process voter registration and absentee by mail ballot applications, including conducting audits of their data entry.
- Maintaining secure areas for ballot storage and election equipment.
- Its partnerships with DHS, DOA OIT, the LAN Administrator, and system vendors related to security of Alaska's election systems.
- Monitoring best practices recommended by the U.S. Election Assistance Commission, National Institute of Standards and Technology, the Cybersecurity, and Infrastructure Security Agency, MS-ISAC and EI-ISAC.
- Integrating PFD non-citizen information; and
- Participating in national election security tabletop exercises.

RECOMMENDATIONS

To improve the effectiveness of the DOE's security and efficiency in administering elections, we make the following recommendations:

1. **Consider Implementing Signature Comparison Software**. This software can be used as another layer of defense against voter fraud. The software would automatically compare a voter's signature to a database of previously recorded signatures available in public records. This extra layer of verification would also alert staff to potential fraudulent ballots without having staff spend the time to find the error manually. This software could also be used for signature verifications on Alaska petitions. Automated Signature Verification is used successfully by banks to evaluate signatures on checks. It also is used in others states like Oregon, Colorado, Washington, and Utah for signature verification during elections. Implementing signature verification may require a statutory revision.

2. **Create a Vendor Risk Management Policy**. A Vendor Risk Management Policy creates guidelines in IT acquisitions to ensure that third-party vendors are not introducing security gaps that can be exploited to stage an attack. As part of the policy, the DOE should request that their vendors:
   a) Provide a copy of their Information Security Policies and Plans to determine whether the vendor practices reasonable security measures.
   b) Allow periodic evaluation and information gathering on how they protect information and systems.
   c) Have documented controls or procedures on how they secure USB devices and any associated removable media.
   d) Document how the vendor will support the organization during execution of a Continuity of Operations Plan.

   At the time it acquired the new Dominion voting machines, the DOE did not have a vendor risk management policy in place that it could implement. We recommend the DOE develop a vendor risk management policy it can apply in future procurements with third-party vendors. It may be appropriate for the State to consider a state-wide Vendor Risk Management Policy.

3. **Continue to Monitor and Improve the Process to Ensure Voter Rolls are Current and Accurate**. We found different examples of when someone should not have been allowed to vote (i.e. convicted felon), and other times when someone should have been able to vote but was unable to. Accurate voter information is foundational to establishing voter trust in the election process and should be a top priority. We recommend the DOE continue to develop a sufficiently resourced, sustainable, repeatable process for ensuring voter rolls contain current and accurate information about voters and their eligibility to vote.

4. **Develop Policy, Procedures and Training for Voter Fraud Prevention and Response**. The DOE does not have any written policies on voter fraud prevention or response. As a result, the DOE staff are left to identify and respond to voter fraud issues based on their experience and expertise, which can lead to subjective, inconsistent, and inadequate responses. The DOE should develop fraud response policies and procedures, and conduct training for all staff members to ensure potential fraudulent votes are dealt with appropriately. The DOE should not rely solely on employees' experience and instincts for identifying voter fraud. The DOE reported that it is reaching out to the National Association of State Election Directors to research other states' best practices. While the DOE does not have the authority to investigate fraud, it is in the best position to see and identify voter fraud when it is occurring so it can refer it to law enforcement authorities for investigation. The DOE should continue to explore best practices, viable fraud detection software, or educational resources to strengthen its ability to detect and deter voter fraud. The DOE also should provide pre-election training to DOE staff who are tasked with preliminary fraud detection responsibilities.

5. **Recruit a Bench of Back-Up Election officials.** The DOE would benefit from having a consistent source of election officials for all polling places across the State. We recommend the DOE use new, innovative methods to recruit a volunteer bank of election workers to serve in polls. We recommend more poll election officials be trained in advance to work the elections than are needed on election day, so that if an election official is a no-show on election day, a trained back-up election official can go in their place. Election officials could possibly be recruited from local off-duty Alaska National Guard members, off-duty VPSOs, the Alaska State Defense Force volunteers or local village/city off-duty employees. Respective Alaska Native Corporations or Tribal Organizations might also be potential resources for recruitment. The DOE has started a program to recruit state workers as election officials, and it reported it will introduce an adopt-a-precinct program as well.

6. **Employ Risk-Limiting Audits to Validate Election Results.** Risk-limiting audits are designed to limit an audit to a statistically predetermined level of confidence that the reported result is correct. This methodology also conserves staff resources by reducing the number of ballots that require auditing, while also providing statistical confidence in the election result. We also recommend the DOE pursue a legislative amendment to allow it to develop a comprehensive audit program to mitigate risk in the elections system.

7. **Audit Precincts in which Unexplained Discrepancies Occur.** We found the DOE did not audit precincts in the 2018 election with reports of unexplained discrepancies, missing ballots, or voting irregularities. We recommend the DOE exercise its authority under AS 15.15.430 (c) to audit ballots in precincts such as these. Episodic auditing of precincts representing less than 5% of the votes cast in districts would deter attempts to manipulate elections through fraudulent voting in those districts. We further recommend that the HCVP be required in every precinct that reported problems

during the election that could have influenced the final vote count. This recommendation would require a statutory change.

8. **Consider Implementing HCVP of All Precincts Using Optical Scan.** We found the DOE uses the HCVP only in precincts that use optical scan, and account for at least 5% of the ballots cast in that district. We recommend a hand count verification of all precincts using optical scans, regardless of the percentage of votes for which they account, in order to confirm the accuracy of the vote and increase voter trust in the elections results. This recommendation would require a statutory change.

9. **Continued Review of Making Vote by Mail a Possible Alternative to In-person Voting in Non-road Connected Rural Areas May be Merited, but Faces Serious Difficulties.** The issues reported during the 2018 election are not new: similar problems plague rural-area elections every election cycle. While many of the precincts in these rural areas do not have many eligible voters, [53] the state's current method for administering elections requires each precinct to have touch screen voting units and election workers available on election day. As noted above, this presents logistical and financial challenges for the DOE.

   Some parts of the state use vote-by-mail (VBM) systems for local elections.[54] Using a hybrid in-person and by-mail approach might be considered to maintain the current electronic system in urban areas while allowing rural areas to use an approach that would minimize machine malfunction, volunteer absenteeism, risk of votes not being counted, and complaints against the DOE. However, using VBM systems in a statewide election has very different challenges than using them in local elections.

   VBM also is very controversial, and without extensive safeguards, will be vulnerable to substantial voter fraud. [55] For example, the former Nevada Attorney General, Adam Laxalt, has discussed publicly seeing, "videos of thousands of ballots that are piled up in apartments and trash cans and in hallways. And this is all because we are doing our first mail-in ballot election in the history of our state all under the cloak of the pandemic."[56]

   It is likely that the safeguards necessary to protect against voter fraud may make VBM in rural communities too difficult. At the minimum, a double authentication system like the one used by the Social Security Administration would be essential. Possibly this could be facilitated through voters' "My Alaska" accounts. Enhanced criminal penalties for "ballot harvesting" and voter intimidation would also be advisable to protect the

[53] Of the 438 precincts in Alaska, 31 have 100 or fewer registered voters.

[54] The Kenai Peninsula Borough uses a hybrid in-person and by-mail system in which smaller communities, like Cooper Landing, Hope, and Tyonek, vote by mail. Perceptions of Universal Ballot Delivery Systems – Findings from a Survey with Registered Voters In Three Areas In Rural (Region IV) Alaska

[55] US Election Assistance Commission; https://www.eac.gov/election-officials/voting-by-mail-absentee-voting National Conference of State Legislators; https://www.ncsl.org/research/elections-and-campaigns/all-mail-elections.aspx; Brennan Center for Justice; https://www.brennancenter.org/our-work/research-reports/why-vote-mail-option-necessary.

[56] See https://www.foxnews.com/media/nevada-adam-laxalt-mail-in-voting-election-fraud.

integrity of any VBM system. Dedicated independent prosecution resources would also need to be provided to prevent any possibility of a lack of voting crime prevention, investigation, and enforcement. To ensure voting integrity with a Rural VBM System, the DOE also would need improved systems of list maintenance, ballot tracking, liaising with the Postal Service, signature verification, and the ability to conduct public outreach on short notice.

Best Security Practices for rural VBM would also include:[57]

- Double signature and identification authentication system.
- Non-USPS drop boxes for ballots.
- Centralized methods for counting ballots to increase cost efficiencies and process/security oversight.
- Proactive registration address updates.
- Communications directly to voters including voter guides mailed to every household, texts on status of ballots, and deadline reminders.
- Using Ballot Tracking Software to follow a ballot from when it is printed, through the mail stream, to the voter, and back to the DOE.[58] Much like a FedEx package, the ballot comes with a barcode that allows election officials and voters to track where the ballot is throughout the process.
- Post-election audits such as the recommended Risk Limiting Audits can identify any irregularities that may remain.
- Because voted mailed ballots are stored for some length of time before the election is complete, physical security is essential. All ballots are currently stored in locked and alarmed ballot rooms. Security cameras, locks that need a bipartisan team to open, and logs of all activities relating to ballot handling can be part of a comprehensive ballot security effort for a VBM program.

It is possible that implementing a VBM system for rural communities could have the potential for litigation as Alaska would be treating categories of voters differently. However, we found Alaska is arguably treating categories of voters differently now—the issues identified in the 2018 primary and general elections indicate votes from several rural communities were not properly counted.

We do not recommend any state election VBM system currently. We believe essential safeguards and technology would be too costly and could not be implemented before the 2020 elections. Moreover, implementing a vote by mail system would likely require

[57] See https://www.eac.gov/sites/default/files/electionofficials/vbm/Signature_Verification_Cure_Process.pdf, https://www.eac.gov/sites/default/files/electionofficials/vbm/Ballot_Drop_Box.pdf, https://www.nass.org/sites/default/files/reports/nass-report-voter-reg-maintenance-final-dec17.pdf, https://www.eac.gov/election-officials/election-security-preparedness#_e9iputrr2xgp, https://www.electioncenter.org/publications/2010%20PPP/Denver_Election%20Paper%20Submittal_Ballot%20Trace_2010.pdf, https://www.brennancenter.org/our-work/analysis-opinion/smart-and-effective-way-safeguard-elections, https://www.eac.gov/sites/default/files/eac_assets/1/6/260.pdf.

[58] See, e.g., https://www.fastcompany.com/90501588/track-your-ballot-like-a-package-how-technology-will-smooth-the-way-for-novembers-mail-in-ballot-surge

a statutory change. Yet, a well-constructed VBM that integrates best security practices could be an alternative for resolving systemic voting challenges in rural communities.

10. **Re-Examine Rules Surrounding Absentee Ballots to Determine if Changes Can Be Made to Expedite Elections or Enhance Integrity of the Voting Process.** The DOE could remove requirements for affidavits or witness signatures on absentee ballot requests, and instead enhance the signature verification process by implementing the use of Signature Verification Software or double authentication. The DOE also could re-examine whether absentee ballots must be received by the close of polls on Election Day, or if they will be counted even if they arrive after. Late-arriving ballots can slow down election results reporting.

    We also recommend the DOE provide a notification process for voters if there is something wrong with their ballot envelope, and give them a chance to correct, or "cure," the ballot before the election is certified. Otherwise, the number of uncounted ballots will be higher for absentee/mailed ballots than for in-person ballots. Ballot Tracking Software would automate identifying ballot errors. The DOE also could reconsider whether to provide prepaid return postage in certain cities, and instead opt for providing secure drop boxes throughout the jurisdiction. This reduces the cost of providing postage for prepaid envelopes.

11. **Work with the Legislature to Repeal or Amend the Permanent Fund Dividend Automatic Voter Registration Program**. At minimum, the opt-out option for applicants should be placed on the PFD application to allow applicants to maintain their current voter information. The DOE also should work with the Permanent Fund Division in streamlining the information sharing to mitigate occurrences of having outdated voter information. We agree with the EPWG's 2018 report, that the goal should be automation of the Automatic Voter Registration Program, and this process should be paperless.

    Given all the problems created by PFD automatic registration, we recommend it should be discontinued unless the Legislature is willing to commit considerable financial support for its continuation and upgrade. No one who wishes to vote and can legally do so requires PFD automatic registration.

12. **Conduct DHS Security Risk and Vulnerability Assessment Testing.** The DOE already has initiated a DHS phishing test, but it should endeavor to enlist the help of DHS to conduct all available testing to identify gaps and deficiencies in both technical and procedural areas. The DOE also should conduct follow-up security assessments every 2-4 years. DHS recommends more frequent assessments if the political subdivision (DOE) has a significant change in structure or circumstance, such as purchasing new equipment, moving to a new office, or changing personnel. The DOE should review the results of the most recent risk assessments every year to ensure recommendations were effectively implemented and identify opportunities for improvement. The DOE reported that it is planning to pursue a DHS RVA post 2020 Election.

13. **Work with the SSO/OIT to Develop a Cybersecurity Preparedness Plan**.[59] The DOE should develop an official cybersecurity strategy. This should include a timeline for security improvements and specific dates for meeting those goals. It also should document areas of emphasis and security training. The DOE should organize the plan around the five security objectives established by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): (1) Identify, (2) Protect, (3) Defend, (4) Respond and (5) Recover.

14. **Give OIT Authority Over the DOE's Cybersecurity.** The DOE and Lt. Governor's office told us that it relies on OIT for the DOE's cybersecurity. However, as described above, we found OIT has no authority over the DOE's cybersecurity and instead the DOE and the LAN Administrator make their own independent decisions concerning cybersecurity for the DOE. Therefore, we recommend the Lt. Governor change the governance structure for the DOE's IT security so it aligns with the understanding and expectation that OIT is responsible and accountable for the DOE's cybersecurity.

15. **Create an Incident Response Plan**.[60] The DOE should create an incident response plan that documents the specific steps to take in case of cyberattack or other types of disasters. According to the SSO, divisions and departments are responsible for developing plans such as these for their own respective systems. Given that the DOE operates its system under the direction and authority of the LAN, the DOE would develop the plan in conjunction with guidance from the LAN. However, we recommend the DOE consult the SSO in developing the incident response plan as well.

    An incident response plan should include:
    a) A clear definition of what constitutes a cyberattack or incident.
    b) A classification system for the severity level of incident types and the appropriate notification and response protocol for each type.
    c) Incident containment processes that minimize the scale and scope of the damage; and
    d) Procedures for restoring systems and operations after an attack.

    At a minimum, an incident response plan should address the following incidents:
    a) Malware
    b) Ransomware
    c) Denial of Service (DoS) and Distributed Denial of Services (DDoS)
    d) Intrusion
    e) Information access
    f) Compromised data
    g) Insider threats
    h) Compromised accounts

[59] https://www.nist.gov/topics/risk-management
[60] Ibid

i) Loss or theft of election and/or computer systems
j) Social engineering attack
k) Data breach

16. **Consider Enlisting the Assistance of a 3rd Party Cybersecurity Provider for Enhanced Cybersecurity Options**. The private sector could be useful in providing additional security measures that the State of Alaska does not have the capabilities to provide. We recommend the use of dedicated cybersecurity personnel who focus solely on offering the best cybersecurity services available on the market. The private sector offers early adoption of emerging security tools that would be difficult to implement in the State of Alaska without a vendor assisting. The DOE has expressed confidentiality concerns about using third-party vendors; however, we found some other states are contracting with some private cybersecurity vendors and this concern could be addressed with an appropriate legally binding confidentiality agreement.

17. **Improve Collaboration Between the DOE and SSO**. The DOE and the state should consider adopting other states' best practice of instituting a policy of collaboration between the SSO and the DOE on cyber security decisions, policies, and procedures. With constant and increasing cyber-attacks across America, the DOE should look to partner with other security agents in the state to use a uniform approach to cybersecurity. Stronger oversight and collaboration between the SSO and DOE would enhance and improve the state's cybersecurity for elections. Collaborating roles and responsibilities should be codified to eliminate or reduce confusion. The DOE recently reported that monthly meetings have started. We recommend these meetings continue on a regular basis.

18. **Re-explore the Option of Securing Voting Equipment in Regional or Local Rural Precincts.** If this is an option, it would save the DOE a considerable amount of money in shipping costs, and prevent repeated damages to voting equipment which can be costly to repair and can potentially interfere with the voting process, including the credibility of the voting outcome. We are aware that the DOE previously attempted this option many years ago without success, but there may have been improvements made to these remote communities that might make it a more viable cost-effective option today.

APPENDIX A

STATE CAPITOL
P.O. Box 110001
Juneau, AK 99811-0001
907-465-3500

550 West Seventh Avenue, Suite 1700
Anchorage, AK 99501
907-269-7450

Governor Michael J. Dunleavy
STATE OF ALASKA

MEMORANDUM

TO: Commissioner Kelly Tshibaka

FROM: Michael J. Dunleavy
Governor

DATE: February 26, 2019

SUBJECT: Mission and Direction

This memorandum provides direction, as we have previously discussed, that in addition to your role as the Commissioner of the Department of Administration, it is my intent and expectation that your expertise be utilized to review, investigate, and provide policy direction, not only as it relates to the Department of Administration, but as it applies statewide in the areas of management, audit, and government efficiency, as directed, on my behalf.

APPENDIX B

THE STATE of ALASKA
GOVERNOR MIKE DUNLEAVY

Department of Administration
OFFICE OF INFORMATION TECHNOLOGY

10TH Fl. State Office Building
PO Box 110206
Juneau, Alaska 99811-0206
Main: 907.465.2220
Fax: 907.465.3450

Memorandum

To: Mark Breunig, Chief Technology Officer III

From: Bill Smith, Chief Information Officer

Date: 2/14/2020

Subject: Appointment of Chief Information Security Officer and Assignment of Responsibility

Pursuant to authority granted the Chief Information Officer (CIO) under Alaska Administrative Order 284, I delegate the role of the Chief Information Security Officer (CISO) for the State of Alaska to position control number 02-X069, appointed to you on 1/10/2019.

The CISO is the organization's senior information security official vested with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. The CISO shall serve under and directly assist me in fulfilment of my responsibilities as CIO per AO284. These responsibilities include but are not limited to:

- Development of the organization-wide information security plan, implementation of the plan, and operation of the organization-wide information security program.
- Development, implementation, and enforcement oversight of information security policies, standards, and practices within all executive branch agencies and among their contractors and any third-party information-sharing partners.
- Regular compliance audit of information security policies, standards, and practices within all executive branch agencies and among their contractors and any third-party information-sharing partners;
- Establishment and operation of a security awareness program for all State personnel regarding appropriate and safe information security practices.
- Development of strategies and requirements for hiring, training, and professional development of information security staff.
- Alignment of information technology services acquisition and management to effectively implement standard information security policies, procedures, controls.

This delegation will remain in effect until revoked or amended.

Enclosures: AO 284