ALASKA STATE LEGISLATURE
SENATE STATE AFFAIRS STANDING COMMITTEE
January 20, 2022
3:34 p.m.

MEMBERS PRESENT

Senator Mike Shower, Chair
Senator Lora Reinbold, Vice Chair
Senator Roger Holland
Senator Scott Kawasaki

MEMBERS ABSENT

Senator Mia Costello

OTHER LEGISLATORS PRESENT

Senator Shelley Hughes
Representative Ronald Gillham

COMMITTEE CALENDAR

PRESENTATION(S):

STATE OF ALASKA IT PROTOCOL UPDATES [ON CYBERSECURITY]

- HEARD

BALLOT MEASURE 2 [RANKED CHOICE VOTING] DISCUSSION

- HEARD

PREVIOUS COMMITTEE ACTION

No previous action to record

WITNESS REGISTER

PAULA VERANA, Commissioner Designee
Department of Administration
Juneau, Alaska
POSITION STATEMENT: Introduced the Chief Information Officer.

BILL SMITH, Chief Information Officer
Office of Information Technology

Department of Administration
Juneau, Alaska.
POSITION STATEMENT: Provided a PowerPoint on IT protocol updates on cybersecurity for the State of Alaska.

NICK MURRAY, Policy Analyst
Maine Policy Institute
Portland, Maine
POSITION STATEMENT: Invited testifier provided a PowerPoint on ranked choice elections.

ACTION NARRATIVE

3:34:07 PM
CHAIR MIKE SHOWER called the Senate State Affairs Standing Committee meeting to order at 3:34 p.m. Present at the call to order were Senators Reinbold, Holland, Kawasaki, and Chair Shower.

STATE OF ALASKA IT PROTOCOL UPDATES

3:34:51 PM
CHAIR SHOWER announced the consideration of State of Alaska Information Technology updates.

CHAIR SHOWER stated that he invited Senator Hughes to join members at the table, although she does not serve on the committee.

CHAIR SHOWER made opening remarks. He expressed concern that in October 2022, a month before the election, a data breach compromised 113,000 Alaskans' election data. The Division of Elections certified the election a month later. Despite assurances that the election data was not used nefariously, the state did not conduct a forensic audit, so it is not possible to know for sure. He said he requested the IT protocol updates because the state has had numerous data breaches.

CHAIR SHOWER related that last year, the Commissioner of the Department of Health and Social Services (DHSS) acknowledged a data breach happened that could have affected every Alaskan. He shared his knowledge and experience about cyberwarfare risks stemming from his military service.

3:37:19 PM

CHAIR SHOWER said he hoped this IT update would inform the legislature, state government, and the public since cybersecurity risks will not diminish or stop. The update will include a broad overview of the state's cybersecurity issues, any state cyberattacks, and potential solutions and ways to mitigate or stave off cyberattacks.

He asked the Commissioner Designee and Chief Information Officer to come forward and provide an update.

3:39:11 PM
PAULA VERANA, Commissioner Designee, Department of Administration, Juneau, Alaska, introduced Bill Smith as the Chief Information Officer (CIO). She said he would provide an IT protocol update, including all things related to cybersecurity for the State of Alaska.

3:39:39 PM
BILL SMITH, Chief Information Officer, Office of Information Technology, Department of Administration, Juneau, Alaska, began an IT protocol update on cybersecurity for the State of Alaska. He stated that his responsibilities included overseeing IT for the State of Alaska. He said cybersecurity is vital to the state and it affects everybody's lives each and every day. He highlighted that the Office of Information Technology's (OIT) priority is cybersecurity, which represents a core element in the department's mission statement. Cybersecurity components are part of every significant initiative undertaken.

MR. SMITH said OIT works to align widely-used government industry standards and frameworks. It allows the state to speak in standard terms to other organizations and ensure that security gaps don't exist. He noted that OIT maintains monthly contact with IT personnel from the Legislative Affairs Agency and the Alaska Court System to collaborate on cybersecurity.

3:42:05 PM
CHAIR SHOWER recognized Representative Ronald Gillham joined the meeting.

3:42:28 PM
MR. SMITH turned to slide 2, Agenda. He said he would briefly review the current global cybersecurity climate, cover the state's current capabilities and enhancements, and discuss OIT's vision for cybersecurity in Alaska going forward.

3:42:43 PM

MR. SMITH turned to slide 3, current global security climate to discuss threat activity drivers:

[Original punctuation provided]

Threat activity drivers:

- Cybercrime is a $6 trillion annual industry
- Industrialization and automation of cyberattack capabilities
- Nation state threats
- Supply chain activity
- Pre-existing vulnerabilities

Breaches are no longer just a technical problem best handled by technical people, but instead threat awareness is the responsibility of the whole organization.

MR. SMITH said cybercrime is a $6 trillion annual industry, making it the third-largest economy globally. It is big business, so it drives cyberthreat. In the past several years, cybercrime has created a perfect storm. He stated that monetary drivers exist, an unprecedented pandemic caused dynamic changes in how organizations view IT, and the pandemic coincided with the industrialization and automation of cyberattacks. Someone with little experience could buy ransomware code for several hundred dollars and pay people to implement it. That industrialization is widespread and acts as a driver to the increasing volume of threats. The resources behind the cyber-threat activities, such as nation-state threats, have generally been focused on intelligence gathering rather than financial aspects. However, the cyberattacks are very similar, and the methods of attacks are the same. He characterized these crimes as having exploded in the past several years.

3:44:36 PM

MR. SMITH discussed supply chain activity. He explained that manipulating software before its release has added a nuance. He discussed the last bullet point on slide 3, pre-existing vulnerabilities. In the current environment, some vulnerabilities get publicized very rapidly. He highlighted one example: the December 2021 Apache Log4j vulnerability that disrupted software worldwide. The scale impacted hundreds of millions of software systems worldwide, but it was simple. It introduced 12 characters into code to take control of the software. It was published in the public domain so people could

access it. Cyberattackers did not create this vulnerability, but they exploited it.

MR. SMITH explained that cybersecurity breaches have moved from the traditional mindset of IT to something that everybody must consider. Government members are no longer consumers of cybersecurity but are active participants.

3:46:29 PM
MR. SMITH said people are taking notice of this threat-rich environment. Nations are collaborating; private-public sector companies and private company competitors share information and resources at an unprecedented level. These discussions provide an opportunity to address the issue.

3:47:12 PM
CHAIR SHOWER asked about nation-state threats. He asked for the types of threats the state currently faces from malware or other attacks to give members an idea of the scope of cyberattacks.

MR. SMITH provided several examples to illustrate the scope of cyberattacks. OIT implemented an automated anti-fraud capability to examine traffic moving into myALASKA and block non-human traffic. IT put this in place because the state received 12 million attempts per day from automated systems. Once cyberattackers realized their futile efforts, they diminished and are now low. Still, cyberattacks can come in cycles. The Apache log4j vulnerability led to over 20,000 attempts to exploit that vulnerability. He said IT fends off attacks and institutes protective measures every day. He is proud of the systems and people, but continuous improvement is necessary since cyberattacks are a constant threat.

3:50:39 PM
MR. SMITH discussed slide 4, Current Capabilities:

[Original punctuation provided]

- **Enterprise Security Solutions to eliminate legacy gaps in coverage**
  - Modernized productivity applications with rapid updates and increased security
  - Significantly expanded our ability to see attackers in real time
  - Expanded Endpoint Detection and Response across the executive branch

    - Upgraded Email Filtering and Spam Detection

- **Key Security Initiatives**
    - Elevated licensing for State of Alaska employees to increase security features (CRF)
    - Conducted comprehensive, detailed network inspection(20K+ devices)
    - Conducted external scanning to identify and address external facing vulnerabilities

- **Established intelligence and response collaboration (MS-ISAC, CISA)**
    - Strengthened existing partner relations with CISA, FBI, and AKNG
    - Expanding partnerships by way of participation in the Joint Cyber Security Multistate Program and the Alaska Cyber Group

3:50:40 PM
MR. SMITH remarked that the state continually improves its safeguards to protect Alaskans' data. Several years ago, OIT moved the executive branch from a single productivity application to one server. He reported that this improved the state's overall system security.

MR. SMITH explained that Expanded Endpoint Detection and Response refers to blocking or isolating the virus or malware with antivirus software. He said removing traditional legacy gaps between agencies has improved the system.

MR. SMITH turned to the second bolded bullet point, Key Security Initiatives. He said the state used COVID-19 funding to elevate licensing for state employees due to elevated security benefits. This has improved email security for employees. OIT continues to implement some features. This summer, OIT contracted with an internationally-respected cybersecurity firm that examined over 20,000 devices, networks, and computers. Besides scanning for recent malware, the firm reviewed the historical records.

3:53:19 PM
CHAIR SHOWER said computer viruses were an issue during his time in the military ten years ago. He recalled that the military provided software for staff to use at home. He wondered if the state gives detection software to employees who use home computers, iPads, cap cards, or flash drives that might cross-contaminate the state's system through the backdoor. He asked

whether OIT provides cybersecurity training to executive branch employees to identify scams.

3:55:25 PM
MR. SMITH replied that during his two years working for OIT, the state had conducted cybersecurity training annually for all executive branch employees. He acknowledged that the state might need to offer it more frequently. Currently, the state does not authorize personal devices to connect to the network. He offered to look at connectivity as employee work habits have evolved.

3:56:35 PM
CHAIR SHOWER highlighted that because of COVID-19, many people are working from home. He expressed concern about malware attacks. He related that he took his smartphone and laptop to China but never used them. Once home, he discovered hackers had switched the language on his phone to Chinese, and the devices contained viruses. He shared scenarios to illustrate malware attacks on the U.S. Department of Defense (DoD) he learned about during his military service. He expressed concern that a cyberattack could rapidly infiltrate the state's system and leave the state in the dark. He asked what proactive steps OIT has taken. He wondered if OIT needed funding, statutory changes, or partnerships with federal agencies or private contractors to do its work. He said the legislature needs to know since the state must prioritize its funding. He expressed concern that the state is vulnerable and at-risk due to its small population.

3:59:30 PM
MR. SMITH responded that his points were accurate. OIT reported that as employees began working remotely during the pandemic, the state spent time increasing its capacity for virtual private networks (VPNs) precisely for those concerns. OIT also spent time on its software patching systems to ensure that the state could patch systems not connected to its network. He advised members that OIT is looking at the right things and making progress.

4:00:24 PM
CHAIR SHOWER pointed out that in addition to the executive branch, the state also consists of the legislative and judicial branches. He asked how the state's network connects to the other branches of government.

MR. SMITH said the executive branch maintains the State of Alaska network, but the legislative branch uses only an isolated portion of it. Once he realized separation existed, he initiated

meetings with the legislature and court system to better understand each other systems. He said he thinks the State of Alaska should have a collaborative and cohesive view of its IT systems. He agreed it would need additional work.

4:01:45 PM
CHAIR SHOWER asked if he has considered whether the state needs an entity or working group that could examine IT interactions between the government branches and respond across the board to achieve a better and more holistic approach.

MR. SMITH acknowledged there is a better way than an ad hoc method. He has discussed this internally but agreed the administration needs to explore a more formal process across agencies.

CHAIR SHOWER suggested that a more formal process must happen quickly because an ad hoc approach doesn't work. An ad hoc response is disjointed, and it is difficult to identify who is in charge, leading to gaps. He advocated for a more structured plan, stating it might be worthwhile to develop a workgroup consisting of members from each branch and experts to develop a comprehensive plan. He expressed interest in working on this together.

4:03:55 PM
SENATOR HUGHES said she has met with some private cybersecurity firms. Some firms expressed concern that the state's efforts might be thwarted since the Office of Information Technology (OIT) may not control other state departments but works in an advisory capacity. For example, she heard anecdotally that some departments might push back on IT suggestions for two-factor authentication. She surmised that the Department of Administration stored significant data. She asked what OIT's authority and role is in cybersecurity.

MR. SMITH answered that the department's holistic view is to consolidate the executive branch's IT services. This has been initiated but not fully completed. He said OIT does have authority across state agencies. OIT's published information security policies are binding for the entire executive branch. For example, OIT updated multifactor authentication required of all state executive branch employees. He described the reaction, not as pushback but rather it illustrated the differences in legacy structure throughout the state agencies. The IT environment has evolved independently over three decades, whereas IT consolidation is relatively new. One of the most

important considerations is rationalizing it, so changes are being made to create a more homogenous environment. It's more likely an agency would indicate that the solution might need additional tweaking to work for their agency. He stated OIT could improve on its collaboration.

4:08:05 PM
SENATOR HUGHES observed that OIT sets the policy that state agencies must follow. She asked whether the statutes provide OIT with the authority to protect personal data. She recalled a conversation in another committee on a bill to allow online applications for state services. If the state allows both an online and paper application process and a breach occurs, she wondered whether the state would shut down the online process and strictly go to a paper process. She recalled that there was a protocol in place to do that. However, Article I, Section 22 of the Alaska Constitution requires the legislature to ensure individuals' privacy. In other words, she asked whether the state needs something statutorily to align with the Alaska Constitution or if the legislature should be satisfied that OIT has adopted policies to ensure Alaskans' privacy is protected. She asked for assurance that something more than an internal policy or the OIT chief's cognizance was in place for continuity in future administrations.

MR. SMITH stated that Administrative Order (AO) 284 created his position. He advised that statutory underpinning and mapping in AO 284 places IT responsibility within DOA. He agreed to investigate whether AO 284 addresses privacy issues.

4:10:13 PM
SENATOR HUGHES surmised that the committee would be interested since privacy concerns impact many other areas.

4:10:24 PM
CHAIR SHOWER stated his preference to address this in statute rather than policy since policies often change in future administrations. Thus, once the administration decides on and vets the appropriate path, it would eliminate IT protocol and authority deviations. He cautioned that OIT must carefully review any proposed bill to ensure it gives OIT sufficient authority and flexibility to respond quickly to cybersecurity threats but not constrain or prohibit the division from carrying out its duties since cyberattacks are real-time threats that change daily. He characterized it as a fine line or balancing act. He said he asked a legislation funding and partnership

organization for ways to assist the legislature on data protection.

4:11:43 PM
CHAIR SHOWER asked if the executive branch departments run separate firewalls or if OIT controls all firewalls to avoid gaps.

MR. SMITH responded that it is a mix, with OIT currently maintaining most of the firewalls in the executive branch. However, a few larger departments have their own firewalls. OIT continually works to ensure that the policies are consistent throughout the executive branch so OIT can ensure that the correct configurations are in place.

4:12:35 PM
CHAIR SHOWER asked for an update on OIT's use of multifactor authentication because it is an issue that arose related to election integrity. He remarked that the private sector routinely uses multifactor authentication even with smartphones. He characterized it as an easy process that the state could use in many applications, including myALASKA transactions. He expressed frustration when agencies argue that implementing multifactor authentication is difficult because banking safeguards data using this technology every day.

MR. SMITH responded that OIT uses Microsoft Azure Active Directory multifactor authentications. It provides state employees the option of using multifactor authentication tools. For example, employees can receive a phone call or a texted code to enter. Employees can also download an application that asks for their authorization using a thumbprint or facial recognition identification, or the department could issue employees a physical fob.

4:14:21 PM
CHAIR SHOWER asked for the estimated cost to implement multifactor authentication. He recalled that one estimate for infrastructure was $5 million.

MR. SMITH answered that he didn’t have the specific figures, but federal Coronavirus Aid, Relief, and Economic Security Act (CARES) funding provided the basic funding for multifactor authentication licensing upgrades. He acknowledged annual operating costs were associated with it. For example, there would be an additional $25-$50 for a fob or token per individual. Many state employees use the free download or

receive texts containing codes to enter, and there is no cost for those.

4:15:43 PM
MR. SMITH displayed slide 5, Enhancements:

[Original punctuation provided]

National Institute of Standards and Technology (NIST) Cybersecurity Framework

Identify
- Asset Management
- Implementation of Multi-Factor Authentication (MFA)

Protect
- Continued hardening of the environment
- Migration to a secure Cloud Framework
- Recurrent Security Training for all state employees

Detect
- Network threat visibility - ability to detect real-time attacks and block malware, phishing attempts

Respond
- Security mentor led incident response rehearsals to improve readiness

MR. SMITH reviewed the state's cybersecurity enhancements currently underway, as shown on the bullet points on slide 5. He explained that OIT is organized by and uses the National Institute of Standards and Technology (NIST) cybersecurity framework in its security policies. He said OIT could break this into various components to identify threats and protect the security environment.

MR. SMITH estimated that the state is approaching 50 percent implementation of multifactor authentication for state employees. He anticipated OIT would finish the full implementation in the coming weeks. He highlighted that its migration to a cloud framework illustrates it uses modernization efforts to improve security and avoid a technology debt. Cloud migration allows OIT to rapidly move to state-of-the-art equipment using technology built with security in mind.

4:17:07 PM

MR. SMITH stated that OIT has been using Recurrent Security Training in the past few years, but it is seeking to improve it even more. He reported that OIT brought in a security mentor to work with the state's security office to ensure that the state uses best practices. This effort helps provide employees with professional development opportunities.

SENATOR SHOWER asked if OIT was tied into the Emergency Operations Center (EOC) and used tabletop exercises. He cautioned that cyberattacks could shut down transportation vectors, the electric grid, and food supply chains. OIT needs a collaborative response plan beyond protecting computer networks since it could be a real-world material infrastructure problem.

4:19:04 PM
MR. SMITH responded that OIT has routinely participated with EOC during the past 18 months to identify ways to collaborate. He said OIT tracks the Alaska Army National Guard's (AKNG) increasing cybersecurity capabilities and looks for ways to use them. He drew attention to the bottom of slide 4 that referenced the AKNG.

4:19:48 PM
MR. SMITH reviewed slide 6: Path forward - Focus on the basics.

[Original punctuation provided]

Focus on executing basic protocols well

- Practicing Good Cyber Hygiene5
- Compliance monitoring
- Enhance response capabilities
- Immediate threat hunting protection against security threats

MR. SMITH stressed that the state could avoid 98 percent of cyberattacks by using good cybersecurity practices, including anti-malware software, applying for least privilege access, enabling multifactor authentication, and keeping software up to date to protect data. He reported that OIT has identified gaps that must be shored up, which is an essential part of the plan moving forward. Ensuring that the enterprise systems across the state do not have gaps, and that once implemented new systems are touched frequently to verify the updates, so they operate at an optimal rate. Further, employees must change passwords often and obtain ongoing continuing education and training on cybersecurity.

4:21:18
MR. SMITH moved to slide 7, Path forward - A holistic view.

[Original punctuation provided]

Simplify the enterprise security environment

- Developing a holistic view of security that is:
- Integrated
- Standardized
- Working towards continuous improvement

MR. SMITH said this effort was tied to the completion of IT consolidation. He stated that the state's security offices must have a consistent view throughout the state system. He related that several months ago, a cyberattack occurred against the federal government and private sector when hackers breached SolarWinds' software, injecting trojanized code into a file later included in its software updates. Once OIT received notification of the cyberattack, IT staff examined the state's systems to identify SolarWinds software. OIT determined that the state had three instances of SolarWinds software. However, that software was not in use. This highlighted that OIT did not have the proper visibility. Since then, OIT has rushed to increase its visibility. He offered his view that OIT has made tremendous strides to address this in the past year, but the effort must be ongoing. Simplifying the complex system and infrastructure provides another aspect of considering the system holistically. IT must be careful about new platforms and tools, ensuring compatibility with the existing tools. This prevents a patchwork of tools. He characterized this as a critical aspect of how OIT builds its IT structure. Lastly, this provides a holistic view of the IT environment, but not OIT's security tools. OIT must think about how to structure the IT environment from a security perspective rather than simply viewing it as a tool since it is tied together.

4:23:22 PM
MR. SMITH turned to slide 8, Path Forward - Zero Trust.

Continue the path to Zero Trust

- Assume breach
- Verify explicitly
- Least privileged access

"A zero trust cybersecurity approach removes the assumption of trust typically given to devices,

> subjects (i.e., the people and things that request information from resources), and networks…. This requires device health attestation, data-level protections, **a robust identity architecture**, and strategic micro-segmentation to create granular trust zones around an organization's digital resources." *National Cybersecurity Center of Excellence (NCCoE)*, *NIST* **Zero Trust guiding principles**

4:23:30 PM
MR. SMITH explained that OIT continues the path forward to zero trust. Zero Trust means OIT assumes that all activity in the network could be a data breach. He said OIT's goal seeks to protect the data rather than the network He recalled Chair Shower characterizing cybersecurity as a castle and moat, which is how IT often visualizes it. Instead, IT must bring the wall around the data instead of around the network. This allows IT to determine whether an individual or a bot is attempting to access data. The system requires individuals to validate by using multifactor authentication and permissions.

Further, OIT determines whether the person has the appropriate authority to access the specific data via identity management. OIT seeks to determine if the device is associated with a person. If so, the OIT process validates it as a safe device. The diagram on the right side of slide 8 illustrates this. Once the user, the app, and the device are validated, the individual would be deemed a trusted agent and have data access. However, it requires significant work and infrastructure to achieve that sophistication. He reported OIT has been working to implement this piece-by-piece. Thus, with each step taken, OIT improves data safety. He anticipated this process would be ongoing over the next several years.

4:25:28 PM
CHAIR SHOWER remarked that he considered this as a starting point. He indicated that the legislature would participate in this process via statutory changes or funding.

4:27:34 PM
SENATOR KAWASAKI asked about the type of training new employees would receive. He related several scams that hackers recently used. One was an email purported to be from Representative Steve Thompson stating he was trapped in the Philippines after losing his passport, so he needed money. He asked if state employees receive training on phishing.

MR. SMITH responded that OIT tailors its training for phishing. This training cycle highlighted remote work and cybersecurity issues designed to create an awareness of ways to be safe, also called cyber hygiene.

4:30:05 PM
SENATOR HUGHES said she serves on the National Council of State Legislatures' (NCSL) Cybersecurity Task Force. She asked whether OIT collaborates with other states. She said she also served on the NCSL's Broadband Task Force. As the state expands its broadband technology, more people apply online, including taking Department of Education and Early Development (DEED) online courses for rural residents. This means the state's network will connect with school districts. She encouraged him to review the report. She asked for an update on OIT's collaboration with other states.

MR. SMITH said he participates in IT calls with Washington, Oregon, Nevada, and California every week to discuss issues with members of the National Association of State CIOs. More importantly, the Multi-State Center for Internet Security (MS-ISAC) sponsored by the Department of Homeland Security (DHS) provides OIT an opportunity to share information across states. Currently, OIT has held discussions with several Northwestern states about creating a joint security operations center.

BALLOT MEASURE 2 DISCUSSION

4:33:08 PMCHAIR SHOWER announced the next business before the committee would be a discussion on Ballot Measure 2 - Ranked Choice Voting.

He invited Nick Murray, invited testifier, to introduce himself.

4:34:44 PM
NICK MURRAY, Policy Analyst, Maine Policy Institute, Portland, Maine provided a PowerPoint on statistics and issues related to ranked choice elections. He explained that the Maine Policy Institute is a small nonprofit public policy organization. He reported that Maine was the first state to use ranked choice voting (RCV) statewide. Maine sent its first ranked choice voting member to the U.S. Congress in November 2018. He stated that his goal is to assist the legislature in avoiding pitfalls, maintaining and increasing voter participation, and minimizing the number of discarded ballots that could disenfranchise voters.

4:35:51 PM
CHAIR SHOWER explained that he invited Mr. Murray to present to the committee since Maine had experience with ranked choice voting.

4:36:24 PM
MR. MURRAY reviewed slide 1, a false majority. He said his PowerPoint was a combination of data from the Maine Policy Institute (MPI) published in 2019 after Maine's RCV in the 2018 election. The report consists of data compiled from 96 RCV elections throughout the country. He said Princeton Professor Nolan McCarty essentially repeated this analysis the following year for use in a court case challenging RCV in 2020. His research consisted of data from the 96 races plus the two Maine cases for a total of 98. He explained that some of the graphs are from the MPI report and others were from Professor McCarty's report.

4:37:24 PM
MR. MURRAY identified one pitfall in RCV is the discarded ballots. In 2018, in over 60 percent of RCV elections, the winner did not earn a majority of the votes. This was true in Maine's Congressional race in 2018, even though the winner had a majority of the total ballots cast in the final round, but only had 49.2 percent of the vote due to the high rate of discarded ballots.

MR. MURRAY directed attention to slides 2-4, "Which ballots are discarded?" He explained that ballots are discarded in three ways, those that were overvoted, undervoted or exhausted. Slide 2 illustrates that overvoting occurs when voters select two candidates for their first choice. Slide 3 illustrates undervoting, where the voter marked the first-choice candidate but skipped the second and third choices and marked the fourth choice. It depends on the state's rules, but Maine rules state that the ballot is undervoted if the voter leaves two candidate choices blank. However, if only one choice was skipped, the voter's subsequent choice would be moved up. Slide 4 shows the final way a ballot is not counted and is considered exhausted. That is when the voter selected candidates who did not make it to the final round. In this instance, Jared F. Golden and Bruce Poliquin were the two candidates left in the final round, but this voter did not select them. Thus, this voter's ballot would be exhausted and not count in the final tally.

4:39:53 PM

SENATOR HUGHES asked whether the 49.2 percent on slide 1 included the first, second, or third choices or just the first choice.

MR. MURRAY answered that the percentage referred to the total number of voters who cast a ballot. The calculation consists of the winners in the final round divided by total votes cast for that race.

SENATOR HUGHES commented that a winner typically receives a majority of the votes cast in a standard election. Under RCV, a winner could receive less than the majority and may not have been the voter's first choice. It could be the voter's fourth choice. The winner might only be the first choice for 20 percent of the voters who cast ballots.

4:41:12 PM
CHAIR SHOWER offered his view that the ranked choice voting (RCV) system suppresses many votes.

4:41:52 PM
MR. MURRAY recalled that a New York mayoral primary candidate only had 30-35 percent of the votes cast. He stated that is the reason the MPI report was titled "A false majority." He said that theme is important. Many proponents of RCV have put forward this as a means to guarantee majority support. However, it doesn't match reality when considering the discarded ballots.

4:42:32 PM
MR. MURRAY turned to slide 5, RCV elections average nearly 11 percent ballots discarded. He said this slide was from Professor McCarty's analysis. It mirrors the MPI's analysis, where almost 11 percent of ballots were discarded in RCV elections. This could be compared with less than 1 percent of mailed ballots being rejected in the average U.S. election. He highlighted that the voters who fell within the 11 percent of RCV discarded ballots did not make any ballot-marking error, but they were not included in that final tally. Those voters may not have ranked all candidates or did not rank a candidate the voter did not like. Professor McCarty found that 20 percent of the ballots were discarded in 15 of 98 elections. For example, the mayoral races in Saint Paul and Minneapolis have used RCV for a substantial time. The goal is to limit the number of disenfranchised voters and ensure that participation is as high as possible. He characterized that as a measure of a sound voting system.

4:44:34 PM
MR. MURRAY stated that certain demographics could have a high rate of disenfranchised voters. He turned to slide 7, a bubble graph illustrating the McCarty analysis for elections with large senior citizen populations.

MR. MURRAY said a similar theme occurs in elections where the demographics show large numbers of noncollege voters. The higher the number of non-college voters result in a higher rate of discarded ballots as shown on slide 8. He stated that Jason McDaniel, a political science professor at San Francisco State University, conducted a study in 2016 that showed RCV exacerbated the voter turnout for certain demographics in the San Francisco population. He quoted the study:

> The complexity of the system presents barriers to participants that decreases voter turnout and raises higher probability of ballot errors.

MR. MURRAY said he also found a correlation between incorrectly marked ballots in foreign-born voters and voters whose primary language was something other than English. Politico reported on the New York City mayoral primary in the South Bronx. He quoted the article, which said "Voters in the South Bronx had a higher incidence of ballot mistakes." He clarified that South Bronx is a socio-economically disadvantaged neighborhood. He highlighted that one could start to see a trend in RCV, where education gaps, English language proficiency, and general knowledge of voting systems could all create barriers for voters.

4:46:38 PM
MR. MURRAY stated that the American Civil Liberties Union (ACLU) of Kansas testified, as follows:

> Low propensity voters are already less likely to participate in elections that do not coincide with congressional or presidential races. By adding additional steps to voting RCV exacerbates this tendency, making it less likely that new and more casual voters will enter the process.

MR. MURRAY said that is consistent with McCarty's analysis.

4:47:06 PM
CHAIR SHOWER remarked that he found this data fairly disturbing. He related his understanding that ranked choice voting (RCV) was more complicated for minority voters. Still, he was unsure of

the causative factor of voter suppression of minorities and the less educated. He asked the causative factor for senior citizens since they are often well-educated.

4:48:32 PM
MR. MURRAY answered that he believed that RCV would raise the barriers of information. He offered that creating a more complex system might affect those voters who do not vote in every election. As Mr. McCarty found in San Francisco, RCV tended to exacerbate the disparity for the groups who are already less likely to vote. He expressed concern that this might affect specific demographics, age-based demographics, or perhaps even younger voters. While it is tough to conclude because there isn't sufficient data, it appears that RCV increased information barriers. He stated that the data reflects this barrier in the higher rates of discarded ballots and reduced participation in certain communities.

4:49:48 PM
CHAIR SHOWER said he reviewed the charts and the Division of Election's information, and he found RCV was not easy because it created a more complicated system. It seemed somewhat intimidating. He highlighted that RCV was more complex than picking one candidate over another. He expressed concern that RCV may be so complicated that it will suppress the vote and disenfranchise voters for specific groups.

MR. MURRAY agreed.

4:51:20 PM
SENATOR KAWASAKI referred to the graph on slide 9, with Mr. McCarty's analysis stating RCV elections average nearly 11 percent discarded ballots. He asked if that data was from the 2018 or 2020 election cycle.

MR. MURRAY answered that this data was derived from 96 elections, including the 2018 Maine elections. He said the report was written in late 2019 and published in early 2020. It compiled election data as far back as 2000 and perhaps even earlier for a few cases.

4:52:13 PM
SENATOR KAWASAKI asked if the discarded ballots included ones where the voter may not have voted for the top two candidates.

MR. MURRAY answered yes.

SENATOR KAWASAKI asked if he could compare the discarded ballots for 2018 and 2020 since the voters would have experienced more information about RCV in the subsequent election.

MR. MURRAY answered that the PowerPoint on [slide 10] shows that data. Mr. McCarty's analysis shows that even when RCV was used over five elections, the rate of discarded ballots was the same. He said the data shows voter education over time was weakly correlated. The discarded ballots represented voters who did not select candidates who advanced to the final round. One pitfall of RCV is that it requires voters to fill in a bubble, thereby voting a preference for a candidate the voter does not support in hopes of getting their ballot to the final round. He compared RCV as a two-dimensional ballot versus a binary ballot. RCV raises the potential for more confusion later on in the ballot process when the Division of Elections reallocates votes. He offered his view that under RCV, voters must vote more strategically.

4:54:13 PM
CHAIR SHOWER asked for an explanation of the difference between a ballot that is discarded versus one that is exhausted. Is the bottom line that their vote does not count, is rejected, or only counts in certain circumstances.

4:54:46 PM
MR. MURRAY answered that an exhausted ballot is when the voter does not vote for a candidate who advances to the final round. He explained that discarded ballots included overvotes, undervotes, and exhausted choices.

CHAIR SHOWER remarked that it would be possible to not count voters' ballots.

4:55:53 PM
SENATOR KAWASAKI pointed out that the legislature appropriated $3 million for the Division of Elections to help educate people on RCV. The division has been working hard to familiarize the public with the process He admitted he was initially confused by RCV, but he read the division's literature, watched the video, and now he understands the RCV process.

CHAIR SHOWER pointed out that the data shows some voters don't take the time to educate themselves on RCV. However, Alaska is stuck with it. The data indicates that well-educated voters successfully voted in RCV, but the uneducated voters did not. He maintained his concern about RCV.

4:57:02 PM
SENATOR HUGHES said the PowerPoint includes slides on discarded and exhausted ballots. Mr. Murray alluded to the fact that RCV could adversely affect voter turnout. She expressed concern that seniors may be confused or not understand how RCV works. She asked how RCV would affect socio-economic voters or disenfranchise voters in races that resulted in more discarded ballots.

4:57:50 PM
MR. MURRAY answered that it generally would do so. He explained that he referenced the McDaniel report because it evaluated RCV in one electorate over several decades. He offered to provide a link to the report. The McDaniel report shows exacerbated divisions in turnout from the demographics already less likely to vote. He recalled that the McDaniel report did not point to seniors expressly but focused on foreign-born, minority neighborhoods where voters' first language was not English. Although he did not view seniors as less likely to vote, the general complexity might effectively appear in exhausted ballots. He stated that Maine's constitution only allows RCV for federal races and primaries. Thus, Maine has used RCV in three elections: the gubernatorial primary in 2018 and June 2020 and a congressional race in 2018.

5:00:16 PM
SENATOR HUGHES commented that Alaska is switching from a more traditional voting process to RCV, but the state already struggles with voter turnout. She asked if Alaska should expect RCV to reduce voter turnout.

MR. MURRAY answered yes; that is a reasonable expectation, based on the data in the PowerPoint.

5:00:46 PM
CHAIR SHOWER asked if write-in votes would be invalidated under RCV.

MR. MURRAY answered that it would depend on Alaska's regulations. Maine requires ballots to have a write-in line. For example, voters would have a line for write-in candidates and have five candidates, giving the voter six choices.

5:01:26 PM
CHAIR SHOWER expressed concern that the RCV process intended to improve the voting process, but that does not appear to happen

statistically. He wondered if the legislature gave Ballot Number 2 initiative sufficient scrutiny. He offered his view that Alaska was misled.

5:02:11 PM
SENATOR REINBOLD commented that this was the first RCV presentation she had seen. She wondered if voters understand the effects of the RCV ballot initiative, which passed by a small margin. She said she hopes the courts consider whether voters understood the issue. She asked how RCV could be equitable if it increases barriers and disenfranchises the less educated. She said RCV causes her tremendous pause.

5:04:15 PM
MR. MURRAY replied that he couldn't comment on any legalities, but her concern relates to the general mismatch of voters' understanding and participation. He discussed the statistics shown on slide 9, comparing the percentage of voters who did not understand RCV to their level of education. He said FairVote commissioned the poll. He identified FairVote as a national group promoting RCV, noting it also ran Maine's initiative. He acknowledged that Alaska's initiative was more complex than Maine's, and campaign financing issues may have complicated it. He reported that over 25 percent of voters not finishing high school and 13 percent of voters with post-graduate degrees found RCV confusing. He pointed out that nearly one in seven of those with a master's or post-graduate degree had difficulty understanding RCV. He stated that Maine was told that RCV would be better for democracy, but he found it problematic since RCV might suppress participation.

5:04:37 PM
MR. MURRAY said more support for a specific candidate does not necessarily increase the candidate's chances of winning due to multiple candidates and multiple rankings. It's difficult to understand the potential outcome until the tabulation is completed.

5:07:00 PM
CHAIR SHOWER asked for the general political leaning of the organization Fair Votes.

MR. MURRAY surmised that FairVote was probably center-left.

5:07:49 PM
MR. MURRAY turned to slide 10, which indicated that more voter experience does not guarantee fewer discarded ballots.

MR. MURRAY said New York City (NYC) spent $50 million to educate voters on the RCV process. The NYC election had over 1 million voters resulting in over 100,000 voters who did not decide on the winner in the last round. He recalled that figure represented about 15 percent of the ballots cast.

MR. MURRAY responded to the claim that RCV might get money out of politics by reviewing slide 12, which showed the independent expenditures in Maine's 2018 gubernatorial. He said Maine experienced independent spending in opposition to candidates for the first time. He remarked that America has generally experienced a significant increase in campaign expenditures in the last two decades. He offered his view that campaign expenditures would not diminish under RCV.

5:09:36 PM
MR. MURRAY turned to slide 11 that displayed the following quotes:

> The promise that ranked choice voting leads to greater democracy is not necessarily fulfilled. - Governor Gavin Newsom (D-California
>
> "[W]hen it comes to elections, every vote cast in our state should count. The evidence and experience from around the country suggests that Ranked Choice Voting will work against this goal, adding unnecessary confusion and potentially reducing voter turnout." - U.S. Senator Mark Begich (D-Alaska)
>
> "Under ranked choice voting, the city of San Francisco has seen a depressed voter turnout in communities of color." - Councilman Daneek Miller (D-Queens), co-chair of the Black, Latino & Asian Caucus of NYC Council.
>
> Also opposed to Ranked choice Voting:
> Jerry Brown, Former California Governor
> The NAACP of New York
> The Vulcan Society (fraternal order of black firefighters)

5:10:13 PM
MR. MURRAY said he hopes his presentation identified some of RCV's pitfalls and that the PowerPoint would help the committee identify amendments to protect voter integrity and

participation. He added that he has some thoughts on ranked choice voting.

CHAIR SHOWER solicited his comments.

5:11:05 PM
MR. MURRAY related that traditional elections typically are decentralized and votes usually are called in from precincts. However, RCV requires a central place to tabulate votes. He stated that Maine hired couriers to deliver the ballots to one location and make appropriate data transfers to the Secretary of State. He related his understanding that Alaska's remote communities might need to rely on electronic data transfer to a centralized location for tabulation. Thus, election security concerns might arise. He stated that RCV requires software for the tabulation algorithm, which should be as transparent as possible for voters' benefits.

5:12:30 PM
CHAIR SHOWER read a quote from slide 11 that resonated: "Under ranked choice voting, the city of San Francisco has seen a depressed voter turnout in communities of color."

CHAIR SHOWER stated his goal is to ensure that everybody eligible to vote gets an opportunity to do so. Voting is one of the most sacred rights in the United States. He anticipated that committee members would help educate people via social media and media.

5:14:29 PM
There being no further business to come before the committee, Chair Shower adjourned the Senate State Affairs Standing Committee meeting at 5:14 p.m.