ALASKA STATE LEGISLATURE
HOUSE STATE AFFAIRS STANDING COMMITTEE
May 10, 2018
9:06 a.m.

MEMBERS PRESENT

Representative Jonathan Kreiss-Tomkins, Chair
Representative Gabrielle LeDoux, Vice Chair
Representative Chris Tuck
Representative Adam Wool
Representative Chris Birch
Representative Gary Knopp
Representative Andy Josephson (alternate)

MEMBERS ABSENT

Representative DeLena Johnson
Representative Chuck Kopp (alternate)

COMMITTEE CALENDAR

PRESENTATION: ELECTION SECURITY: STATE POLICIES

- HEARD

PREVIOUS COMMITTEE ACTION

No previous action to record

WITNESS REGISTER

WENDY UNDERHILL, Director
Redistricting and Elections
National Conference of State Legislatures (NCSL)
Denver, Colorado
POSITION STATEMENT: Presented a PowerPoint on Election Security: State Policies.

MAURICE TURNER, Senior Technologist
Center for Democracy and Technology
Washington, D.C.
POSITION STATEMENT: Presented a PowerPoint on Cyber Security.

DANIELLE ROOT, Voting Rights Manager
Center for American Progress (CAP)
Washington, D.C.

POSITION STATEMENT: Provided a presentation on cyberattacks.

JOSIE BAHNKE, Director
Central Office
Division of Elections
Office of the Lieutenant Governor
Juneau, Alaska
POSITION STATEMENT: Answered questions during the presentation on Election Security.

PHILLIP MALANDER, Systems Administrator
Central Office
Division of Elections
Office of the Lieutenant Governor
Juneau, Alaska
POSITION STATEMENT: Answered questions during the Presentation on Election Security.

ACTION NARRATIVE

9:06:02 AM

CHAIR JONATHAN KREISS-TOMKINS called the House State Affairs Standing Committee meeting to order at 9:06 a.m. Representatives Kreiss-Tomkins, Josephson (alternate), Knopp, and Birch were present at the call to order. Representatives Wool, Knopp, and LeDoux arrived as the meeting was in progress.

PRESENTATION: ELECTION SECURITY: STATE POLICIES

9:06:22 AM

CHAIR KREISS-TOMKINS announced that the only order of business would be a Presentation: Election Security: State Policies.

9:07:42 AM

WENDY UNDERHILL, Director, Redistricting and Elections, National Conference of State Legislatures (NCSL), began a PowerPoint on Election Security. She stated that election security was a key issue in all states, not just in Alaska. The NCSL redistricting and elections team has spent most of its time in the past year working on election security, she said.

9:08:15 AM

MS. UNDERHILL turned to slide 2, titled "What Does NCSL Do?" She stated the NCSL is a non-partisan organization that works for legislators and staff throughout the nation. The NCSL does not make recommendations on policy issues since legislatures make those decisions; however, the organization provides research on a number of topics, including election security.

9:09:19 AM

MS. UNDERHILL referred to slide 3, titled "The Plan for the Next 15 Minutes." She said she would provide a quick national overview on threats to election security, including where the threats have shown up or might show up and, in particular, pointing out policy choices that the state might like to consider. She acknowledged that although she is not a security expert, Maurice Turner who is an expert would testify later. Election security was not a new issue even though it may seem as though it is new, she said. She stated that election security was relative, such as whether the system is more secure than prior systems.

9:10:30 AM

MS. UNDERHILL referred to slide 4, which provided a flowchart of statewide voter registration databases. She directed attention to the bottom of the slide, showing that registrations can come to the state via several mechanisms, including self, third-party, online, and DMV [Department/Division of Motor Vehicle] registrations. Some states are currently automating their voter registration processes, including Alaska, since it has automated its system via the permanent fund dividend application process. The next most common source of voter registration was via an online registration system, using paper forms that are mailed in by voters. Voter registration drives and local election voter registration provide other means to register voters in person, she said.

MS. UNDERHILL reported that statewide voter registration databases are updated on an ongoing basis by state and local officials, depending on the state. The databases are checked against other sources of data within the state or by using out-of-state resources. She said that the registration process was separated from the voting process so any "messing around" with registration does not interfere with vote counting. She cautioned that if "bad actors" did gain access to a voter registration system it could cause havoc. For example, it would be possible for people to change or remove individual records or

even to delete a whole database, which could disrupt an entire election. Voters tend not to make any distinction between voter registration and elections, so any tampering would be viewed as tampering with elections.

9:12:42 AM

MS. UNDERHILL referred to slide 5, titled "Voter Registration: Policy Options." She said some states have same-day registration, such that a person could appear at a polling place on Election Day and register to vote. She acknowledged that this policy has been adopted because people are interested in increased voter turnout; however, this option does provide a failsafe for any registration. She stated that maintaining voter lists translates to good elections. Data is checked by using in state and out-of-state sources, noting Alaska is a member of the Electronic Registration Information Center (ERIC), which is a national cooperative where states share data. Electronic poll books are in use in some jurisdictions; however, she cautioned that if the poll book is electronic, it is important to have a backup on paper or on a stand-alone laptop. Therefore, any intrusion on Election Day would not have an impact through an electronic poll book, she said.

9:14:21 AM

CHAIR KREISS-TOMKINS asked for an explanation of poll books and the significance of electronic poll books.

MS. UNDERHILL explained poll books. Throughout the last 80 years, jurisdictions have printed out all registered voters, creating a paper poll book. These poll books are distributed to the polling place at the precinct level and voters sign the register after providing poll workers with identification. That data can be in paper or it can also be on a computer as an electronic register, which often is used as a means to speed up checking in voters at polling places where lines are an issue. The electronic poll books can be a direct line to the statewide registration database or the poll book can be kept on a separate laptop and uploaded to the statewide voter registration database.

9:15:50 AM

MS. UNDERHILL continued to review slide 5, stating that voter registration systems can be reviewed for security and Mr. Turner would discuss this in more detail. The state or local election

officials can also perform certain security reviews in advance of the election. The federal government has released an extra $300 million to states and she assumed that Alaska's share would likely be $3 million, which can be used for election security. Some states are using this funding to update their voter registration databases, she said.

9:16:50 AM

REPRESENTATIVE BIRCH referred to the recent Anchorage municipal "vote by mail" election. He indicated a lot of expired information occurred during the election process. He asked whether she had any recommendations or innovative ways to clean up voter registration lists, for example, to update voter registration when people move.

MS. UNDERHILL responded that as states consider "vote by mail" elections they all have that same question. She acknowledged that having "clean voter lists" for mail elections was important since states do not want to mail twice as many ballots as actual voters. She emphasized how important it is to check data throughout the year, for example, states can compare vital records to their election database to identify death records and update their voter databases. The DMV can also notify the Division of Elections of any address changes. In turn, the DMV could mail out a postcard to verify the address change. She acknowledged that it takes a lot of proactive work prior to Election Day to keep voter databases updated. She reported that Colorado has one-fiftieth of the number of provisional ballots being used due to "clean voter" lists and the state is quite proud of its database.

9:19:34 AM

REPRESENTATIVE LEDOUX asked whether any "red" states have solely vote-by-mail elections or if it was primarily "blue" states.

MS. UNDERHILL responded that three states have all vote-by-mail elections, including Washington, Oregon, and Colorado. She stated that Colorado, where she lives, was considered a "purple" state since one body is held by Republicans and the other by Democrats. She said that Washington State has had all vote-by-mail elections for some time, although she was unsure if it was a "blue" state at the time it shifted to a vote-by-mail election. Utah has nearly all "vote by mail" elections, although its counties are allowed to make the decision; she anticipated that Utah would be an all "vote by mail" election in 2018.

States considering moving to all "vote by mail" elections include Hawaii and California, both "blue" states, and Montana, a "red" state.

CHAIR KREISS-TOMKINS asked for clarification on reasons that western states are considering "vote by mail" but eastern states have not done so.

MS. UNDERHILL responded that she was unsure; however, it was mostly likely cultural, although size may be a consideration. Newer states tend to have more of an appetite for change. She also noted that legislators from eastern states have raised issues about concern that ballots might be stolen from mailboxes.

9:23:42 AM

MS. UNDERHILL added that some legislators from Indiana, which is a "red" state, have also expressed interest in "vote by mail" elections. However, Indiana has not taken any action, she said.

MS. UNDERHILL referred to slide 6, titled "Voting Itself." She explained voting options, including absentee and mail voting, which are considered similar; in-person voting consists of polling place voting and early in-person voting at a local election office, and electronically-transmitted ballots have been considered to be online voting. Electronically-transmitted ballots have triggered the most security-related concerns; however, all states are required to send ballots out electronically to some citizens, primarily to overseas military voters, so outbound blank ballots via the Internet were considered normal.

MS. UNDERHILL reported that nearly two-thirds of states allow voters to return their ballots in some electronic form via an e-mail attachment or a web portal, she said. Both of those options cause concern by cyber-security people since e-mail attachments could be hacked and changed, she said. The portal not only allows the votes to come in but could become a target of an attack. She pointed out that tradeoffs exist, for example, in terms of all mail elections the tradeoff might be that Native Americans may not have access to private mailboxes or people in rural areas may also have spotty delivery. In terms of electronic transmission, overseas voters may not be able to return a ballot by any other means, she said.

9:26:40 AM

REPRESENTATIVE TUCK asked how in-person voting is different from vote centers.

MS. UNDERHILL answered that in traditional in-person voting a person must show up at his/her own precinct, but for jurisdictions with a vote center model, everyone in a county, borough, or jurisdiction can vote at any vote center and obtain an accurate ballot. She described this as being more convenient for people because they can vote on their way to the office or school. It saves the state money because fewer facilities are involved and lessens the need for poll workers, which can be challenging for some jurisdictions, she said.

9:28:10 AM

MS. UNDERHILL referred to slide 7, titled "Voting Itself: Pre-Election Policy Choices." She said that training includes training for election officials, but it could be for poll workers. She recalled one study showed the number of states requiring training has increased and they offer voluntary new training. The training might include cyber-security training or how to perform chain-of-custody using bipartisan teams or how to perform physical security for the equipment, including cameras or locks. Most states do perform accuracy testing just before an election by running a test stack of ballots marked for George Washington and Abe Lincoln. The election division knows in advance what the count should read, the machine counts the ballots, and the comparison shows the count. She remarked that it is nice to invite the public in to observe the count and that helps to build the culture of transparency. The right time to do contingency planning is prior to a problem, in case a cyber disaster or natural disaster occurs. States can also review their recertification requirements, for example, some states require paper ballots, or no Internet connectivity for voter equipment, and others remove obsolete references to lever machines or for certain font size for ballots.

9:30:41 AM

MS. UNDERHILL referred to slide 8, titled "Election Day." She stated that prohibiting Internet connectivity for voting equipment is the most important aspect. She said some states might be concerned about crime.

MS. UNDERHILL referred to slide 9, titled "Post Election Policy Choices." She highlighted post-election audits, which provide a

means to confirm that the tabulating equipment counted votes accurately. She said Alaska does have a law relating to post-election audits. All states require a paper ballot or record for audits.

MS. UNDERHILL referred to slide 10, titled "Voting Technology" that showed images of some of the current voting technology being used.

MS. UNDERHILL turned to slide 11, titled "Voting equipment: Policy Choices." She mentioned paper ballots; however, sometimes voting machines provide a record of the winning candidates, but not all of the candidates, with a barcode or QR code [Quick response code] at the top. She suggested this was something to discuss with cyber security personnel. She said that people with disabilities have a right to vote securely and privately and it is important to have systems that can be used at home, even if it is a paper ballot.

9:32:50 AM

MS. UNDERHILL referred to slide 12, which showed a flowchart diagram. She offered to briefly cover results reporting, noting that the results are unofficial results and although it is not good if someone tampers with results as they are transferred from the local office to the state and to a public display, however, it will not change the outcome of an election.

9:33:10 AM

MS. UNDERHILL referred to slide 13, titled "Disinformation and Other Campaign Shenanigans." She reported that several days ago the US Senate Intelligence Committee referred back to all of the activities in 2016 as an effort to undermine confidence in the voting process. She remarked that the committee stated it had not seen any evidence that vote tallies were manipulated or that voter registration information was deleted or modified.

9:33:50 AM

MS. UNDERHILL referred to slide 14, titled "Resources," and she offered to send those to the committee. She provided her contact information, including her e-mail: wendy.underhill@ncsl.org.

9:34:20 AM

CHAIR KREISS-TOMKINS turned to the next speaker, Mr. Turner, center for Democracy & Technology.

MAURICE TURNER, Senior Technologist, Center for Democracy and Technology, expressed his goal to cover threats to the voter registration systems, voting, and reporting results. When it comes to threats to voter registration the article in the Anchorage Daily News [not identified] shows what can happen when an attacker probes a network and finds a vulnerability. When talking about threats to voter registration, it relates to what it means to have an unauthorized actor go in and change information in the voter registration database.

MR. TURNER described this can happen when the person accesses the local information technology (IT) infrastructure or any cloud-based infrastructure that the state or [boroughs] might contract out. One way hackers operate would be through "fishing," which is where an individual with access, perhaps the local IT administrator or election official, with legitimate access to the database (DB) receives an e-mail, which looks legitimate but is an attempt to get the username and password for the person and subsequently impersonate them. That would be the likely way a person would gain access, he said.

9:36:34 AM

MR. TURNER highlighted another way the database can be disrupted, which is by targeting the IT infrastructure and bringing down the infrastructure, so local jurisdictions do not have access to the state or cloud-based infrastructure. He stated that local election officials are typically pretty good with contingency planning, especially given the fact that paper was the only way to conduct elections. The paper records provide a backup, he said.

9:37:27 AM

REPRESENTATIVE BIRCH stated that the frontend of the worldwide web is what people see, but the backend maintains and manages the records. He asked Mr. Turner whether he could speak to a secure database and the webpages and how they are separate.

MR. TURNER said the best practice would be to make sure the frontend and backend systems are disconnected, and the data is only transferred on a periodic basis, whether it would be at the end of the day or periodically throughout the day. He agreed having the two connected directly and continuously would be a

bad idea since any user would have the ability to read and write to the database on the backend.

9:39:25 AM

MR. TURNER directed attention to "Threats to the Voting Itself." When it comes to voting there are typically three areas for effective security procedures, including administrative controls, such as staff trained on policies and procedures; technical controls, such as the best IT systems; and also physical controls, including cameras throughout the facilities and the strongest locks one can buy. However, these are meaningless if the organization does not have appropriate administrative goals in place to properly implement the technical and physical controls. The goal is to be certain that there are no gaps in any of the controls. All three controls need to be in place in order to have an effective security plan when it comes to the voting itself.

9:40:28 AM

MR. TURNER related the security gaps, noting the importance of having a paper trail with some measure of accountability for the vote record that can be audited. The trend has been to go towards the best practice of a risk-limiting audit. He offered to cover that at a future hearing since it is definitely a separate body of work. He emphasized the need for a paper trail because without one it is not possible to have an effective audit. He stated that accessibility features are protected by federal law, which are typically not part of the design process when the voting systems are being developed; however, they should be since it can cause gaps. He acknowledged that often these features may be added on at the end of the process. He mentioned malware, which is malicious code that could be introduced into a voting system through a wired network connection or through a wireless networking connection. Malware could cause significant disruption such that voters could not cast their ballots, or the voting record could potentially be changed.

9:42:17 AM

MR. TURNER related that last year at the largest "hacking" convention in Las Vegas, CDC participated in a voting machine hacking village, in which every single voting machine that was available were subject to having vulnerabilities exploited and successfully hacked. The first machine had a Wi-Fi network

built into it, so it broadcast its own network. This voting machine was hacked from two rooms away within ten minutes.

9:43:02 AM

CHAIR KREISS-TOMKINS asked whether the demonstration voting machines that were hacked were the same type of voting machines that Alaska uses.

MR. TURNER answered that not every type of voting machine used throughout the country was represented at the conference. However, every onsite model was successfully hacked, he said.

9:43:39 AM

MR. TURNER provided another example of how malware can disrupt a large IT infrastructure. The City of Atlanta recently was hit with ransomware, a dreaded type of malware installed by a malicious actor on a system and it spreads as quickly and as far as possible. The user sees a pop-up screen that demands money be sent to a particular address because the user's data has been encrypted or locked up and cannot be accessed. The ransom was less than $50,000; however, the city was unable to pay it. Atlanta ultimately spent over $2 million in data recovery and remediation. Malware can be very small, but it can spread and have a massive impact.

9:44:51 AM

MR. TURNER said the last security gap when it comes to threats to the voting process itself is "information silos." Information silos happens when information stays within a particular department or organization. The FBI [Federal Bureau of Investigation], DHS [Department of Homeland Security], state, county, and city officials have recognized the importance and benefits of sharing information through all levels of government and across to different jurisdictions to make sure if something bad happens in one jurisdiction it can be prevented in others. He emphasized that DHS was doing a much better job, working with states and elected officials to make sure information is shared as broadly as possible.

9:46:12 AM

CHAIR KREISS-TOMKINS asked Mr. Turner to identify the biggest single vulnerability in Alaska's voting and election system and

his foremost recommendation for improvement to the security of Alaska's election system.

MR. TURNER said he was very impressed with Alaska's election system. He stated that the CAP [Center for American Progress] score was a "B". He suggested that additional consideration be given to make sure that only the appropriate people have access to systems, such that two-factor authentication be used at the local level. The two-factor authentication ensures that the local election officials are protecting their own legitimate access to the election and voting systems.

9:47:32 AM

REPRESENTATIVE BIRCH stated that Alaska's machines were purchased in 1998, so even though it is old it produces a hard copy record. He did not believe there was any intersection between the voting machine and the Internet. He asked whether newer technology could be used, for example, optically scanning the ballot and reporting the numbers, but retaining the ballot.

MR. TURNER answered that if the machines were produced in the late 1990s that they would not have any network connectivity. Typically, newer machines will be "off the shelf" so it would be incumbent upon the purchasing department to thoroughly vet and thoroughly test any new machines. Whether the testing would be done by state staff or contractors, it is important to have a level of assurance that the new machine can be tested to make sure that the machines do not have any functions or features it does not want. For example, the state may decide to not have network connectivity; however, the machine may have that functionality. If the only control over network access being turned on or off was by software that would provide a point of access for a malicious actor to gain access to the machine and turn on network connectivity. He emphasized that fully informing a procurement process was crucial so that the options and specifications are known.

9:50:39 AM

REPRESENTATIVE BIRCH asked whether Mr. Turner had any sense of the number of voting jurisdictions in which a hard copy ballot is retained in addition to an optically-scanned image.

MR. TURNER said he did not know but he offered to research and provide it to the committee.

9:51:26 AM

MR. TURNER turned to the "Intelligence Report." The goal of the Russian influence campaign was really to sow doubt by spreading misinformation. One of the ways to combat this activity is to ensure that only dedicated devices are used for election process, including the "public-facing front end" whether it was dedicated USB flash drives that would only be used one time in one way to ensure against compromising the information contained on the drive.

9:52:18 AM

MR. TURNER highlighted the threats to reporting results, including misinformation, such as reporting unofficial results most likely through social media. Secondly, we are likely to see denial of service attacks [DDoS or distributed denial of service], which is when hundreds or thousands of machines focus their requests on one website, for example, the State of Alaska's reporting website, to prevent legitimate traffic from getting through so it appears that the server is taken offline. He said some services like Cloudflare's (indisc.) or Google's "Project Shield" that can help protect against these types of automated DDOS attacks, but the real goal is to make sure that a plan to get unofficial reports out if service attacks occur. The plan if a service attack occurred or some other type of misinformation happened could include social media, press releases, traditional means, television or radio.

9:54:50 AM

REPRESENTATIVE KREISS-TOMKINS turned to the next presenter, Danielle Root, Center for American Progress (CAP), and said Ms. root would discuss Alaska's CAP report card, which was on members' desks.

9:55:22 AM

DANIELLE ROOT, Voting Rights Manager, Center for American Progress (CAP), stated that in 2016, primarily Russian hackers took unprecedented steps to infiltrate and disrupt [federal], state and local election systems. National security experts and state election officials do not know the full extent to which hackers breached election infrastructure. So far there has been no evidence that election outcomes were manipulated or altered; however, it is known that hackers attempted to breach the election infrastructure of at least 20 states, including Alaska.

For example, Russian operatives reportedly trolled Alaska's election-related databases in the weeks leading up to the 2016 elections. The infamous hacker, CyberZeist, obtained unauthorized access to Alaska's election website on Election Day, but did not succeed because built-in cyber defenses prevented the hacker from altering data or causing service disruptions. She cautioned that hackers are using more sophisticated techniques and may try again. Americans have been warned that attacks on election infrastructure have and will continue in future elections, including the upcoming 2018 midterm elections. Unfortunately, security experts and policy makers agree that state and local elections continue to be ill equipped to withstand attacks from hackers and foreign adversaries such as Russia.

9:57:00 AM

MS. ROOT reported that in February 2018, the Thunder for American Progress published a comprehensive review of the election-security preparedness in all 50 states and Washington D.C. detailing the continuing vulnerabilities of state election infrastructure and assigning grades based on election readiness. Alaska received a "B" which was the highest grade awarded. Alaska earned points for adhering to minimum cyber security best practices related to voter registration systems and for its widespread use of paper ballots for conducting elections to key areas of election security.

9:57:43 AM

MS. ROOT indicated that Alaska's election infrastructure remains vulnerable, which means that the state is open to election-related attacks. These vulnerabilities must be addressed. One area needing improvement is the lack of post-election auditing procedures. Currently, the number of ballots included in Alaska's post-election audits are ones based on a fixed percentage as opposed to a statistically-significant number tied to the margin of victory of one or more ballot contests as is common with risk-limiting audits. The [risk-limiting audits] are considered the "gold standard" of post-election audits as mentioned by other presenters today. Many states are moving towards risk-limiting audits and the CAP recommends Alaska do so.

9:58:27 AM

MS. ROOT stated that linking the number of ballots included in the post-election audit to the margin of victory rather than a fixed-percentage or number helps to ensure that enough ballots are examined to create convincing evidence that the outcome is correct. It also saves resources by guaranteeing election officials only examine the precise number of ballots necessary, she said.

MS. ROOT noted that Alaska's post-election audits also do not include voters stationed or living overseas, absentee or UOCAVA [Uniformed and Overseas Citizens Absentee Voting Act] ballots. In 2016, UOCAVA ballots amounted to more than 8,000 of ballots cast in Alaska during the presidential election. She emphasized that CAP recommends that all ballot types, including regular, early voting, absentee, provisional, and UOCAVA be eligible for inclusion in post-election audits. She cautioned that by only allowing certain categories of ballots, election officials may fail to detect anomalies in the tabulation of other ballot types.

9:59:29 AM

MS. ROOT emphasized that Alaska should terminate its use of electronic absentee voting, noting Alaska is the only state that allows any eligible voter to return a voted ballot electronically. Although she acknowledged that Alaska moved away from web portals, the state still allows voted ballots to be returned via fax. As Ms. Underhill mentioned earlier, computer scientists and computer experts have long warned that returning ballots via fax was insecure and subject to hacking and a myriad of ballot delivery problems. Voters deserve to have the security of their ballots protected and to have their ballots counted as they intended. She said that having their ballots transmitted through the mail means a paper record of intent exists instead of only a vulnerable Internet transaction that puts the security of their ballots at risk.

MS. ROOT advised that Alaska was awarded $3 million as part of the 2018 HAVA Election Security Fund to bolster its election preparedness. While she was glad that Alaska intended to use the funding to replace old voting machines and bolster its cyber security protections; she also cautioned that the state should consider using some of its funding to strengthen the state's post-election auditing procedures and require all voted ballots be submitted in-person or returned by mail. She concluded that by taking these steps Alaska could significantly improve its election-security preparedness.

10:01:04 AM

REPRESENTATIVE TUCK asked Ms. Root the percentage of ballots returned electronically in Alaska.

MS. ROOT said that information did not appear to exist, that the UOCAVA ballots were tracked but it does not track how many are returned electronically. Some advocacy groups are trying to obtain that information, but to date no public information was available, she said.

10:02:10 AM

REPRESENTATIVE KNOPP asked for clarification on the issue with fax-returned ballots and if it was voter information security and privacy or if it was due to the potential for ballot manipulation.

MS. ROOT responded that it depends on how the fax is transmitted since some states fax via the Internet and that is how ballots are also returned. She said this means that these ballots are vulnerable to manipulation. Other states use a dial-up fax, and any fax service is subject service disruption. Therefore, any type of cyberattack could prevent an election office from receiving or counting the voted ballots sent via fax. She pointed out that mail delivery also can be unreliable. She highlighted that if a large number of ballots being returned via fax could be affected by one service disruption, which could result in a large number of ballots not being counted.

10:04:02 AM

REPRESENTATVE TUCK directed attention to an audit synopsis provided in committee members' packets. He asked Ms. Root to identify the UOCAVA acronym.

MS. ROOT answered that UOCAVA refers to the Uniformed and Overseas Citizens Absentee Voting Act ballots. States are required to send out electronically or by mail ballots to US citizens living outside the country but UOCAVA does not require ballots to be returned electronically, she said.

10:05:02 AM

REPRESENTATIVE TUCK asked about the report referred to the DRE machine with VVPR under the section voter-verified audit trail. He asked for clarification on the acronym.

MS. ROOT answered the electronic machines were ones that print out a receipt of the voter's ballot choices, such that the voter would select their candidate or ballot initiative on a touch screen or machine; that the voter can view their decisions in a viewing window and subsequently confirm that the printed ballot matched what they chose on the touch screen. Once the voter touched "yes," the information would be preserved, and election officials could later review the information during an audit. However, election officials do not recommend this method and instead recommends paper ballots because not all voters check the paper receipt before submitting it.

10:07:28 AM

The committee took a brief at-ease.

10:08:03 AM

CHAIR KREISS-TOMKINS asked for the DOE's perspective on risk-limiting audits. He further asked about changing the state's practices on ballots submitted by fax.

10:08:38 AM

JOSIE BAHNKE, Director, Central Office, Division of Elections, Office of the Lieutenant Governor, stated that the division attended a technology fair with four federally-certified vendors looking at new election technology.

MS. BAHNKE referred to two issues, the process of risk-limited audits and the return of ballots online or by fax as the weaknesses in the Alaska election system. She described Alaska's audit process as being very robust. She said the DOE has looked at other state's risk-limiting audits, such as Colorado, who has adopted the risk-limiting audits. She advised members that Alaska is in the process of reviewing the risk-limiting audit process. In terms of ballot by fax, under UOCAVA, the state is required to allow for the return of absentee ballots online or by fax. The CAP has reported ballot returns as a weakness in Alaska's election system and due to the ongoing cyber-security concerns the DOE made the decision to suspend the return of those ballots online. However, the state

will still allow those ballots to be returned from overseas and nationally via fax or by mail.

10:11:16 AM

REPRESENTATIVE LEDOUX related her understanding that [UOCAVA] voters can receive their ballot online but can return the ballot by fax or by mail. She asked whether there was a time when the ballot could be returned by Internet.

MS. BAHNKE answered yes. In further response, she indicated that the DOE implemented Internet ballot returns in 2014 and 2016.

CHAIR KREISS-TOMKINS said he remembered friends returning their ballots by e-mail.

10:12:18 AM

REPRESENTATIVE LEDOUX asked whether this will allow oversees ballots to be returned by Internet means.

MS. BAHNKE answered that currently the division can provide online ballots to any voters, that online ballots are not restricted to UOCAVA voters.

10:12:42 AM

REPRESENTATIVE LEDOUX asked whether any group or geographic area in Alaska is allowed to return ballots through the Internet.

MS. BAHNKE answered the DOE made decision to suspend that practice due to ongoing cyber security threats until a more secure solution exists. In further response, she agreed the practice was suspended for all groups.

10:13:28 AM

REPRESENTATIVE BIRCH recalled testimony on the potential for disruption for ballots returned by fax. He asked for an estimate of how many ballots were faxed in the last election cycle.

MS. BAHNKE answered she did not have the precise number but estimated that under 1,000 were returned by fax.

10:14:05 AM

REPRESENTATIVE BIRCH directed attention to the discussion on the competence of the paper ballot audit trail. He asked how the [voting] information was transmitted from [rural] Alaska locations to election central on Election Day.

MS. BAHNKE deferred to Mr. Malander.

10:15:12 AM

PHILLIP MALANDER, Systems Administrator, Division of Elections, Office of the Lieutenant Governor, advised that the information is transmitted back via phone lines either verbally or via Paymo [an online project management application].

10:15:32 AM

REPRESENTATIVE BIRCH asked whether there would be an electronic transmission. He further asked whether that was susceptible to any cyber security issue and if it was considered an Internet connection.

MR. MALANDER said that generally the division does not consider that to be an Internet connection. Every system has some vulnerabilities but the risks in that area are considered relatively low.

10:16:13 AM

CHAIR KREISS-TOMKINS related his understanding that when Shishmaref or Nome election results are transmitted verbally or by phone line that it means the information is "called in."

MR. MALANDER answered yes; that is correct.

10:16:33 AM

REPRESENTATIVE BIRCH related that Alaska's voting equipment is now about 30 years old, so he wondered whether the division has been looking at vendors who offer similar voting capacity with paper ballots that provide an audit trail as well as an electronic or optical scan and transmittal.

MS. BAHNKE answered that the division recently reviewed four federally-certified vendors at the technology fair and all of them used paper ballots. She did not see Alaska moving away from that type of ballot.

10:17:17 AM

REPRESENTATIVE BIRCH asked for clarification on the training regime since there have been some issues in rural areas.

MS. BAHNKE answered that by statute the director submits a training plan to the Lieutenant Governor by March 1 in an election year. She offered to provide a copy of the election training plan. Since 2016, the division has been working to improve every aspect of its election management. Election training was one area, specifically, in which the division has improved its in-person training. The DOE has spent last month in the KTOO studio providing more interactive training, including making DVDs of the training. The division will have links to that training on its website, so she felt confident that the concern has been addressed. She said division was also confident it is ready for the 2018 election.

10:18:47 AM

REPRESENTATIVE LEDOUX asked whether any concern exists that people living in major cities can vote over a longer period of time, so they have more voting opportunity than those in rural areas. For example, a person living in Anchorage can take an absentee ballot to the Anchorage International Airport US Postal Facility and have the ballot postmarked on Election Day. She was unsure if that opportunity existed in the villages.

MS. BAHNKE answered that access to the ballot is central to her role as the director; however, she said she did not have an opinion on that issue.

10:20:18 AM

REPRESENTATIVE LEDOUX said she was surprised that the recent Anchorage "Vote by Mail" election administrative costs were higher than for routine in person elections. She asked whether an all-mail ballot would cost the state more to administer.

MS. BAHNKE answered that the Municipality of Anchorage briefed the Election Policy Workgroup yesterday on its municipal election. In 2018, the MOA was required to purchase new equipment and software in order to conduct its vote-by-mail election. Those will not be ongoing costs, she said. The DOE reviewed other states whose elections are exclusively vote-by-

mail elections and these states have realized cost savings. She offered to provide the information to the committee.

10:22:30 AM

CHAIR KREISS-TOMKINS related his understanding that the cost of Anchorage's municipal vote-by-mail election was driven by one-time upfront expenditures that would not be necessary in future years.

MS. BAHNKE answered yes.

10:22:44 AM

CHAIR KREISS-TOMKINS said one recommendation Ms. Root made for Alaska was to include all ballots, including UOCAVA [Uniformed and Overseas Citizens Absentee Voting Act] ballots in post-election audits. He asked whether the division had a perspective on that recommendation or if it has an intent to implement anything along those lines.

MS. BAHNKE answered yes; that the division does plan on doing so.

10:23:10 AM

ADJOURNMENT

There being no further business before the committee, the House State Affairs Standing Committee meeting was adjourned at 10:23 a.m.