**Auditing Subcommittee Proposal**

**2018 HAVA Election Security Funds**

**Proposal #1: Engage an expert in statistical analysis to study Minnesota’s Post-election Review and to recommend changes to the Post-election Review process**

Minnesota Statutes 206.89 states that after every state general election, Minnesota counties must perform a post-election review of election results returned by the optical scan ballot counters used in the state. The review is a hand count of the ballots for each eligible election (U.S. President, U.S. Senator, U.S. Representative, and Governor) in the selected precincts compared with the results from the voting system used in those precincts. The purpose of this review is to verify accurate tabulation of the voting system. Because current statute (M.S. 206.89 Subd. 4) specifies that some valid votes must not be included in evaluating voting systems’ performance, adjustments are applied to the differences identified through this comparison. However, the unadjusted differences are also published.

It is proposed that the Office engage an outside expert to analyze the post-election review, including unadjusted differences, to quantify its likelihood of detecting tabulation errors, subject to the assumption those errors are large enough to change election outcomes and other suitable assumptions. This will inform any necessary improvements to increase the likelihood of detecting tabulation errors.

**Proposal #2: Conduct a study of Minnesota’s data sharing partners**

The Office of the Secretary of State exchanges data with third parties including the Courts, the Department of Public Safety, Social Security Administration, and more. This data is shared to ensure Minnesota’s voter registration list is as accurate as possible and any potential eligibility challenges are addressed.

It is proposed that the Office engage an outside consultant to thoroughly examine and audit the security of information being moved between the Office and other agencies and entities. The proposed consultant will work with the Office to address any potential security concerns and develop any additional protocols needed.

**Communications Subcommittee Proposal**

**2018 HAVA Election Security Funds**

**Proposal #1: Invest in improvements for securing information sharing with counties**

As election officials continue to be the targets of phishing attacks, it is proposed that the Office of the Secretary of State develops or contracts with a third party vendor to secure sensitive information and data exchanges between counties and the Office. This may take many forms, including enhanced email security (removing hyperlinks, adding a disclaimer to emails sent and received, etc.), and developing a secured portal where links and other sensitive information is to be shared. Such improvements have already been implemented in a number of Minnesota counties, this would expand upon that and secure the information coming from the Secretary of State office as well.

**Proposal #2: Enhancing website security and accessibility**

The Office’s public website (<https://www.sos.state.mn.us>) is the Office’s primary public information channel. It is a place voters go to find their polling place, learn their rights as a voter, and more. Strengthening the security of this website is vital to ensure that the information being distributed to the public on the website is reliable and accurate, and secure from those who wish to spread disinformation and potentially cause voter suppression. For these reasons, it is proposed that the Office invest in additional security measures to enhance the security of the website. This proposal compliments the cybersecurity subcommittee proposal of investing in software that would validate the code of the website to ensure its accuracy and security.

Additionally, it is proposed that the Office makes all pages of its website accessible to those who may have a disability. In addition to making the desktop website accessible, it is proposed that the Office invest resources to make all webpages mobile-friendly. This will allow all Minnesotans to have equal access to the same reliable and accurate information, regardless of how they visit the website or any disabilities they may have.

**Proposal #3: Recruiting and training election judges**

It is proposed that the Office of the Secretary of State dedicate additional resources to assist counties and cities in recruiting election judges and conducting additional election judge training related to accessibility at the polling place, using e-poll books, and cybersecurity in general. Election judges are at the front lines of our elections, having them equipped with the latest training on issues relevant to today’s elections will ensure elections continue to run smoothly and voters continue to receive the assistance needed.

**Cybersecurity Subcommittee Proposal**

**2018 HAVA Election Security Funds**

**Proposal #1: Automatic Behavioral Analysis***Recommended by the U.S. Department of Homeland Security and the Election Infrastructure Subsector Government Coordinating Council*

Database Activity Monitoring Software (DAM) is technology that monitors and analyzes database activity in real-time to alert and block suspicious activity. This collects all log-ins, log-outs, updates, and privileged activities. The DAM product creates an audit trail to show the “who, what, when, where, and how” for each database that is being monitored.

Investing in this software will allow the Office of the Secretary of State to have increased monitoring capabilities to oversee its databases, and quickly identify and block any malicious activity.

**Proposal #2: Network Segmentation***Recommended by the U.S. Department of Homeland Security*

Network segmentation is the practice of splitting the Office’s network into subnetworks. These subnetworks limit what the users are able to access. For example, users in the Elections Division (or Elections Segment) would only be able to access elections data. Similarly, Business Services would only be able to access Business Services data.

Network segmentation is vital for the Office because if a workstation in Business Services is compromised without being segmented into a subnetwork, that malware or ransomware could potentially travel to other departments such as elections.

**Proposal #3: Security Information and Event Management (SIEM) software***Recommended by the U.S. Department of Homeland Security*

Security Information and Event Management (SIEM) is technology that provides real-time analysis of logs and security alerts generated by network hardware and applications in a single location.

Currently, the Office’s IT administrators are required to manually search each department’s logs and security alerts. SIEM technology will allow IT administrators to search one comprehensive log. This technology is time efficient and will reduce the time necessary to look through possible suspicious activity.

**Proposal #4: Next generation anti-virus software**

As viruses and malware advance, so must antivirus software. Additional antivirus software will detect new viruses and malware without daily/hourly signature updates, and is needed to augment the Office’s current “signature based” antivirus software with next generation “behavior based” software.

“Signature based” software looks at specific known or previously identified malicious coding and then blocks that malicious coding. “Behavior based” software analyzes what that coding does, even if the coding has not been previously identified as a known malicious code, and instead blocks the code based on the malicious behavior.

**Proposal #5: Privileged Access Management (PAM)***Recommended by the U.S. Department of Homeland Security and the Election Infrastructure Subsector Government Coordinating Council*

Privileged Access Management (PAM) refers to systems and processes for giving organizations better control and monitoring capability into who can gain privileged access to the computer or system. Like DAM, it creates the audit trail to show the “who, what, when, where and how” for each privileged account and helps protect the misuse of privileged accounts.

An additional example of privileged access management is granting an employee access to a system like the Statewide Voter Registration System on a temporary basis. Rather than manually turning “on” or “off” that employee’s privileges, PAM will automatically remove access outside of the parameters originally set.

This automated system ensures that the right users have the right access at the right time, and IT administrators can see who has access when, and for where.

**Proposal #6: Infrastructure Upgrade**

The Office of the Secretary of State will need an infrastructure upgrade or replacement to accommodate for the additional capacity needed to support the additional load of the SIEM and DAM systems.

**Proposal #7: Additional Network Storage and Backup Storage**

Added network storage is needed to store the additional logs that are captured by the SIEM and DAM systems. In order for the Office to remain compliant with Minnesota Statutes regarding data practices and data retention, the Office simply needs more storage capacity.

**Proposal #8: Data Core Continuous Data Protection (CDP)**

Continuous Data Protection (CDP) provides automatic captures of data on network storage for recovery in the event of data corruption or a ransomware infection.

For example, in the event that a virus causes damage to the network, the network can be “rolled back” to any point in time prior to that virus in a matter of seconds. Currently, the Office needs to manually restore the network after any sort of data corruption or infection. In the event of data corruption or a ransomware infection immediately before or during an election, hours can be too long and may be detrimental to the administration of Minnesota’s elections.

**Proposal #9: Cybersecurity training for counties and cities***Recommended by the Election Infrastructure Subsector Government Coordinating Council*

It is proposed that the Office hire a “cyber navigator” to assist counties and cities with election related cybersecurity needs, including assistance responding to cybersecurity incidents. The purpose of a navigator is to provide practical cybersecurity knowledge, support, and services to local election officials who otherwise would not have access to them. These navigators can conduct assessments of local election offices. After conducting assessments, the navigators can work with county IT staff or vendors to create cyber security policies, mitigate vulnerabilities discovered during the assessments, and establish best cyber hygiene practices within the office. Additionally, these navigators can serve as a resource for local election offices as they consider improvements to the cybersecurity of the office.

**Proposal #10: Additional licensing for systems scanning/testing***Recommended by the Election Infrastructure Subsector Government Coordinating Council and the National Institute of Standards and Technology*

This is a joint recommendation with the HAVA Working Group Communications Subcommittee.

Currently, the Office of the Secretary of State maintains four licenses to scan the online absentee ballot application and voter registration tools, the Minnesota Business and Lien System, and the notary services online portal. Additional licenses are needed so that all of the Office’s public facing websites and online tools can be scanned for vulnerabilities. It is proposed that the Office purchase 20 additional licenses to ensure all of the Office’s public facing websites can be scanned and a full vulnerability review of the underlying code can be done.

**Proposal #11: Policy Writer***Recommended by the U.S. Department of Homeland Security*

The Department of Homeland Security and this subcommittee recommends that the Office hire a policy writer to develop written based cybersecurity policies and procedures. This policy writer’s services are anticipated to be approximately six months in length, with an approximate hourly rate of $140/hour. Once initial policies are done, the Office believes current staff will be able to handle the annual reviews and updates.

**Proposal #12: Ongoing support for multi-factor authentication (MFA)***Recommended by the Election Infrastructure Subsector Government Coordinating Council and the National Institute of Standards and Technology*

Multi-Factor Authentication (MFA) is a security system recommended by the Department of Homeland Security and a National Institute of Standards and Technology (NIST) standard that requires more than one piece of information to verify a user’s identity for a login. Using MFA provides an extra safeguard for the Office of the Secretary of State when county or local election officials access our system.

With the actual security system already purchased by our office, the ongoing support for the system includes maintenance, version upgrades, security patches, and live support. By purchasing ongoing support, the Office is able to protect the MFA system and the 5,000 licenses purchased from expiring and maintain the security system recommended by IT experts.

**Equipment and e-Poll book Subcommittee Proposal**

**2018 HAVA Election Security Funds**

**Proposal #1: Expand absentee and mail-voting for voters with a disability**

Mail voting in Minnesota, whether in all mail jurisdictions or by absentee ballot, is currently not fully accessible to voters with disabilities. All forms of domestic mail voting currently require ballots to be sent to voters in paper form and to be completed manually. Voters serving in the military or living abroad, however, have the ability to receive their application via email, mail, or fax. If materials are received via email, they still must be printed, completed, and returned by mail.

It is proposed that the Office of the Secretary of State make absentee and mail voting for voters with a disability accessible. Accessible absentee and mail voting can be accomplished by either expanding or improving the current process for military and overseas voters or purchasing software that will allow voters with a disability to receive and mark their ballot electronically, and then return the printed ballot to their local election official. This will allow Minnesota’s voters with disabilities to vote privately and independently, with meaningful access to the ballot.

**Proposal #2: Provide sub grants to local jurisdictions for improved election security and accessibility**

It is proposed that the Office invest in the security of local jurisdictions’ election security by providing sub grants to local jurisdictions for the following items:

1. Updated computers and/or software for election administration
2. Additional physical security for election equipment storage
3. Increased polling place accessibility

Each jurisdiction will have the ability to spend their allotted funds on any of the above items, remaining consistent with the requirements of the 2018 HAVA Election Security Funds and improving the administration of elections.

**SVRS Subcommittee Proposal**

**2018 HAVA Election Security Funds**

**Proposal: Strengthen, secure, and modernize Minnesota’s Statewide Voter Registration System (SVRS)**

Minnesota’s Statewide Voter Registration System was launched in 2004 using over $1.2 million of state general fund dollars and over $5.1 million in funds appropriated from the federal HAVA account. Since its development, the Office has added various components to accommodate changes to voting and elections. Because of this, the system is in need of investment to keep it functioning well.

It is proposed that the Office invest in a re-work of the system. Instead of re-writing the system from scratch with a large rollout, this would be done piece by piece over an estimated four years’ time. To complete this, it is proposed the Office hire three additional staff, including an IT Business Analyst, IT Developer, and an Elections Administration Specialist to supplement current staff during this project.