**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 (SEIM) 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.