Testimony before the House Committee on Homeland Security
October 15, 2019

Steven S. Sandvoss
Executive Director
Illinois State Board of Elections

As the Committee is aware, in June of 2016 the Illinois State Board of Elections (SBE) was the victim of a cyber-attack which at the time was of unknown origin. It has since been learned that the attack was perpetrated by Russian operatives who were seeking unauthorized access into the voter registration database maintained by the SBE. In response to this attack, measures were immediately undertaken to close the access point of the intrusion, assess the extent of the penetration, determine whether any data was manipulated or destroyed, and ascertain which voter records were improperly accessed, with the purpose of alerting said voters and giving guidance to assist them in protecting their sensitive information. It should be noted that an analysis of the breach did not reveal any evidence that specific voters were targeted or that the attack focused on any particular region or demographic. The SBE quickly alerted Federal law enforcement, and fully cooperated with their investigation. Following the initial steps described above, the SBE undertook an unprecedented effort to secure its voter registration database as well as other IT related applications.

In March of 2018, the EAC provided $380 million in grant money to the states to assist in their cyber-security efforts. Illinois' share was $13.2 million, with a requirement that the State provide a 5% match; which amounted to $661,615. Shortly after receiving this grant money, legislation was passed in Illinois that earmarked no less than half of the grant money to a Cyber Navigator Program (CNP), to be created and administered by the SBE.

In order to receive any of the grant money, Illinois' Election Authorities (EAs) must agree to participate in the CNP. (The EAs consist of 101 county clerks, 1 county board of election commissioners and 6 city boards of election commissioners, who are responsible for maintaining a list of registered voters within their jurisdiction, securing election voting and tabulating equipment and conducting the actual election on election day, as well as early and mail in voting.)

The CNP consists of 3 basic parts; 1) Requiring the EAs to adopt the Illinois Century Network (ICN) as their internet service provider for all traffic between their offices and the SBE. 2) Engaging in a Cyber Security Information Sharing Program with the EAs to share cyber-security related information and 3) Creation of a team of "Cyber Navigators" to provide cyber-assistance to the EAs.

Illinois Century Network (ICN)

The ICN is a state managed network delivering network and internet services to government agencies in Illinois. The goal of the ICN is to provide EAs with a cleaner and safer internet. The SBE Plan would bring all network traffic to and from the EAs to an internal "10 dot IP" network system and "whitelisting" IP addresses for access to the IVRS website. Isolating this network to one under the complete control of the SBE and Department of Innovation and Technology (DoIT) ensures that voter registration data and

EA management operations never actually flow over the internet. Additionally, this provides us the ability to provide additional security measures and monitoring.

Cyber Security Information Sharing Program-

In partnership with the Illinois State Police's division of Statewide Terrorism and Intelligence Center (STIC), the SBE is overseeing the Cyber Security Information Sharing Program, which involves researching and gathering of information related to pertinent cyber-attacks and cyber resiliency and sharing that information with all federal and state stakeholders. Our goal is to consolidate numerous information sources and, with feedback from local Election Authorities, distill it into the most valuable, actionable information possible.

Cyber Navigators

The Cyber Navigators are assisting the EAs by performing onsite risk assessments and providing resources to ensure Election Security for 2020 and beyond. Currently 9 Navigators are assigned in 4 regional zones in the state. (2 per zone, and 1 lead navigator). The Navigators will be offering additional services such as phishing assessments, penetration testing and educational trainings. They will also be performing additional risk assessments on physical security and best practices in securing voting equipment.

In addition to the CNP, the SBE worked in partnership with the Illinois National Guard's cyber security team for coordination of a cyber-defense system to provide cyber protection for both the SBE and the EAs prior to and on Election Day. Members of the Guard were stationed in all regions of the state, at the SBE, at STIC and their own bases to be ready in the event of a statewide cyber event.

Following the creation of the CNP, the SBE released $2.9 million of the aforementioned grant funds to the participating EAs to make purchases to upgrade election related computer systems and to address cyber vulnerabilities identified through the risk assessments performed by the Cyber Navigators and/or other assessments of existing election systems. Funds could also be used to implement cyber security best practices for election systems and other activities designed to improve the security of the election systems.

Steps Taken to Improve the SBE's Cyber Defenses

In addition to the CNP, the SBE took the following steps to beef up its own cyber security.

- Hired two additional highly experienced IT staff, including a Chief Information Security Officer (CISO) with over 20 years of Information Security experience
- We have deployed advanced Next Generation Endpoint Security applications which protect agency systems from ransomware and other types of malware. This includes machine learning Endpoint Detection and Remediation (EDR) technologies to help with incident response, forensics and remediation of security events.
- New agency perimeter firewalls have been installed which also includes network intrusion prevention systems. Web application firewalls were also deployed to protect our agency's public facing applications.

- Secure Web Gateways have been deployed which provides category and reputation filtering to ensure agency Internet traffic is protected from malicious sources.
- Our email security posture has increased significantly due to implementations of strict spam/phishing policies and creation of agency Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting & Conformance (DMARC) records.

- Data Loss Prevention (DLP) technologies have been deployed to protect against sensitive data exfiltration. We are also in the process of deploying full disk encryption solutions to our endpoints.
- We partner with the Illinois Department of Innovation and Technology to transfer network and system logs to their 24/7 Security Operations Center (SOC).
- We are running weekly internal vulnerability scans against all agency systems and websites. Illinois Department of Innovation and Technology is running weekly vulnerability scans against our public facing websites. DoIT and DHS have also performed penetration tests and risk & vulnerability assessments.
- Future initiatives include implementations of additional email, DLP, log management and cybersecurity education technologies.

Looking to the future, the SBE believes it is necessary to maintain the Cyber Navigator Program indefinitely and possibly expand it to address the continuing needs of the EAs. Cyber Security is an ongoing, ever escalating process that doesn't have an end date, and as such there will be an ongoing need for funds to maintain the program. At present, the primary mission of the Cyber Navigators is to perform risk assessments of the IT systems of all the EAs who are participating in the CNP (all 108 EAs are participating in the CNP and have completed the first round of risk assessments). The EAs are in the process of evaluating the Assessments to determine what type of security enhancements are needed and are accessing the HAVA grant funds to cover the expenses. Some of the other steps that have been taken to enhance security leading up to next years elections are as follows:

- Working with the election equipment and management vendors to improve their security posture. This involves a series of questions related to company ownership, personnel, cloud security and processes for identifying cyber security risks, incident handling and recovery, testing, patching and anomaly handling of hardware and software and process for handling the movement of data.
- Participating in Table Top Exercises
- Working with the Emergency Management officials to coordinate preparedness for the upcoming election cycle
- Developing a PR campaign to combat misinformation/disinformation, particularly on social media. The SBE has produced videos to assist the election officials and voters on how to spot and report same as well as videos on how to maintain voting machine security and integrity.