UNITED STATES ELECTION ASSISTANCE COMMISSION

TESTIMONY

BEFORE THE SUBCOMMITTEE ON INFORMATION TECHNOLOGY OF THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

SEPTEMBER 28, 2016

U.S. Election Assistance Commission

1335 East West Highway, Suite 4300, Silver Spring, Maryland 20910

Introduction

Good afternoon Mr. Chairman and Members of the Subcommittee on Information Technology of the Committee on Oversight and Government Reform.

I am pleased to be here this afternoon on behalf of the U.S. Election Assistance Commission (EAC) to discuss cybersecurity and ensuring the integrity of the ballot box.

The EAC is a bipartisan commission consisting of four members; currently there are three members actively serving on the Commission. The EAC's mission is to guide, assist, and direct the effective administration of Federal elections through funding, innovation, guidance, information and regulation. The Election Assistance Commission ("the EAC") was created by the Help America Vote Act of 2002 (HAVA). HAVA was enacted after the 2000 presidential election highlighted a number of election administration concerns related to voting systems throughout the nation. The EAC was charged with three duties: (1) develop and administer a voting machine testing and certification program, (2) develop and administer a national clearing house for election administration information, and (3) distribute HAVA grants to states to allow them to purchase new, more secure voting machines and systems.

Since its inception, the EAC has and continues to carry its charge. 47 of 50 states use the EAC's voluntary voting machine Testing and Certification Program in part or as a whole; we produce the most comprehensive election administration survey in the country; and we produce volumes of materials designed to help Election Administrators run their elections more efficiently and efficaciously. These materials help the better states understand and react to the current cyber security threats against their voting systems. States and local election officials run the elections, and we support them.

Scope of My Testimony

This testimony discusses election security through three topics: (1) an overview of the American election administration system's inherent security (2) the breaches of two states' voter registration databases and how they exemplify the strength of the American election administration system, and (3) the EAC's support regarding the security of the American election administration system. Election security may only recently have been brought to many citizens' minds, but we at the EAC and election officials around the country have been focusing on the security of American elections for many years.

1. Overview of the American Election Administration System

The American election administration system is comprised of 50 states and territories. These states and territories are made up of thousands of county and local election jurisdictions. Each of these states, territories and local jurisdictions has developed their own processes and procedures for conducting federal, state and local elections. Each state's election systems are uniquely designed and autonomous from one another. There is not a single or uniform national system that manages the federal elections. Because of the decentralized nature of the American election administration system, there is no single, uniform national system that would affect the outcome of election results for the November 2016 Presidential Election. The complexity of our American election system both deters potential attacks and allows election officials to ensure the integrity of elections in the event of an attack. This complexity protects both national and state-level elections.

These many autonomous components allow states to secure their election with many layers of security. These layers start at the ballot collection process. Citizens cast their votes at a voting machine that is not connected to the internet. Physical security measures ensure that potential bad actors cannot access the voting machines without being noticed. Local election administrators collect the votes from the voting machines and physically transport, not electronically transmit, them to the election headquarters where they are tallied. This physical transportation ensures that a hacker cannot alter the tally during transportation. These results are subsequently reported to the state election official, who then reports those results to the public. States use standards of care and security procedures during this process to further ensure security. Each of these layers includes its own security processes and procedures, and each is capable of operating autonomously. These security measures are both abundant and redundant.

(a) Decentralized Election System

The American election administration system is a vast, decentralized, and non-uniform system comprised of thousands of local jurisdictions and moving parts. This decentralization establishes an inherent level of security in that it is not a uniform system with a single point of access. These attributes also allow election officials to ensure the integrity of their elections in the event of an attack by allowing election officials to monitor and audit the election process at many levels throughout the process.

First, a large amount of resources and time would be required to develop and execute an attack on the American election system because of the decentralized and non-uniform nature of the system as a whole. Because voting machines are not connected to the internet, a bad actor would need to physically access hundreds of voting machines that collect the votes. As stated above, a vast array of differing security systems and protocols protects each of these voting machines. This makes it incredibly complex to attempt to affect an election because a potential bad actor would need to learn and then access each of these systems. A bad actor would also need the man-power necessary to physically access each of these systems. Not only would a bad actor need to physically access each system, but that access would need to be done without being detected because of auditing and monitoring procedures discussed below. The resources required to complete either of these steps is immense.

To put this in perspective, consider Wisconsin, which has over one thousand four hundred (1400) local jurisdictions. Many of these jurisdictions have more than one polling place, and each of these polling places has multiple voting machines. Additionally, each one of these jurisdictions may have its own, unique security practices and protocols. So, if someone were to attempt to attack Wisconsin's elections, they would have to gain information about and successfully breach a significant portion of the voting machines in a significant portion of the 1400 jurisdictions without being detected. From a national perspective, there are more than 114,000 active polling places on Election Day. The required number of people needed to access this many different points is immense, and this surely is a deterrent against attack.

Second, the many layers of the American election system allow for monitoring and auditing of the system at each layer. The system allows election officials to be able to monitor for problems at multiple stages and incrementally verify the results of the election as not being the result of tampering.

Starting at the voting machine and progressing sequentially to the reporting of results, vote tallies and results can be and are audited in a layered, sequential format which allows for isolation and examination in the event of an error or anomaly. First, each individual voting

machine can be audited. Second, the polling location's votes can be audited as a whole. Third, the jurisdiction's results can be audited. Fourth the state's results can be audited. These many audit points are a result of the decentralized design of the system, and they also provide a method by which state election officials can detect tampering or anomalies.

It is important to note that audits are different from recounts and can identify anomalies and errors within the system. Recounts are methods by which vote tallies are verified. Recounts only ensure that votes were counted correctly. However, audits are methods by which the integrity of the system is verified. Audits ensure that the system collected votes correctly and was not compromised. As an example, some touch-screen voting machines, direct-recording electronic voting machines, store votes on memory cards, and these memory cards are used to tally votes. Many of these machines also produce a paper document that records the votes. This paper trail can then be used to verify the electronic tallies aggregated from the memory cards. This is just one of many ways voting systems are able to be audited, and auditing allows election administrators to identify and isolate attempts to tamper with the system.

The American election administration system is secure. It is secure because, by nature, it deters potential attackers with its complexity and lack of central access point. It is also secure because its design allows it to be audited; this allows election officials to isolate potential breaches, tampering, and anomalies.

2. The Recent Breaches of Voter Registration Databases in Arizona and Illinois

American Elections are secure, but this does not always prevent bad actors from attempting to affect them. This year, hackers accessed a number of computer systems related to the election, not voting systems. Breaches of these computer systems that are germane to this hearing include: (1) Arizona's voter registration list, (2) Illinois's voter registration list, and (3) the Democratic National Committee's email system. These breaches are important because they exemplify two important attributes of the American election administration system. First, while the voter registration systems were attacked, they demonstrate that the system was able to detect the hacks and the election officials were able to determine whether any data was lost or changed. Even though hackers breached the first level of security in Arizona and Illinois, the security monitoring and redundancy programs worked and election operations were not adversely affected. Second, the attacks on the voter registration databases differ in both form and potential effect from the breach of the Democratic National Convention's email system. These breaches can be used as a way to examine the security of the American election administration system and demonstrate its strength.

Based on the information we have, the breaches of the voter registration databases and the breaches of the DNC's email systems differ from each other in both form and potential effect. They differ in form because the attacks on the voter registration databases were attacks on government protected databases, while the attack on the DNC's system was on the email system. They differ in potential effect because attacks on a voter registration database do have the potential to directly affect actual election operations, i.e. interfere with voters' ability to obtain a ballot at the polling place, but attacks on a private committee's email servers affect only election political operations tangentially by interfering with the private committee's ability to advocate. It is important to remember that these two types of breaches are not commensurate and need to be examined separately.

When examining the breaches in Arizona and Illinois, it is important to remember that their security and redundancy systems worked. Using the above discussed layers of security, state and local election officials worked with state and federal law enforcement to quickly

identify the issue, evaluate potential impacts of the breaches, and ensure that the data was in the same condition as it was before the breach. In both cases there were processes in place to identify the intrusion, mitigate the damage, and audit the records to ensure accuracy. Had there been changes to data, election officials would have been able to identify those changes and use backup data, which they create on a regular basis as part of the system redundancy. Also, because America does not have one singular election administration system, an attack and breach of one state's voter registration system does not compromise the entire country. So, other states were not adversely affected by the breaches in Arizona and Illinois. Instead, other states were able to use these incidents as learning opportunities and able to take steps to ensure their systems remain secure.

This type of security preparedness and responsiveness is what helps keep American elections secure, even when they may be the target of some bad actors. This is why one of the many ways the EAC supports and furthers the security of the American election administration system is by helping states develop and share best practices.

3. EAC's Support of the American Election Administration System

The American election administration system is a complex system with many inherent security features. The EAC believes that every American's vote is important and should be safeguarded. That is why, since its inception, the EAC has incorporated both physical and cyber security of elections into its work. There are four areas which the EAC focuses its security efforts: (a) the EAC's Voluntary Voting System Guidelines; (b) testing; (c) monitoring; and (d) best practices, training, and guides.

(a) The EAC's Voluntary Voting System Guidelines

The Voluntary Voting System Guidelines (VVSG) are a comprehensive set of voting machine requirements. The EAC drafts, maintains, and monitors compliance with the VVSG. The VVSG include more than 1000 requirements including requirements for security, software, hardware, functionality, usability and accessibility. Within security, the VVSG focuses on general data security and more specifically data transmission. Within the topic of security, the VVSG focuses on general data security and more specifically data transmission.

Each state determines how to certify voting machines as acceptable for use in its elections. 47 out of 50 states have incorporated either the entirety or part of the VVSG system into their certification process. Some states require EAC certification of systems before the voting system may be used in the state. Other states use the VVSG to draft their own certification procedures. Still others require that EAC labs test voting systems before they may be used in the state.

What is truly innovative about the VVSG is the way in which they are drafted. Last year my fellow commissioners and I worked to update our drafting process. Alongside the National Institute of Standards and Technology (NIST), we created a system that leverages working groups and combines the expertise of government entities, private sector businesses, and private citizens to continually remain apprised of new innovations in the field. Cyber security is no exception. When redesigning the drafting structure in 2015, we made sure to include a security working group that represents the security community in the drafting process of all areas of the guidelines.

The security group is an active working group that provides up-to-date information on cyber security throughout the drafting process. For example, the electronic transmission of vote

tallies presents the potential for vulnerabilities in cyber security if the transmission system is not properly designed. However, electronic transmission of vote tallies is a desirable option for some election administrators because it saves time and resources. Techniques like our drafting structure allow us to stay ahead of these developments and their potential vulnerabilities. While the VVSG allow for electronic transmission of tallies, they only allow for this type of transmission if the voting system contains the proper security protocols. The VVSG allow election officials to develop their systems with new technologies while simultaneously ensuring that security is maintained. We are already working on the next set of guidelines.

(b) Testing and Certification

A critical part of our Testing and Certification Program is our voting system test laboratories. The EAC tests voting machines against VVSG requirements in EAC labs. When a machine meets the requirements, the EAC certifies the machine as conforming to the VVSG. In states that require EAC certification before a machine may be used in that state, completion of this process is a requirement that must be met before the machine may be procured by state officials. In all states, certification gives state officials confidence that the machines that are purchased are of the highest quality.

In the testing process, voting machines are tested against physical and cyber security requirements found in the VVSG. Regarding cyber security, machines are tested and assessed against requirements for: passwords, user roles, access controls, audit logs, vulnerabilities, and source code. Test laboratories also review system documentation for all aspects of the voting system being tested. This includes all functional models, settings, and user manuals. All testing information including test plans and test reports are available on our website for anyone to review.

These labs test voting systems against the requirements contained in the VVSG. Approval by one of these laboratories is required before our testing and certification program will certify a system. Before a laboratory can test a system under the EAC's program it must undergo a thorough accreditation process. In order to be accredited, the National Voluntary Laboratory Accreditation Program (NVLAP) must inspect the lab. Based on this inspection the Director of NIST must recommend the lab to the EAC. The EAC then conducts its own accreditation assessment to ensure full compliance with all EAC programmatic requirements. If the lab passes the EAC assessment, then the EAC may accredit the lab. Once a lab is approved and becomes operational, it is subjected to an audit conducted by the EAC or NIST to ensure the lab remains in compliance with the approval standards. Last year, the commissioners of the EAC accredited a new test laboratory for the first time in five years to allow for a more efficient and effective certification process.

Use of the Testing and Certification Program provides an additional level of security in the electoral system and gives state officials an additional level of confidence when making a purchasing decision or working to maintain their voting system.

(c) Monitoring

The EAC conducts a quality monitoring program for all EAC certified systems. Monitoring occurs throughout the entire election process, not just on Election Day. This monitoring includes: manufacturing facility audits; review and testing of operational machines; field anomaly reporting; investigation into reported field anomalies and dissemination of product advisories. All reports, system advisory notices and investigations are available to election officials and the public. Our monitoring program has successfully worked with state and local

election officials as well as voting system vendors to identify operational issues with EAC certified voting systems before the election, resolve these issues, test and certify the resolutions, and deploy the improved system before Election Day. To the EAC, monitoring is about ensuring quality of elections, and ensuring the quality of American elections is our highest priority.

(d) Best Practices, Training, and Guides

The EAC's work in security goes beyond voting machines. The EAC helps election officials focus on their elections by providing them with best practices and industry trends from around the country. We prepare and distribute best practices, training, and guides to election officials in an effort to arm election administrators with the best and most up-to-date information. These resources are in an easy-to-digest and actionable format.

Specifically regarding security, we prepare, maintain, and distribute Election Management Guidelines and Quick tips. To help ensure that the American election administration system is ready for contemporary threats and protected against potential vulnerabilities, we publish materials and training guides related to current events. For example, after learning about the hacks in Arizona and Illinois, we re-distributed our election security preparedness resources which includes a checklist for securing voter registration data. Regarding implementation, we continually publish and update our Managing Election Technology resources. These help election administrators to better implement election systems.

Ever aware of the broader community and our charge to act as the national clearing house of election administration information, we also host roundtables on a variety of topics related to voting system security, co-host symposiums with NIST about security and the Future of Voting, and ensure the topic of cyber security is present in our public meetings and other events. At the last EAC public meeting, we hosted a discussion of states' best practices concerning contingency planning and system security. Experts in the field, such as Secretaries of State and testing lab directors, led a robust discussion of modern and cutting edge techniques. We invite you to attend our future meetings and watch the videos of our previous meetings which you can find online.

Conclusion

The American election administration system inherently deters bad actors who may want to adversely affect the election process, and the system allows the front line of dedicated election officials to audit and monitor the system in a way that allows them to solve problems as they arise. There will always be threats to American elections. The attacks on Arizona's and Illinois's systems reminded the country of this. The EAC, however, works everyday to ensure that local officials are best prepared to prevent these threats from coming to fruition.

Voters should have confidence in the elections. I was recently in Arizona when I was approached by a gentleman who told me that he knew American elections were secure because he had worked as a poll worker. Working as a poll worker allowed the voter to see exactly how elections work and all of the security measures that are in place in every election cycle. He was confident in our elections because he had seen them for himself. Any and all Americans who might have questions or concerns about our electoral system should volunteer as poll workers or speak to their local election officials. The time commitment of volunteering is low, and you will be providing a valuable public service.