Testimony of Matthew Masterson
Chairman U.S. Election Assistance Commission
Joint Hearing of House Ways and Means Committee & Senate Education, Health, and Environmental Affairs Committee
Maryland Legislature
September 6, 2017

Introduction

Since its inception in 2002, the U.S. Election Assistance Commission (EAC) has supported election officials' ongoing efforts to provide accessible and accurate elections to American voters. Election security, both physical and cyber, is not a new concept for election officials nationwide. Since the implementation of electronic voting systems and statewide voter registration databases more than a decade ago, election officials have focused on ways to better secure the election process. However, coming out of the 2016 federal election, all of us must recognize that we are in a new operating environment—one that poses both new challenges and new opportunities to collaborate.

The reality is that in today's world, if you operate any kind of IT system, including election systems, you must realize you are a target of nation state actors from across the globe. These actors are persistent and creative, which makes the threat they pose very real and ever-changing. To address these threats and shore up voter confidence in our nation's election system, the EAC is focused on three key cybersecurity efforts to support election officials, including:

1. Improving the overall cyber-hygiene of election offices and systems. This includes a focus on training, awareness and best practices.
2. Working with the Department of Homeland Security and other federal partners to create formalized information- and intelligence-sharing channels to state and local election officials. This will ensure that election officials receive timely and actionable information as it becomes available.
3. Helping election officials better secure their election systems via best practices, improved voting system standards and guidance on maintaining aging voting equipment or purchasing new equipment.

Before I provide more details about those efforts, I'd like to offer a little background about the EAC and our mission. The EAC is a bipartisan independent federal agency created by The Help America Vote Act (HAVA). HAVA charges the EAC with helping election officials administer elections in a variety of ways. This includes but is not limited to:

- Developing Voluntary Voting System Guidelines (VVSG) for testing voting systems;
- Administering a voluntary federal voting system testing and certification program;
- Acting as a clearinghouse to the states for purchasing, implementing, testing, updating and maintaining voting systems; and

- Providing best practices to the states regarding every facet of the election process, including security for voting systems and polling places, election database support and contingency planning for elections in general.

Efforts to Provide Cybersecurity Support to State and Local Election Leaders

The EAC's efforts to support the 2016 election cycle began immediately following the appointment of the three new commissioners—after four years without a quorum of commissioners—in January 2015. Ever mindful that the EAC has been carrying out the basic provisions of HAVA since its inception, the commissioners focused on strengthening that support for election administrators nationwide with security-related tools and best practices for conducting elections. The commission focused on providing best practices related to the pre-election testing of voting systems, designing ballots, processing of absentee ballots, securing voter registration databases, securing voting systems, creating contingency plans, conducting post-election audits and other election-related activities.

Election officials' preparation for the November 2016 general election began earnestly in 2015. These efforts included robust preparation for securing the election process. Election officials manage voter registration databases that include externally facing web portals, general and specific-use computer servers, voting systems, connected components of election systems, tabulation machines and more. Election officials are aware that these systems need to be protected properly against cybersecurity threats, and election officials use many layers of security to do so.

The EAC's 2015 efforts to support election officials in their election security preparation began with providing best practices in the following areas:

- Procuring new voting equipment and systems;
- Managing existing technologies;
- Security protocols for voter registration databases;
- Pre-election testing procedures and practices;
- Protocols for securing voting equipment, including chain of custody and access control procedures;
- Updating and revising election procedures;
- Election contingency planning; and
- Post-election audit practices.

The EAC's clearinghouse collected best practices in each of these areas and used a variety of channels to distribute information to the states, territories and election jurisdictions to support election preparation efforts. The EAC held public events that allowed election administrators to share their best practices. We webcast and recorded multiple events and posted these events on our website for viewing by election administrators and the general public.

The EAC reemphasized three cybersecurity topics:

1. best practices for securing and maintaining election technology;
2. procuring secure voting technology; and
3. creating cybersecurity contingency plans.

The EAC clearinghouse topics that supported these educational efforts included security plans, voting technology maintenance and security plans, requests for proposals, and other procurement documents related to acquiring voting system components.

In addition to strengthening its clearinghouse function, the EAC furthered its testing and certification function by adopting an updated version of its Voluntary Voting System Guidelines (VVSG), which included improved security testing provisions, and continued its voting system quality monitoring program. The EAC accredited a new voting system testing laboratory (VSTL) and created a new structure for crafting the EAC's next iteration of the VVSG. This new structure reemphasizes cybersecurity and auditability as a driving force in the VVSG drafting and review processes.

In 2016, the EAC built on 2015's progress and added additional topics to the EAC clearinghouse as a part of the commission's "BeReady16" campaign. Among the new topics were election security preparedness, pre-election testing, managing election technology, e-pollbook requirements, and post-election audits and recounts. Last year focused on helping these officials improve their jurisdiction's equipment security and readiness for the 2016 election.

As part of this work, the EAC created the following original products to help election administrators protect their systems:

- Cybersecurity checklists that helped election administrators secure their voter registration and election night reporting systems;
- Guides on aging equipment, which included steps for ensuring security of these systems;
- Contingency planning guides for both physical and cyber threats; and
- "Tech Time" videos featuring some of the very best technology management practices and emphasizing how to best leverage technology at the local level.

Last summer, in the wake of reports about email system hacking and attacks on two state-level voter registration systems, the EAC's efforts turned toward working with the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) to help protect U.S. elections from specific cybersecurity threats identified by these agencies. Over the course of several months, the EAC met on multiple occasions with staff from DHS, the FBI and the White House to discuss specific and nonspecific threats, state and local election system security and protocols, and the dynamics of the election system and its 8,000-plus jurisdictions nationwide.

During this process, the EAC participated on and convened conference calls with federal officials, secretaries of state, federal law enforcement, state and local election officials, and

federal agency personnel. These discussions focused on topics such as security flashes from the FBI, critical infrastructure, the subtleties of the nation's election system, and the dynamics of successfully communicating information to every level of election officials responsible for running the nation's election system.

The EAC regularly provided DHS with perspective, information and data related to the election system. The EAC often helped DHS shape communications in a manner that would be useful to the states and local election officials.

During this critical time of preparation, the EAC communicated real-time DHS and FBI cybersecurity information to election officials around the country. This information included current data on cyber threats, tactics for protecting election systems against these threats, and the availability and value of DHS resources for protecting cyber-assets. The EAC acted as an intermediary that helped DHS best understand elections and election administrator feedback, as well as to strategically plan the most impactful ways to assist election administrators in their work to protect U.S. elections from cybersecurity threats. In addition, during this time, the commission remained focused on continued development of the next generation of the EAC's VVSG and the administration of its voting machine testing and certification program.

Looking Ahead

Recognizing that cybersecurity threats are persistent and adaptive, the next part of my testimony focuses on the road ahead. System operators must utilize a variety of layers of security processes, procedures and protocols to create a resilient environment that protects, detects and recovers from various cyber threats. Some of the current practices that election officials may utilize to improve the resilience of the process include:

- Logic and accuracy testing, a pre-election test of the functionality of the election systems that will be used to run that specific election;
- Access control protocols, a procedure that allows access to election systems to only those who need access and limits that access to only those functions the individual needs;
- Chain of custody procedures, a way of tracking who had access to systems and when they had access;
- Post-election audits, a post-election tool used to detect the presence of any anomalies that could have been present in the system during an election;
- Air gapping, a method by which voting machines are isolated from the internet by design;
- Hash analysis, a tool that audits the code present on voting and tabulation machines for anomalies and differences between the expected state of the code and the current state of the code at the time of the hash;
- Regular IT system maintenance, including IP access management for public-facing portals, a tool that limits digital access to publicly facing access points;
- Physical security measures, including the use of specific tamper-evident seals;

- Public tests of equipment tabulation to verify results tabulated against expected outcomes; and
- Continuity of operation planning that ensures the integrity and operation of the election in the event that critical systems are unavailable or unusable.

These tools and practices are designed to prevent and detect threats, maintain the integrity of the process and instill voter confidence. However, even with these layers of security in place there is no such thing as a completely secure system or process. Given the new threat environment election systems now operate in, it is incumbent on all of us to review these practices and identify new ones in order to improve the overall resilience of the election process.

The EAC plans to continue working with election officials to improve the security of election systems in order to prevent and detect interference, foreign or domestic, in U.S. elections. This work will rely on continuing our collaboration with federal partners, such as DHS and the FBI, to provide current, up-to-date information regarding cyber threats and access to available security assets to election officials around the country.

The EAC is working with DHS and state and local election officials to understand and implement the critical infrastructure designation of elections that was declared by the former Secretary of DHS in January. The goal of this effort is to ensure that state and local election officials across the country have access to timely actionable information and intelligence via regular information sharing among the federal, state and local level.

The EAC is continuing to produce best practices, including checklists and products that promote cybersecurity for the benefit of the elections industry. To this end, the EAC has begun expanding on the secure voting system procurement help it is already providing to election officials, as well as developing cyber incident response planning tools for election officials. As election officials currently evaluate election technology purchasing decisions, the EAC is providing RFP development guidance, providing cybersecurity documents and plans, and creating forums to bring cybersecurity experts from the private sector and academia and election officials together, so that election officials will have the best information moving forward.

More and more election officials recognize that they are managers of complex IT systems. To support them in this role, the EAC is offering hands-on election-related IT training for state and local election officials. This training focuses on the mindset, knowledge base and resources needed by election officials to manage their disparate and dependent systems.

The EAC is also continuing to administer its Testing and Certification program, which currently includes working on a new version of the EAC's VVSG so that voting machines can continue to be tested to the most up-to-date standards possible. This VVSG development effort is utilizing a public working group structure to ensure input from subject matter experts from a variety of areas, including cybersecurity. The new standards should be complete in early 2018.

Conclusion

The election process is in a new operating environment where nation state actors are attempting to meddle and undermine confidence in our democratic process. It is incumbent on all levels and branches of government to recognize this new threat environment and work together to adapt and improve. The EAC looks forward to engaging the best and brightest in elections, cybersecurity and technology to produce meaningful guidance on better securing the election process.

We will leverage cybersecurity resources made available to us to share best practices, tools and resources with election officials to improve the baseline security of election systems. We will also reassess the risk environment for election systems and work with election administrators, election system vendors, the National Institute of Standards and Technology, DHS and the FBI to provide current and actionable steps election officials can take to mitigate those risks.

As we work to finalize the next version of standards to test voting systems, we will continue to engage the cybersecurity community, as well as experts in accessibility, usability and election administration to ensure voting systems are tested and certified to the highest standards possible without undercutting each American's ability to cast their ballot privately and independently.

And while we recognize the important role the EAC plays in helping state and local election officials protect their systems, these election officials remain the frontline defenders in our democracy. Here are five things they can do right now:

1. Ensure that all aspects of voting systems (voting system, election management systems, ballot creation, etc) are properly air gapped from the internet. This includes using clean media to load ballots and provide results on election night.
2. Audit systems, data, processes and procedures for pre-election testing, post-election auditing, chain-of-command, access controls and physical security to ensure they are up to date and follow current practices;
3. Ensure proper data security protocols and processes are being followed;
4. Develop a comprehensive incident response and recovery plan; and
5. Take advantage of all available resources including those from DHS, state government, academia and the private sector.

The diligent efforts of those involved in administering the 2016 election maintained the integrity of that election, but the next time that may not be enough. We need less finger-pointing and more candid and open conversations among election administrators, federal agencies, private industry, and cyber and national security experts. Elections are more secure when we fully coordinate efforts to address existing threats, share cutting-edge strategies to address them, improve information sharing, and help jurisdictions best protect systems when budgets are tight. This type of coordinated response from all levels

of government and the private sector will ensure the continued accessibility, accuracy and integrity of our election process.