Testimony of Matthew Masterson
Commissioner, U.S. Election Assistance Commission
Committee on Elections and Redistricting
California State Assembly
March 7, 2017

Good morning Mr. Chairman and distinguished members of the committee. Thank you for the opportunity to offer testimony this morning.

By now, there can be no doubt about the real and sophisticated threats against our nation's election systems, including disinformation campaigns via social media and other outlets, as well as cyber threats against our election infrastructure. The 2016 Federal Elections demonstrated 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 are a target of nation state actors from across the globe and others seeking to disrupt democracy.

These actors are persistent, adaptable, creative, well-resourced, and by all accounts, they will be back in 2018, 2020 and beyond. Their goal is to undermine Americans' confidence in the security and integrity of their democracy. Our goal must be to stop them, and election officials from across the nation are laser focused on that. They have risen to the challenge of improving election security, working each day to strengthen their ability to prevent, detect and recover from potential attacks.

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.

Today, jurisdictions use a multi-layered approach to ensure the integrity of elections. In order to protect voter's personal information, for example, only authorized personnel have access to the voter registration database. Database traffic is monitored for irregularities. Every time a record is accessed or changed, details from that session are logged, and routine offline backups help ensure all data can be restored if any unexpected modifications are made.

In addition, all voting equipment is publicly tested prior to the election to ensure the systems are ready to run that election. Post-election audits are becoming the norm and election officials across the country are looking to implement more efficient and more effective audits to provide voters with greater confidence in the outcome of the election.

Chain of custody procedures associated with transporting and securing ballots are followed throughout the election process. Voting equipment is sealed and monitored throughout the election process by election officials and approved observers. Ballots and other sensitive election materials are kept in safes and other secure areas maintained by a clerk's office, which is often within a secure facility. These are just a few of the measures in place to secure our nation's election systems.

While election officials are at the heart of these efforts, we at the U.S. Election Assistance Commission have long helped them in their work to administer elections.

For those not familiar with the U.S. Election Assistance Commission, or the EAC, 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, or 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, or VVSG, for testing voting systems;
- Administering a voluntary federal voting system testing and certification program;
- Acting as a clearinghouse for states 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.

Ahead of the 2016 elections, our work to advise election officials on best practices took on a new dimension. In the wake of reports about 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. 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 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 also 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 timely and actionable information from DHS and FBI 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 better understand elections and election administrator feedback and provided guidance to help strategically plan the most impactful ways to assist election administrators in protecting U.S. elections from cybersecurity threats. In addition,

during this time, the commission remained focused on developing the next generation of the VVSG and administering our voting machine testing and certification program.

This relationship was formalized in January of last year when DHS designated elections as part of the nation's critical infrastructure. Since then, the EAC has worked to ensure state and local election officials understand how the designation will impact their election offices, polling places, and the voters they serve. The Commission also played an instrumental role in ensuring that state and local officials have a voice at the table as DHS works to establish the structure that will support election systems.

The EAC led the effort to convene an Election Infrastructure Subsector Working Group (EISWG) consisting of state and local election officials. In collaboration with DHS, the EAC worked to establish the Elections Government Sector Coordinating Council, or GCC, about whose work my colleague Neal Kelley will speak about later today. The GCC will inform how the DHS works with state and local jurisdictions to implement the designation of elections systems as part of the nation's critical infrastructure and is an important milestone in the effort to establish a critical infrastructure subsector that can facilitate timely information sharing and coordination between election officials and the federal government on issues such as cyber and physical security.

The EAC and DHS continue to direct the development of the Critical Infrastructure subsector while the GCC works to establish information sharing protocols, complete a draft sector specific plan and participate in the Multistate Information Sharing Analysis Center, or MS-ISAC, pilot program. The MS-ISAC is the entity that provides information sharing capabilities to state and local owners and operators of election systems so they can better secure their systems against cyber threats. These capabilities will include threat-related notifications; assessments of news relevant to targeted stakeholders; cyber security assessment services; a 24/7 operations center with access to cybersecurity subject matter experts; timely sharing of actionable information and real-time monitoring for network activity by malicious actors.

This on its own however is not enough. Election officials around the country are being tasked with combatting sophisticated cyber threats using technology that is by and large, older than the first-generation iPhone. Election administrators' crucial work of strengthening the resilience of election systems is made more difficult by the dangerously low funding currently allocated to update systems and develop additional security expertise. Election officials must have access to resources, monetary and otherwise, that help them secure the process. If we don't invest in election administration and integrity, election officials will continually have to make risk-based budget decisions in an increasingly difficult operating environment.

In order funnel more resources to their efforts, the EAC has worked to go beyond the federal government and begin forming more public/private partnerships. In addition to our work with the FBI and DHS, the EAC has also worked with NIST, NASS, NASED, NGA, Election Center and iGo, as well as private sector entities such as Harvard's Belfer Center, the Center for Internet Security (CIS), the Center for Democracy and Technology (CDT), Google, CloudFlare and others. The purpose of these partnerships is to improve awareness among the nation's election officials about the nature of this threat and bolster the overall resilience of the election process.

In order to protect the security and integrity of our elections, the nation must be prepared to deploy coordinated responses to coordinated attacks should they occur in the 2018 midterm elections and beyond. Election officials need to draw on the expertise of new partners in the federal government and private industry, academia, even patriotic and so-called "white hat" hackers if we are to combat sophisticated attacks from nation-state actors.

Working across sectors and industries bolsters the vast web of physical and online security, election personnel and the different technologies and processes in each jurisdiction that make up a secure election system. If necessity is the mother of invention, we have clearly seen that this year with the host of innovative new election security approaches and resources generated, such as tabletop playbooks, customized information technology trainings, and best practices handbooks.

Even so, more resources and services are needed ahead of the 2018 midterm elections and beyond. There are however, a number of things I advise all election officials to do to strengthen the ability of election systems to prevent, detect and recover from potential attacks.

Specifically, here are five things they can do right now:

1. Ensure that all aspects of voting systems (such as 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. If a vendor performs these tasks for you, educate yourself about the security protections they have in place and hold them accountable.
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. Assess your data risks and secure systems appropriately. Regularly back up the data and test your backups to make sure it is available and functional in the case of an incident.
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. Protecting election systems against advanced sophisticated threats cannot be done alone. The good news is that because of all the attention that has been paid to election systems since 2016, there are a number of resources available that election officials have never had before.

As the election community works to confront emerging threats, the EAC stands ready to provide resources and support to state and local election officials who are on the front lines of defense. We continue to produce best practices, including checklists and products that promote cybersecurity for the benefit of the elections community. To this end, the EAC has begun expanding on the secure voting system procurement help it already provides to election officials, as well as developing cyber incident response planning tools for election officials.

As election officials evaluate election technology purchasing decisions, the EAC provides request-for-proposals development guidance, cybersecurity documents and plans, and 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 offers 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 also continues to test voting machines against the most up-to-date standards possible through its Testing and Certification program. The most recent version of the VVSG (VVSG 2.0) were adopted by the EAC's Technical Guidelines Development Committee (TGDC) in September. The new voting system testing guidelines are expected to be released in mid-2018. These guidelines are written to encourage innovation and competition and, once released, will be the most comprehensive set of standards against which voting systems can be tested in the United States.

The diligent efforts of those involved in administering the 2016 election maintained the integrity of that election, but we can – and should – always seek to do more. Voters want and expect a coordinated whole-of-nation response to these threats against our democracy so they can head to the polls (or ballot drop box) with confidence.

And to those voters, I say get involved! Officials run elections at the local level so all voters can engage in the process directly. Become a poll worker, observe pre-election testing and post-election auditing, ask questions and engage your local election officials. They want to hear from you.

We need less finger-pointing and more candid and open conversations among election administrators, federal agencies, private industry, cyber and national security experts and legislators. We need a plan to invest in election infrastructure on a regular basis. These threats aren't going away and regular funding and resources to support local election officials are needed to help protect the process. 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.