U.S. ELECTION ASSISTANCE COMMISSION
1335 East West Highway – Suite 4300
Silver Spring, MD 20910

HAND DELIVERY

March 31, 2017

Senator Amy Klobuchar
United States Senator
Washington, DC 20510

Dear Senator Klobuchar,

Thank you for the February 23, 2017, correspondence requesting information on the U.S. Election Assistance Commission's (EAC) activities and efforts in cybersecurity support for the November 2016 Presidential General Election.

As indicated in the correspondence, "sophisticated cybercriminals will continue to target our election systems and we must ensure that our state and local election administrators have the resources they need to make critical cybersecurity upgrades." Election security, both physical and cyber, is and has been a priority for election officials nationwide since the implementation of electronic voting systems, and the EAC has supported their efforts since its inception.

As you know, the Help America Vote Act (HAVA) charges the EAC with helping election officials administer elections. 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.

The EAC's efforts to support the 2016 election cycle began immediately following the appointment of the three new Commissioners in January 2015. Ever mindful that the EAC has been carrying out the basic provisions of HAVA from its inception, the Commissioners focused on supporting election administrators nationwide with 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 related election activities.

In answering the questions set forth in your correspondence, we have highlighted a number of 2015 activities the EAC conducted in anticipation of election officials' priorities in administering the 2016 general election and 2016 activities focused on supporting their work during a presidential election cycle, including our security activities in connection with the Department of Homeland Security, the Federal Bureau of Investigation, and other federal entities.

1) What actions did the EAC take before the November 2016 election to protect U.S. elections from threats to cybersecurity?

Election officials' preparation for the November 2016 general election began earnestly in 2015. These efforts included robust preparation for securing the election process. Cybersecurity preparation comes naturally to election administrators because elections already involve a considerable number of information technology (IT) components. Election officials manage voter registration databases that include externally facing web-portals, general- and specific-use computer servers, air-gapped 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 through both election management and system design, 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 the above areas and distributed information in a variety of ways 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) cybersecurity contingency planning. 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, adopted an updated version of its VVSG that 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 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 & Recounts. 2016 focused on helping these officials ensure their jurisdiction's equipment was secure and ready for the 2016 election.

As part of our 2016 efforts focused on cybersecurity threats, 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.

In the wake of reports about email system hacking and attempted attacks on two state-level voter registration systems in summer 2016, 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, state and local election officials, federal law enforcement, 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 also acted as an intermediary that helped DHS best understand elections, election administrator feedback, and to strategically plan the most impactful ways to assist election administrators in their work to protect U.S. elections from threats to cybersecurity. During this time, the Commission also 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.

2) To your knowledge, please describe the full extent of foreign interference and hacking that occurred in any national, state, or local election system-including voter registration databases, and voting infrastructure-during the November 2016 election.

The EAC is aware that on January 6, 2017, the Office of the Director of National Intelligence (ODNI) released an Intelligence Community Assessment (ICA) titled *Assessing Russian Activities and Intentions in Recent US Elections*, and the EAC has appraised itself of the contents of the unclassified version of this report.

The EAC Commissioners and staff do not possess the necessary security clearance to receive classified intelligence and are not in a position to assess the credibility or veracity of the information in the ODNI report. The EAC defers to the intelligence community for more specific information regarding instances of cyberattacks that may have occurred during the 2016 election cycle. Our resources are not focused on identifying foreign intelligence activities. We note, however, that the type of threats identified in the ODNI report are same types of threats discussed in the DHS and FBI materials that the EAC shared with state and local election officials throughout the 2016 election cycle.

The EAC's guidance documents, hands-on assistance, and combined work with DHS and other members of the intelligence community are all assets that can help identify and prevent these types of threats in the future. The EAC has continued to work with DHS and NIST after the 2016 election, and it looks forward to playing a key role in helping state and local election officials address their evolving cybersecurity needs.

3) In your opinion, are current state and local election systems appropriately prepared to respond to and resolve cybersecurity threats to U.S. elections?

Generally speaking, yes. However, the complexity of the U.S. election system makes answering a question about the entire system with a single answer difficult. The U.S. election system is the aggregate of more than 8,000 individually operating and often autonomous election jurisdictions. These jurisdictions vary in size, number of voters, and administrative resources. They also have varied practices, policies, laws, regulations, and procedures. It is this diverse and decentralized system that the FBI and the DHS described as a security asset.

Cybersecurity threats are ever-evolving. Election systems and their security protocols are designed and operated in ways that detect and prevent interference. Still, election officials could benefit from continued guidance related to emerging threats and best practices in addressing incidents that may occur. Additionally, the level of cybersecurity for systems varies from jurisdiction-to-jurisdiction because the amount of resources that election officials and administrators have at their disposal to protect their systems also varies. Dedicated, honorable and professional state and local election officials manage election systems across the country. They pride themselves in the security and integrity of the elections they conduct. Our experience and observation informs our belief that they take every precaution available to secure their systems, which includes utilizing tools such as:

- Logic and Accuracy Testing, a pre-election investigation of the functionality of a voting machine;
- 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 have 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 completely removed 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 publically 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 security threats, maintain the integrity of the process and instill voter confidence.

4) In your opinion, are state and local election systems currently able to identify instances of foreign interferences in U.S. elections through tools like post-election audits?

As described, election officials possess the capabilities necessary to identify anomalies in the voting process. The goal of these processes is to prevent and detect problems, but these processes are not necessarily designed to identify the actual interfering party. A local election system may include an internet-facing voter registration system, optical or digital scan voting units, electronic voting machines, an electronic ballot marking device, and an election management system that programs the election for the voting machines and also serves to consolidate all vote totals for display on election night. In addition, there may also be an election night reporting tool that displays the election night totals to the public. Election officials use many processes and tools, including pre-election testing, physical security, logical security, access controls, chain of custody procedures, hash audits, regular IT management reviews and analysis, post-election audits, and other layers of security to protect these systems.

A post-election audit of these components would indicate if there was a discrepancy in the vote count, but it would not necessarily lead an auditor to conclude that interference had occurred in the election. An investigation into a vote total discrepancy between the audited components may lead to a conclusion that the system malfunctioned or a discovery that there may have been some type of interference. Either way, that information may not necessarily lead to the conclusion that there was foreign involvement.

For internet-connected systems, including online voter registration systems, election officials use offline and redundant recordkeeping and regular IT maintenance to detect anomalies. For online voter registration systems, election officials keep a redundant copy of their voter registration lists on a server that is not the same server as where the online voter registration database is kept. Election officials then use this offline and redundant list to check the list on the online voter registration system for discrepancies, which may indicate errors. For other internet-connected systems, such as public facing websites, election officials use tactics such as IP address access management to detect anomalies.

Public L&A testing is used by local election officials to audit the functionality of a voting machine before an election is conducted to detect anomalies. It examines whether a particular machine is correctly and accurately receiving and recording votes. L&A testing may identify the inaccurate recording of votes and other functionality issues on a machine, but most often it demonstrates that the machine being tested is indeed functioning properly.

5) What foreign cybersecurity threats are we most likely to encounter in future elections?

Cybersecurity threats are adaptive and persistent. They change in form and function with time and technology. As such, it is difficult to predict specific cybersecurity threats U.S. elections are likely to encounter in the future. However, it is likely that the components of U.S. elections that are connected to the internet are most likely to face cybersecurity threats. This does not include many components of election systems, such as voting machines that are air gapped and are therefore not connected to the internet. Still, states have public facing websites that educate voters and other public facing portals that are not connected to voting machines. These are more likely to encounter threats in future elections.

In the face of these threats, the EAC is well positioned to continue to effectively and efficiently communicate threat information as provided by the intelligence community including DHS and the FBI and information concerning solutions to these threats to the election officials and administrators who need this information to secure the elections they administer. EAC will continue its work developing and disseminating cybersecurity best practices like the checklists and common cyber practices we provided in 2016 to state and local election officials.

6) What are the EAC's plans moving forward to prevent foreign interferences in U.S. Elections?

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 the 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 the critical infrastructure designation of elections that was recently declared by the former Secretary of DHS. We are discussing the possibility of the EAC serving as a Co-Sector Specific Agency (Co-SSA) over the elections critical infrastructure. Should the designation stand, the EAC and DHS agree that an arrangement in which the EAC serves in an official capacity throughout the development of a sector-specific cyber plan for elections would help ensure that election officials' interests are represented throughout the process.

The EAC will also increase the production of 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 voting technology purchasing decisions, the EAC is providing RFP development guidance, providing cybersecurity documents and plans, and creating forums to bring cybersecurity experts and election officials together, so that election officials will have the best information moving forward.

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 securely 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 2018.

7) Does the EAC have recommendations to Congress and the Administration on appropriate actions to defend our U.S. election system from foreign interference and respond to threats?

The EAC recommends that Congress and the Administration ensure that election officials and administrators have the resources they need to protect their elections. Cybersecurity threats are adaptive and persistent. Resources that Congress and the Administration can provide come in three forms: (1) financial resources; (2) information; and (3) representation.

Financial resources

Both states and the EAC could do more to protect U.S. elections if provided the opportunity. A lack of financial resources often prevents this work from occurring. State and local officials consistently request funding to buy new voting machines, which are one of the most critical cyber-assets of U.S. elections. Most jurisdictions are using voting machines that the jurisdictions bought more than a decade ago with HAVA funds provided by Congress and distributed by the EAC.

More robust machines are available, but most jurisdictions lack the resources necessary to purchase them. In fact, the EAC has certified or modified the certification of thirty-seven voting systems, and in 2015, the EAC approved and implemented a new level of certification, VVSG1.1. If jurisdictions were allotted resources from state and local governments or Congress, should it so decide, to purchase newer machines certified to newer standards, then the cybersecurity defenses of U.S. elections would improve.

Voting machines are not the only assets that need to be protected. Voter registration databases and voter education websites, such as the website that informs voters of their polling location and voter requirements, often contain an internet-facing portal. In 2016, both Illinois and Arizona reported breaches of their voter registration databases. The motivations for such breaches vary and may include poaching personal information of voters for the purposes of identity theft, obtaining data that can be sold to other criminal

actors, or for the purpose of damaging the election system, but often even more impactful is the damage that these breaches have on public confidence of elections.

Additionally, resources that help smaller jurisdictions operate with methods, tactics, and knowledge of the same standard as large jurisdictions improve the cybersecurity of U.S. elections. The EAC, through its clearinghouse function, works to help small jurisdictions learn from all jurisdictions and implement new practices and tactics even when smaller jurisdictions do not have the time or resources to research and test new tactics and tools on their own. Still, increased resources in this area would improve the cybersecurity of U.S. elections.

Information

Current and accurate information is critical to cybersecurity. The disaggregated nature of U.S. elections makes active and consistent information sharing a necessity. Information that the federal government has on current and potential cyber threats to U.S. elections and the many systems supporting U.S. elections should be shared with states quickly, consistently, and in a form that allows the states to effectively use it. The EAC has successfully served as an intermediary between state and local officials and our federal partners. Throughout the 2016 election cycle the EAC received information from DHS and the FBI and shared it with state and local officials from all fifty states. Perhaps more importantly, the EAC also shared information from local and state officials with our federal partners, allowing those election officials to stay focused on the task at hand, administering a presidential election. As threats grow, the need for this support will likely also expand, and the Commission stands ready to efficiently and effectively share this information with our stakeholders.

Representation

As the federal government continues to provide resources to election officials and election systems through its various agencies (EAC, DHS, FBI, DOJ, DOD, USPS, HHS, GSA, etc.), it should do so in a manner that helps election officials, not hinders them. The only way to do this effectively and efficiently is to have an intermediary that understands the complex election administration process and that will directly support the approximately 8,000 election jurisdictions across the country. That is why the EAC recommends that DHS leverage the EAC as a Co-SSA under DHS's Critical Infrastructure System.

Co-SSAs help DHS build the plans that structure information sharing in critical infrastructure sectors. These plans dictate how information is shared and how resources are provided. The EAC is dedicated to helping election officials secure their elections. So, if elections are critical infrastructure, the EAC seems the natural choice for ensuring that election officials have representation in the critical infrastructure sector's management and to ensure that they receive the resources and information they need in the best way possible.

Other components of the federal government can leverage the EAC to help election administrators. The EAC works with the FBI, DHS, DOJ, DOD, HHS and USPS to assist

election officials. The Commission is confident that these types of partnerships have helped election officials, voters, and other election stakeholders.

Lastly, the EAC sees value in its continued testimony before Congress concerning election administration issues. The EAC welcomes communicating its research, knowledge, and expertise of election administration to members of Congress as they form policy and write laws concerning U.S. elections. The Commission will continue striving to provide Congress with the best possible information it needs in its service to the people.

Conclusion

In the face of dire warnings, heightened scrutiny and unprecedented threats election officials across the U.S administered a presidential election that was accurate, accessible and had integrity. We are thankful for their diligence, professionalism and patriotism.

In September 2016, then Chairman Thomas Hicks testified on the security of U.S. elections before the Subcommittee on Information Technology of the House of Representatives' Committee on Oversight and Government Reform. He testified that U.S. elections were secure. The EAC continues to stand by this assertion and by Commissioner Hicks's testimony, which is attached.

The EAC and election officials will continue to work to strengthen election security and protect the integrity of our nation's vote. We will adapt to the challenges that await U.S. elections in the future. We will also not lose sight of one of the greatest values of secure elections, the confidence that they inspire in voters. If public confidence is eroded, so is the security and value of our elections. As our country moves forward, our united efforts to safeguard against threats must include a concerted effort to reinforce and strengthen public confidence in America's elections.

Sincerely,

Matthew V. Masterson
Chairman

Thomas Hicks
Acting Vice Chairman

Christy A. McCormick
Commissioner