NASS
National Association of Secretaries of State

October 9, 2017

The Honorable Richard Burr
Chairman of the U.S. Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

The Honorable Mark Warner
Vice Chairman of the U.S. Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

Re: Proactive Election Cybersecurity Initiatives by Secretaries of State

Dear Senators Burr and Warner:

The members of the National Association of Secretaries of State (NASS) would like to provide you with a more complete understanding of the work done by state election officials to protect their election systems from future cyberattacks. While we know the work of your Committee is focused on activity around the 2016 election, the focus of the Secretaries is on the next election.

Ensuring the integrity of the voting process is central to the role of the chief state election official. This role includes cyber preparedness and contingency planning, as well as administrative and technical support for local election officials. Secretaries of State are actively engaged in bolstering cybersecurity and resilience levels for future elections. They are focused on key digital and human components of their state systems: voter registration databases, election management systems, election night reporting systems, electronic voting machines, and cyber training for state and local election staff.

They are committed to voluntarily working with their federal, state and local partners, including the U.S. Election Assistance Commission (EAC) and the U.S. Department of Homeland Security (DHS) to receive input on threats and share information on risk assessment and threat mitigation in our elections. We are not naïve about the likelihood of future cyberattacks against digital elements of election systems. All 50 states consider themselves a target and act and react accordingly.

Later this week, state and local election officials will convene with these federal partners to establish the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC). We have been assured that this is the first step in establishing better communications protocols for all stakeholders and holds the potential for establishing an election-specific Information Sharing and Analysis Center (ISAC).

While DHS has struggled to provide the necessary resources to hold the convening this week, the EAC generously stepped forward to enable the gathering. It is imperative that DHS find sufficient resources to hold the EIS-GCC meetings and provide technical resources and network monitoring services for those state and local governments who request them. It is not clear that the current DHS funding is sufficient to accomplish this. This is something we would ask Congress to address.

The decentralization of our election system is an obvious benefit to protecting against wholesale disruptions to our elections, however decentralization has another benefit: 50 state laboratories, with skilled IT and election professionals tackling cybersecurity challenges. Some examples of the innovative and highly collaborative work being done in the states include:

- **Establishing Cybersecurity Task Forces**. Many Secretaries and Governors have established state cybersecurity task forces, which provide the opportunity to share information with other state and local officials on overall cybersecurity efforts and those specific to elections.

- **Obtaining Security Clearances for Secretaries of State/Chief State Election Officials and Their Designated Staff**. In order to have priority access to timely threat information, chief state election officials have begun the security clearance process through DHS. Once the clearances have been finalized for the chief state election official, a second clearance process will begin for key staff to enable action by state IT offices regarding any classified information.

- **Working with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and State Fusion Centers**. State and local governments are establishing working relationships with MS-ISAC and their State Fusion Centers to enable better threat information sharing. As mentioned earlier, MS-ISAC is working with several states over the next few months to pilot an elections-specific ISAC to enable better, more targeted information for election officials.

- **Leveraging National Guard Cybersecurity Expertise**. In at least one state, an Air National Guard cybersecurity specialist is embedded in the state's Fusion Center for the purpose of monitoring the election space. Other states work with the National Guard on exercises to improve their cyber posture.

- **Updating Security Tools and Procedures**. While in many cases, cyber security tools and practice were already in place, new tools are constantly added. These include the use of dual or multifactor authentication; strengthened data encryption; improved data classification to monitor different types of threats; enhanced tracking of worker access to data; use of data access cards; statistical analysis of data patterns, including artificial intelligence analysis of logs; launching Google Shield; and reviewing procedures to minimize potential unauthorized physical access to machines.

- **Creating Incident Response Plans**. States have Emergency Preparedness Plans for Elections, and they are now including cyber incident responses into their preparedness plans.

- **Cyber Cross-Training and Audits for County Elections Staff**. Many states conduct annual conferences for their local election officials. Cybersecurity presentations and training are frequent agenda items at these conferences. Other states conduct yearly tests for county staff that interact with state voter registration systems and are required to adhere to state security standards.

- **Providing Free, Updated Software to Counties**. Some states are able to provide cyber tools to local officials such as malware detection. They are also able to monitor activity in order to assist in reacting and responding to events quickly.

These examples demonstrate the diverse cybersecurity initiatives being developed by Secretaries of State across the nation.

Additionally, Secretaries of State are working in collaboration via the National Association of Secretaries of State (NASS) Election Security Task Force, created for sharing resources, best practices and technical advice between states. In addition to the NASS Task Force, there are a number of organizations that have stepped up to create tools for state and local governments including Harvard's Belfer Center, the Democracy Fund and the Center for Democracy and Technology.

We appreciate the focus your committee is bringing to the vital issue of elections cybersecurity. There is no doubt that more can – and will – be done to bolster resources, security protocols and technical support for state and local election officials heading into future elections. The lesson from 2016 is that we are the frontline in securing election systems from very real threats that exist in the digital age.

Sincerely,

Hon. Connie Lawson, Indiana Secretary of State
NASS President