Statement from the

Honorable Jim Condos

Vermont Secretary of State

President-elect, National Association of Secretaries of State

Member, Election Infrastructure Government Coordinating Council (EIS-GCC)

Before the U.S. Senate Select Committee on Intelligence

Open Hearing: Election Security

March 21, 2018
Washington, D.C.

National Association of Secretaries of State
444 North Capitol Street, NW – Suite 401
Washington, D.C. 20001
202-624-3525 Phone/202-624-3527 Fax
www.nass.org

Hon. Jim Condos, Vermont Secretary of State
Statement Before the U.S. Senate Select
Committee on Intelligence
March 21, 2018 | Washington, D.C.

NASS
National Association
of Secretaries of State

Thank you for the chance to appear before you today to represent the nation's Secretaries of State, 40 of whom serve as the chief state election official in their respective states.

My name is Jim Condos, and I am the Vermont Secretary of State. I am also president-elect of the nonpartisan National Association of Secretaries of State (NASS), and a member of the Department of Homeland Security's (DHS) new Election Infrastructure Government Coordinating Council (EIS-GCC).

NASS President Connie Lawson of Indiana was not able to be here today, but I want to acknowledge her outstanding leadership. Our organization is comprised of members with strong and often differing opinions, but when we speak for NASS, we speak with one voice.

It is an honor to be here with my fellow panelists to discuss what states are doing to secure state and locally-run elections from cyber threats. We are in the 2018 election cycle with November's General Election only eight months away. I want to assure you – and all Americans – that election officials across the U.S. are taking cybersecurity very seriously. While it is important to ask what really happened in the 2016 cycle and learn from it, we believe it is even more important for us to be discussing what lies just ahead.

As you know, DHS reported to this committee in June 2017 that 21 states were targeted during the 2016 election cycle. The 21 states were then notified by DHS in September 2017. Of the 21 states, NASS is aware of only one actual breach – a breach of a state voter registration system. **No votes were changed.** It is also important to note that **all 50 states consider their election systems a target**. Secretaries of State across the nation are diligently working each day to safeguard the elections process with their own IT teams, private sector security companies, the federal government, and other partner organizations.

I. CRITICAL INFRASTRUCTURE DESIGNATION AND STATE AND LOCAL ELECTION CYBERSECURITY EFFORTS

When former DHS Secretary Jeh Johnson announced the "critical infrastructure" designation for election systems in January 2017, our members raised many questions and expressed serious concerns about the potential federal overreach into the administration of elections – a state and local government responsibility.

While NASS members remain concerned with potential federal overreach, we understand that the "critical infrastructure" designation is in place. Therefore, we are focused on improving communication between the states and with DHS to achieve our shared goal of election security. We believe that federal agencies have more information and resources to share and help mitigate cyber threats.

Under the leadership of DHS Secretary Kirstjen Nielsen, we are working together to correct incident notification procedures, receive security clearances, and utilize new federal resources available to the states. NASS is committed to facilitating this relationship.

State and local autonomy over elections is our best asset against cyberattacks. Our decentralized, low-connectivity electoral process is inherently designed to withstand and deter threats.

Ensuring the integrity of the voting process is central to our role as chief elections officials. We work every day to improve our cyber preparedness and contingency planning, and to provide administrative and technical support for local election officials. The processes and procedures surrounding our election systems incorporate both cybersecurity and physical security. For example, while cyber defenses are employed for digital systems, secure storage facilities for equipment such as voting machines and electronic poll books are vitally important as well.

States use many resources available to them to bolster cybersecurity. Some utilize resources provided by DHS, such as cyber-hygiene scans, risk and vulnerability assessments, penetration testing and consulting. Others use the private sector security companies for these services; and still others partner with colleges and universities.

States have and are implementing cybersecurity best practices developed for their own state systems, but have also taken advantage of broader cyber best practices and incident response plans developed by civic-minded organizations like Harvard's Belfer Center, the Center for Internet Security, and numerous federal agencies. These tools include checklists for cyber practices, table top exercises and sample incident response plans. These organizations also convene forums throughout the year for state officials to share experiences and discuss challenges.

In Vermont we began a thorough review of our cyber posture in 2013, when we issued an RFP for both physical and cybersecurity risk assessments which was completed in 2014. In the fall of 2015, we completed implementation of a new election management platform providing for our election night reporting, voter registration, overseas and military voting, etc. Because this system was new, it included built-in cyber security risk measures.

Some of the acknowledged "best practices" that Vermont uses include:

- Paper ballots
- Post-election audits
- No internet (Wi-Fi or hard-wire) connection of our vote tabulators
- Daily backup of our voter registration database
- Same day voter registration
- Automatic voter registration
- Daily monitoring of traffic to our site
- Blacklisting of known problem or suspected IP addresses
- Additional penetration testing

We have no less than three firewalls between the outside internet and our cyber systems as well as:

- Joining the Multi-State – Information Sharing Analysis Center (MS-ISAC),
- Receiving weekly DHS cyber-hygiene scans,
- Having met with both DHS and FBI Contacts

I would be glad to elaborate during the question and answer portion of this hearing or anytime in the future.

As a result of the "critical infrastructure" designation, an Election Infrastructure Government Coordinating Council (EIS-GCC) was established to improve communications between state and local officials and the federal government and to share resources. The EIS-GCC is comprised of 29 members, of which 24 are state and local election officials. **This is the first group of its kind** and helps us stay on the same page and share vital information. Through the EIS-GCC, a number of states have participated in a pilot program to share election-specific threat indicators. Additionally, a full Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) will be operational by May 2018. States will have the option to put monitors on their election-networks to track traffic, detect anomalies and share with other states.

Secretaries and their staffs are also working with their legislatures to try and secure more funding for improved cybersecurity, new voting machines and to strengthen existing election systems. These efforts have become more challenging as election officials work to counter cybersecurity threats to election systems.

II. FEDERAL FUNDS TO FURTHER AID STATES IN BOLSTERING ELECTION CYBERSECURITY

Presuming that the members of this committee want to know how Congress can assist state and local officials in ensuring the integrity of our election systems, my colleagues and I have a prepared "ask."
One of the most critical resources that Congress could provide to the states is the remaining $396 million in Help America Vote Act of 2002 (HAVA) funds.

NASS and its members have repeatedly called on Congress to appropriate these previously-approved funds so that states could conduct the necessary work to implement additional cybersecurity protections and begin to purchase new voting systems. Every state in the country would benefit. Timing is absolutely critical as we are only eight months from the November General Election.

HAVA was the first piece of federal legislation to provide funding for election administration improvements, and states used the opportunity to enhance the security, accessibility, accuracy and reliability of election systems. Implementation of HAVA was a success, and it helped improve the voting experience for all Americans over the last 15 years.

Our existing election infrastructure is aging and election officials are increasingly required to modernize and innovate in order to ensure that elections continue to be administered in a secure and efficient manner. Meeting the ongoing demands for updated equipment and ongoing cybersecurity upgrades requires funding that the states simply do not have within their own budgets.

Providing the remaining funding under HAVA will not solve all of the challenges election officials face, but it will help states enhance the efficiency and security of elections, including the purchase of new voting systems, the implementation of additional cybersecurity tools, and the hiring of additional IT professionals.

Election officials make every effort to ensure elections are administered in a secure manner, whether it is protecting voter registration data from cybersecurity threats or making sure that the votes cast are protected from tampering or manipulation. As election officials work to fulfill this commitment and to improve voter confidence, we ask Congress to fulfill its commitment to states by fully funding HAVA.

III. THE 2018 ELECTION CYCLE AND RESTORING VOTER CONFIDENCE

Safeguarding the integrity of our elections process will require the ongoing commitment and vigilance of the federal, state and local governments and our public and private partner institutions. We must collaboratively work to guarantee secure elections, thus restoring voter confidence in our systems and in our democracy.

We ask that Congress, DHS and others such as the Election Assistance Commission, help us rebuild America's confidence in our election systems by promoting state and local efforts and providing clear, accurate risk assessments.

In conclusion, 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.

I want to again thank the Members of this Committee for holding this hearing and giving me the opportunity to speak about this important matter on behalf of NASS.

I look forward to answering any questions you may have for me.