Hon. CONNIE LAWSON, INDIANA Secretary of State

President, National Association of Secretaries of State

Remarks For NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, MEDICINE COMMITTEE ON THE FUTURE OF VOTING

FEBRUARY 21, 2018

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

Remarks by Hon. Connie Lawson, NASS President:

Cybersecurity and potential attacks on the nation's election systems from malicious foreign actors have been the focus of much media attention and conference agendas, but most importantly, these issues are a top priority for state election officials. As you well know, in January 2017, the U.S. Department of Homeland Security designated state and local voting systems as ***critical infrastructure*** in order to offer a federal response to such foreign threats.

Secretaries of State are bolstering cybersecurity and resilience levels, as well as physical security and administrative protocols for future elections by focusing on the key digital components of their state election systems such as: voter registration databases, election management systems, election night reporting systems.

States Are Taking a Proactive Approach.

Secretaries of State are committed to working with their federal, state and local partners on a voluntary basis, including the U.S. Election Assistance Commission (EAC) and the U.S. Department of Homeland Security, to solicit input on threats and share information on risk assessment and threat mitigation. However, we have also established working relationships with organizations to include: MS-ISAC, Harvard's Belfer Center, the Center for Internet Security, the National Guard and many private sector companies to help us continue to improve.

With our government partners, we have focused on:

- Establishing clear and effective structures for threat and intelligence information-sharing, victim notification processes and cyber incident response
- Identifying threat mitigation practices and state legislation/policy trends for consideration

●Conducting risk assessments and implementing continuous vulnerability assessments

●Ensuring that election offices have sufficient equipment, technical support and resources to maintain a sound security posture for their computer-based systems

●Fostering a culture of risk awareness with strong cyber hygiene practices

●Simply communicating with one another constructively on a regular basis

Entities like MS-ISAC, Belfer and CIS have worked tirelessly with us to create resources, best practices and technical advice.

Areas of Shared State Interest – Federal, State and Local

As just mentioned, we are intensely focused on establishing clear and effective structures for threat and intelligence information-sharing, victim notification processes and cyber incident response. This has been our top priority.

●Secretaries are in the process of obtaining federal government security clearances in order to access timely threat information. We have also been able to designate two senior staff members in our office to begin this process so that we can take whatever information we are given and make it actionable.

●We established an Elections Infrastructure Government Coordinating Council to convene federal, state and local officials on a regular basis. The purpose of this Council is to focus on communications protocols – threat notification, incidence response, and external communications. Election 2016 showed us that there was a great deal of work that needed to be done to improve this communication. The Council is now finalizing communications processes for election-specific notifications

●We have also promoted the leveraging of MS-ISAC and State Fusion

Centers for continuous monitoring, threat detection and incident awareness/response.

●We have developed a state-specific cyber incident response playbook, in the event of a major attack, with Harvard University Kennedy School of Government's Belfer Center.

Secretaries are also identifying threat mitigation practices and state policy trends for consideration.

●We have worked with the Center for Internet Security as they developed the Handbook for Elections Infrastructure Security. Both this document and the Belfer document were released last week during the NASS 2018 Winter Conference.

● As always, emergency planning for our offices includes reviewing and updating policies for back-up paper ballots and equipment, paper printouts/records for polling place use, post-election audits, back-up voter lists (paper and electronic) and voter data security. This is more important now than ever and our cyber incident response/emergency plans reflect that.

States and working with DHS, state agencies and private sector firms to conduct risk assessments by:

- Regularly monitoring election system threats and vulnerabilities to defend any related cyber networks against attacks, including phishing scams, malware, denial-of-service attacks and other common practices employed by malicious actors.
- Working with in-house IT advisors, private security partners, state CIOs/CISOs, Homeland Security Advisors, the Department of Homeland Security and others to ensure that state election systems are secured with technologies and standard operating practices that can successfully diagnose potential cyber threats, track cyberattacks, provide mitigation options and enhance the resilience of state systems.
- Documenting and reviewing all security procedures/systems, including pre- and post-election protocols and testing procedures,

physical security and chain of custody policies and response to reported hardware/software issues.

It is imperative that election offices have sufficient equipment, technical support and resources to maintain a sound security posture for their computer-based systems, including:

● Consulting with key stakeholders regarding current levels of investment in state and local election infrastructure. Requesting regular cybersecurity briefings from Governor/State CIO or CISO.

● Replacing aging voting equipment that is nearing end of life, no longer meets state testing and certification requirements, or will soon fail to meet such requirements due to lack of technical support/replacement parts.

● Bringing laws and policies guiding election administration into compliance with existing legal exemptions for critical infrastructure information-sharing under federal law.

We are also working within our offices to foster a culture of risk awareness with strong cyber hygiene practices, including:

● Training or guidance on cyber hygiene protocols for elections officials, along with establishing clear communication protocols between state-local officials.

● Providing guidance on procedures for reporting election issues and security-related incidents (i.e. state hotlines, poll worker guidance, state task force, DHS/FBI coordination, state fusion center with law enforcement).

What Else Will Combat Foreign Threats?

We believe there are also a number of specific things that can be done to help us combat threats to our election systems:

- Keeping elections state and locally-run (decentralized),
- Keeping voting equipment offline and leaving voting machines unnetworked,

- Keeping voter lists clean and up-to-date and
- Urging our fellow citizens to take part volunteering at the polls.
- Finally getting Congress to appropriate the remaining $396 million in Help America Vote Act (HAVA) funds. This action alone will help elections officials get money quickly for more cybersecurity assistance and new voting machines.

Our “ask” of this group is to work with those in state and local government to share your expertise. Understand the limitations we face in resources and staffing and help us find solutions to those challenges. Thank you, our NASS Executive Director, Leslie Reynolds, will be able to take your questions. It has been a pleasure speaking to you about these important efforts.