Statement from the

Honorable Tom Schedler

Louisiana Secretary of State

Former President, National Association of Secretaries of State (NASS),
Co-Chair, NASS Elections Committee

Member, NASS Election Cybersecurity Task Force

Before the U.S. Subcommittee on Information Technology and
Subcommittee on Intergovernmental
Affairs of the House Committee on Oversight and Government
Reform

Cybersecurity of Voting Machines

November 29, 2017
Washington, DC

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

Securing elections occurring this November, in 2018, and beyond are of critical importance to our nation and our Secretaries of State. We are not naïve about the likelihood of future cyberattacks against digital elements of election systems, but we also know paper ballots include fraud vulnerabilities as well unless proper procedures and protocols are adopted and followed by election officials. That is why all 50 states continue to prepare accordingly.

Chief state election officials and their staff are constantly evaluating and developing programs to safeguard the integrity of their elections systems. In the last year-plus, those efforts have largely focused on the latest form of potential fraud--cyberattacks. My perspective comes from serving as Louisiana Secretary of State and past president of the National Association of Secretaries of State, or NASS, which represents a majority of the nation's chief state election officials. I also serve as the current co-chair of the NASS Elections Committee, and a member of the NASS Election Cybersecurity Task Force. Most recently, I was also appointed by NASS to serve as one of eight (8) Secretaries on the newly formed Election Infrastructure Subsector Government Coordinating Council.

Let me begin by thanking this Committee and Chairman Hurd for the invitation to participate today. It is important for you to hear the perspective of those who oversee elections across the country. First, I'd like to address the important developments taking place through the NASS Election Security Task Force.

NASS Election Security Task Force

The NASS Election Security Task Force was established in February 2017. This is a bipartisan body of the nation's chief state election officials. The mission of the Task Force is to promote the unique priorities and challenges that exist regarding cybersecurity and elections. In addition to helping states share information and combat cyber threats, the Task Force is charged with providing guidance on NASS efforts to create partnerships with public/private stakeholders, including the US Department of Homeland Security (DHS) and the US Election Assistance Commission (EAC). For example, the Task Force regularly works with elections and cybersecurity experts like the Center for Democracy and Technology, the Democracy Fund, and Harvard's Belfer Center plus other organizations looking to provide support and advice.

NASS has been a key player in the development of the new Election Infrastructure Subsector Coordinating Council (EIS-GCC). This "Council" is required as a result of the new designation for elections as critical infrastructure. Over the past several months we have worked with other state and local election official organizations as well as DHS and the EAC to try to make this "Council" function for a critical infrastructure sector that is really unlike any other. Instead of being chaired by a federal agency, it will be run by an Executive Committee of federal, state and local officials.

The "Council" is designed to facilitate improved communications between federal, state and local officials on threats and vulnerability information which as you know, did not go extremely well in 2016. The "Council" will meet numerous times over the next year to establish communication

protocols for threat sharing and notification. The goals are to fine-tune DHS resources and tools available for state and local governments, and to discuss and review cyber best practices for sharing with state and local election officials.

In full transparency, NASS opposed the Critical Infrastructure designation in February 2017 because our members were concerned about the possibility of federal overreach and because the designation came without meaningful consultation with any election officials. My colleagues and I understood that we could continue to get the same support and services from DHS without a Critical Infrastructure designation, thus it seemed an unnecessary and overly burdensome and bureaucratic move. However, the designation is still with us and we have made a good faith effort to work together with DHS to improve lines of communications on election cybersecurity issues.

Part of these improved communications includes our successful lobbying for chief state election officials to obtain security clearances. We have often been told by DHS that they can't share some piece of information because it is classified. Hopefully, these new clearances will address this problem. DHS is also working to secure two additional clearances for staff designated by the Secretary of State. This will help to turn classified information into actionable information that states can employ to further protect their systems.

Innovative Cybersecurity Initiatives at the State Level

Ensuring the integrity of the voting process is central to the role of the chief state election official. Allow me to share with you some of the ways we are working hard to bolster election cybersecurity in the states:

Hosting State Cybersecurity Summits for Elections/IT Officials: In conjunction with the Rhode Island State Board of Elections, Secretary of State Nellie M. Gorbea recently convened over 100 local elections and IT officials for a Cybersecurity Summit at Salve Regina University in Newport, Rhode Island.

The three-hour forum highlighted national conversations around elections and cybersecurity and trained attendees on best practices to help keep these systems secure. Secretary Gorbea noted that Rhode Island has modernized its elections infrastructure over the past three years.

Leveraging National Guard Cybersecurity Expertise: In West Virginia, Secretary Mac Warner has added an Air National Guard cybersecurity specialist to his office staff.

The specialist holds top security clearance in the Air National Guard and will assess the state's elections systems and cybersecurity defenses. The specialist is embedded in the state's Fusion Center, which anticipates, prevents, and monitors criminal and terrorist activity in the state. The Fusion Center, the state's Division of Homeland Security and Emergency Management, and the National Guard are all part of West Virginia's Department of Military Affairs and Public Safety.

Several other states work with the National Guard on a variety of exercises to improve their cyber posture. For example, the Colorado National Guard's Defensive Cyber Support team works with the Secretary of State's cyber team to monitor online voter registration system activity. They are prepared to assist if cybersecurity incidents occur. In Ohio, the National Guard's cyber unit conducts penetration tests to check the state elections system for vulnerabilities or malicious activity. And in states like Rhode Island, the Secretary of State incorporates the National Guard in their statewide cybersecurity training for elections and IT officials.

Initiating Third-Party Risk Assessment of Electronic Data System: Vermont Secretary of State Jim Condos solicited a third-party risk assessment of its physical and electronic data systems in 2015. The process led his office to build new firewalls around several of its web applications and to begin regular penetration testing.

Vermont, along with many other states, also conducts audits within 30 days of each election. Votes are recounted in a sampling of precincts to reveal any discrepancies between the paper ballots and Election Day tallies. New risk-limiting audits are beginning in Colorado this November and a handful of states around the country have recently passed legislation to employ this practice. We will be watching and learning from these states as other states begin to pursue activity like this.

Assisting the Locals

Secretaries of State have a strong, pre-existing relationship with local election officials. Colorado's office provides endpoint protection software for counties to install on their computers to detect virus and malware infections.

Advanced malware detection software like Malwarebytes, BitDefender, and Crowdstrike can help prevent infection of computers by phishing attacks and provide monitoring in order to assist in reacting and responding to events quickly.

Additionally, the Colorado Secretary's staff provide cyber cross-training and audits for county elections staff. They also conduct yearly tests for county staff who interact with state voter registration systems and require them to adhere to state security standards.

Other Cybersecurity Initiatives Involving One or More States:

Establishing State 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.

Working with the Multi-State Information Sharing and Analysis Center (MS-ISAC): The mission of the MS-ISAC is to improve the cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.

Seven states are working with MS-ISAC on a pilot project to develop an elections-specific ISAC. This will enable more targeted information for state elections officials as they partner with MS-ISAC. The seven states participating in this pilot project are: Colorado, Indiana, New Jersey, Texas, Virginia, Vermont, and Washington.

Retaining, Updating Security Tools and Procedures. States are constantly adding new cybersecurity tools and procedures. 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 these plans now include cyber incident responses. Some have or are developing disaster recovery plans that include strategies when election systems and data are disrupted. Table top exercises are also included incident response plans. The exercises test emergency procedures and communications.

Monitoring Social Media Accounts: As Election Day approaches, some states monitor their office's social media with increased scrutiny. They note any increased use of certain terms on Facebook or Twitter that indicate potential meddling in the election process. By picking up on these terms quickly, they are able to react instantly, heading off any orchestrated attempt to influence the election via social media.

The Security of Voting Systems

With the passage of the Help America Vote Act in 2002, states were required to purchase at least one piece of accessible voting equipment for each polling place. Back in 2002, the accessible equipment available to purchase were Direct Recording Electronic Equipment (DRE's). The Election Assistance Commission and the National Institute for Standards and Technology (NIST) began updating the existing voting system guidelines to address these new systems. They have been updated in full or in part only a handful of times since then.

Just last month, the EAC released their latest draft of the Voluntary Voting System Guidelines (VVSG 2.0). The guidelines are a set of manufacturing specifications that voting systems can be tested against to determine if they meet certain standards of functionality, accessibility, accuracy, auditability and security capabilities. VVSG 2.0 have been approved by the EAC's Technical Guidelines Development Committee (TGDC) and is currently going through a public comment period. The next step will be consideration by the EAC Board of Advisors and Standards Board and final approval by the EAC Commissioners which is expected in the Spring of 2018.

In Louisiana, we take pride that we go above and beyond in following best practices in terms of our voting machines. We are a top down state: the state purchases, controls, stores, repairs, and

programs all of the voting machines across the state. Additionally, we have the most current software available on all of our voting machines, and we test each and every one before and after the election. Once the machines are tested, a tamper proof seal is placed on them to protect against any intrusions.

Let's face it: not all counties and municipalities in a state are set up this way so we are not necessarily equal. But in Louisiana, because no one touches our voting machines except our staff; because they are never sent out to the manufacturer for repairs; because they are not handled by individuals or companies who program voting machines and; because they are very tightly controlled by our office and our office alone, I have the utmost confidence in our vote tallies. In fact, in many ways, our machines are overwhelmingly trusted by our voters when compared to their confidence in the security of mailed, paper ballots.

The bottom line is, because the State of Louisiana purchases and maintains all of our voting machines even a poor parish (county) can have just as secure an experience on Election Day as a wealthy one. That's the definition of a fair and impartial election.

My conclusion, after more than a year of intense questioning of my own staff and experts, is: we believe we have the most up-to-date and effective processes and procedures in place to keep our voting machines safe and operational. Machines that have been hacked at attention-grabbing conferences like DEFCON do not take into account any of the security/safety measures I just outlined and are not set up in real world election environments by any stretch of the imagination. To me, that is not an accurate test or a level playing field.

Since the Presidential Election of 2016, my staff have managed five elections. Absent the hype about Russian hacking, we have received no complaints from voters at all about the performance or accuracy of our voting machines. None.

Do we need to be prepared? Yes. Do we need to continue to update our processes and procedures? Yes. Do we need to vigilant? Yes. Each state has to decide for itself how best to secure their citizens' election system. Louisiana is not a same day/automatic voter registration state. Louisiana only uses paper ballots for absentee voters, so it is quite limited. Louisiana does have a Photo I.D. law that has been in place since 1997 and is well accepted by voters. These choices have protected the integrity of our election systems in Louisiana very well.

As Secretaries of State we look to NASS for additional guidance on best practices for cybersecurity from groups like the EAC and NIST. We are looking to DHS for clearance so we can receive classified information on credible threats to mitigate our risks. Most of all, we are looking for the remaining $396 million federal HAVA dollars that have never been appropriated to help us replace aging equipment purchased over ten years ago. These are the real needs to secure our election cybersecurity going forward.

Thank you for this opportunity to comment.