STATEMENT FROM THE
HONORABLE CONNIE LAWSON

INDIANA SECRETARY OF STATE
PRESIDENT-ELECT, NATIONAL ASSOCIATION OF SECRETARIES OF STATE
CO-CHAIR, NASS ELECTION SECURITY TASK FORCE

BEFORE THE U.S. SENATE SELECT COMMITTEE ON INTELLIGENCE

RUSSIAN INTERFERENCE IN THE 2016 ELECTION

JUNE 21, 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

STATEMENT OF

HON. CONNIE LAWSON
INDIANA SECRETARY OF STATE
PRESIDENT-ELECT, NATIONAL ASSOCIATION OF SECRETARIES OF STATE
CO-CHAIR, NASS ELECTION SECURITY TASK FORCE

CONCERNING

RUSSIAN INTERFERENCE IN THE 2016 U.S. ELECTIONS

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

JUNE 21, 2017

Good morning, Chairman Burr, Vice Chairman Warner and distinguished Members of the Committee. Thank you for the chance to appear before you today to represent the nation's Secretaries of State, forty of whom serve as the chief state election official in their respective states. My name is Connie Lawson, and I am the Indiana Secretary of State. I am also president-elect of the bipartisan National Association of Secretaries of State (NASS), and in that leadership capacity, I also Co-Chair the NASS Election Security Task Force. NASS President Denise Merrill of Connecticut was not able to be here today, but I do want to acknowledge her outstanding leadership around the last election cycle and point out that we are a bipartisan organization.

It is an honor to be here with my distinguished fellow panelists to discuss what is ultimately our government's capacity to secure state and locally-run elections from Russian and other very significant and persistent nation-state cyberthreats. With statewide elections in New Jersey and Virginia this year, and many more contests to follow in 2018, 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, we believe it is even more important for us to be discussing what lies ahead.

In this regard, we are struggling to understand – and implement – the U.S. Department of Homeland Security's January 2017 Executive Order designating elections as "critical infrastructure." I am part of the bipartisan majority of Secretaries of State who support a push to rescind the measure, which clashes with some of the most basic principles of our democracy and already seems likely to cause more problems than it actually solves. Furthermore, the time it has

taken to educate DHS on state and local elections, even after the designation was made, has been a drain on limited resources, which should be invested in strengthening election security.

I. FOREIGN TARGETING OF STATE AND LOCAL ELECTION SYSTEMS

First and foremost, I applaud you for holding this hearing today. This forum offers a chance to separate FACTS from FICTION regarding the 2016 presidential election.

As Senator Warner noted in a letter sent yesterday (June 20, 2017) to Homeland Security Secretary Kelly, we have not seen any credible evidence that vote casting or counting was subject to manipulation in any state or locality in the 2016 election cycle, or any reason to question the results. While still alarming, there is a big difference between manipulating VOTERS and manipulating VOTES.

Here is what chief state election officials know about documented foreign targeting of state and local election systems in the 2016 election cycle, as confirmed by DHS:

- No major cybersecurity issues were reported on Election Day: November 8, 2016. In certain areas of the nation where machine calibration or e-pollbook issues arose, they were immediately flagged to the attention of DHS.

- DHS confirmed to NASS that 33 states and 36 county jurisdictions had taken advantage of the agency's voluntary assistance by Election Day. NASS and DHS also achieved a joint goal of ensuring that all 50 states were notified of the federal government resources that were available to them upon request, including cyber hygiene scans on Internet-facing systems and risk and vulnerability assessments. Those states that did not utilize DHS assistance received similar support from their own state.

- We also learned that foreign-based hackers were able to gain access to voter registration systems in Arizona and Illinois last summer, prompting the Federal Bureau of Investigation (FBI) to warn state election offices to increase their election security measures for the November 2016 election. To our knowledge, no data was deleted or modified as part of the breaches, and these are not systems involved in vote tallying. A representative from the Illinois State Board of Elections is here to discuss that today, so I will let him speak to this subject.

- Of course, in more recent days, we have learned from a top-secret NSA report that the identity of a company providing voter registration support services in several states was compromised, and some 122 local election offices received spear phishing emails as a result. The vendor targeted by Russian military phishing emails operates in six Indiana counties, but here is where it is important to understand how elections work in many of the states.

In Indiana, these six counties use this vendor's e-pollbook equipment, which is not connected to voting machines or tabulation machines.

While there is clearly a pattern of foreign targeting of election systems in the last cycle, it is also very important to underscore that voting machines are not connected to the Internet or networked in any way. I say this not only for the benefit of this Committee, but for the media as well. We must understand how to label, describe and discuss election infrastructure responsibly and accurately when informing the public about elections, because there has been a great deal of misinformation publicized, including statements from the federal government.

We have submitted for the record the Report on NASS Facts & Findings on Cybersecurity and Foreign Targeting of the 2016 U.S. Elections from March 2017.

It is gravely concerning that election officials have only recently learned about the threat referenced in the leaked NSA report, especially – and I emphasize this – given the fact that DHS repeatedly told state election officials no credible threat existed in the fall of 2016.

Secretaries of State took part in three calls where former DHS Secretary Jeh Johnson was asked whether any documented threats existed, on:

- August 15, 2016;
- September 8, 2016; and
- October 12, 2016.

Each time Secretary Johnson was directly asked about specific, credible threats and each time he confirmed that none existed.

We have submitted into the record a DHS readout of the first call that NASS had with Secretary Johnson after we proactively reached out to DHS and requested such a call. It remains unclear why our intelligence agencies would withhold timely and specific threat information from chief state election officials, who can use it to better defend their systems and neutralize specific threats.

I hope this Committee will be using its time to seek out the answer to this important question.

II. PROTECTING STATE AND LOCAL ELECTIONS FROM CYBER THREATS

Before I talk about ongoing cyber threats and the critical infrastructure designation for elections, I want to emphasize some of the systemic safeguards we have against cyber attackers. Our system is complex and decentralized, with a great deal of agility and low levels of connectivity. It is not a massive, centralized bureaucracy, but rather locally-run, bottom-up system.

As we repeatedly emphasized during the 2016 election cycle, diversity serves as a major check on the capabilities of nefarious actors to manipulate our voting process, because there is NO NATIONAL SYSTEM to target. Even within states, much diversity can exist from one locality to the next.

Researchers at Harvard University's Belfer Center noted in a 2016 report that for a federal election, manipulation at a level required to swing the result would be a significant undertaking. Their cybersecurity researchers noted that "for some methods of interference, manipulating 1,000 votes requires 1,000 times as much effort as manipulating one vote."[1]

While electoral interference can take many forms, including physical and cyber-based attacks, for the sake of today's hearing, I'll focus on three chief areas of concern to Secretaries of State:

- Attacks that target access to data or systems;
- Attacks that target their integrity; and
- Attacks that target their availability.

To my knowledge, we have only seen documented attacks of the first variety. Of course, that does not mean our adversaries won't try again. We are not naïve about the likelihood of future cyberattacks against digital elements of election systems.

I work with an excellent team, including Indiana's Information Sharing and Analysis Center (IN-ISAC). Indiana's Voting System Technical Oversight Program, run by Ball State University, requires all voting systems, tabulation systems and e-pollbooks to be certified prior to use. Indiana is developing more rigorous authentication processes.

I have every confidence that other panelists will address voting equipment risks and conceptual attack scenarios that are well-documented by academic researchers. Access control, data processing, cryptography and software design are important issues to be addressed moving ahead.

I would also caution that effective election administration is a constant balancing act between SECURITY and ACCESSIBILTY. Remember, our electoral process has been around for well over 200 years – long before the digital age. We can take down every electronic or online system we have, switch to paper ballots and hand counts and use only paper voter registration forms, but this type of security-first approach will result in a reduction to voter accessibility.

In some cases, the trade-offs may not be worthwhile. For example, finding that hackers accessed or copied voter file information is *by itself* not enormously significant—interested parties can often legally purchase voting roll information without hacking, as it's considered a matter of public record

[1] Ben Buchanan and Michael Sulmeyer. *Hacking Chads: The Motivations, Threats and Effects of Electoral Insecurity,* Harvard Kennedy School Belfer Center for Science and International Affairs, October 2016, pg. 12.

in most states. I don't want to get into discussing speculative "what if" scenarios here today, but I am happy to come back to this issue if you have any questions.

III. THE FUNDAMENTAL UNIQUENESS OF ELECTIONS AS CRITICAL INFRASTRUCTURE

This leads me to the Department of Homeland Security's designation of election systems as so-called "critical infrastructure" on January 6, 2017. It cannot be stressed enough: Elections are FUNDAMENTALLY DIFFERENT from any other sector or subsector of critical infrastructure.

At the outset, I want to appropriately describe the relationship between NASS and DHS. This winter, NASS adopted a bipartisan position opposing the designation. While some may find it inconsistent for NASS to collaborate with and educate DHS while working to have the designation rescinded, we must ensure the states have appropriate representation, regardless of the underlying position.

There is no question that expanded information-sharing between all levels of government will be helpful for increasing the resiliency of our electoral system.

Some additional issues that exist with the designation include:

- A lack of clear parameters around the order, which currently gives DHS and other federal agencies a large amount of unchecked executive authority over our elections process. At no time between August 2016 and January 2017 did NASS and its members ever have a thorough discussion or review of what the designation means (including questions answered) with DHS or anyone else at the federal level. In fact, my colleagues and I across the nation continued to ask for information at the time the designation was announced. We actually held a call with Secretary Johnson the day before, on January 5th, and the decision to move forward with the designation was never mentioned. Serious questions remain about the actual benefits of the designation, and the role of the other federal agencies as outlined in Presidential Policy Directive 21 (PPD-21), such as the Department of Justice, the Commerce Department, the General Services Agency and the U.S. Election Assistance Commission.

- According to PPD-21, which guides the federal government's approach, DHS – not the states – becomes the center of work to protect elections against independent and state-sponsored attacks – particularly cyberattacks. While election officials have been told their participation is "voluntary," it remains to be seen just how voluntary such commitments will be down the road. Will states be required to conform to new federal standards set forth with no real process or oversight in place? What resources or threat information will be withheld from states that do not voluntarily participate?

- There are also concerns about maintaining public trust in elections. U.S. government military and intelligence agencies can classify their work to shield it from public scrutiny. How will the broad exemptions from public records and sunshine laws that are afforded to critical infrastructure affect transparency in our electoral process? Right now, our system is designed to foster transparency and participation from end to end – from public testing of voting equipment to poll watchers to public counting of the ballots to post-election audits.

- Finally, Secretaries of State have serious concerns about the lack of federal government information-sharing regarding documented threats against election systems, particularly in the wake of the leaked NSA report. DHS touted threat-sharing as a key justification for the decision to designate elections as critical infrastructure. Yet, nearly six months after the designation and in spite of comments by DHS that they are rushing to establish their elections subsector, no Secretary of State is currently authorized to receive classified threat information from our intelligence agencies.

Think about that for a moment. If you are looking to improve election security, wouldn't you logically want to ensure that election officials are getting important information to help protect their systems? In fact, we have yet to hear any definitive statement by DHS on whether this designation will stand.

What is obvious is that setting up a hastily-formed subsector of critical infrastructure around elections isn't going to make us more secure. Thus far, there is a large knowledge gap that is unfortunately eroding confidence in the election process and shredding the rights that states hold to determine their own election procedures, subject to Acts of Congress. If the designation reduces diversity, autonomy and transparency in state and local election systems, the potential for adverse effects from perceived or real cyberattacks will likely be much GREATER – and not the other way around.

IV. PREPARING FOR THE 2018 CYCLE

I will conclude by briefly discussing preparations around upcoming elections, which as I mentioned are already underway.

The NASS Election Cybersecurity Task Force, which currently has members from 27 states, was created to ensure that state election officials are working together to combat threats and foster effective partnerships with the federal government and other public-private stakeholders. Some of the specific deliverables include:

- Developing resolutions on election cybersecurity to assist state election offices;

- Assisting NASS with guidance on federal government outreach and information-sharing related to election cybersecurity, including the DHS critical infrastructure designation for election infrastructure, assuming it will be retained under the President's administration;
- Developing and convening forums where new governance approaches and best practices can be discussed; and
- Sponsoring technical forums for those who are directly responsible for protecting digital election processes and systems.

We have already begun some important data collection to inform the work of the states. Additionally, we are also continuing our outreach to and education of DHS so the appropriate officials can receive classified information.

In the meantime, the DHS Inspector General is conducting an independent investigation into evidence of unauthorized scans that were performed from a DHS IP address against the Georgia Secretary of State's computer network. The Indiana Secretary of State's office has also submitted results of a state investigation that concluded with a "high degree of certainty" that similar unauthorized activity was detected against their computer network from the same IP address. Other states have similar concerns.

We need a forthright accounting from the Inspector General's office as soon as possible and hope to hear more on the status of this investigative work very soon.

In guarding against cyber threats, the trend line is positive, but more can be done. All but five states require their voting machines to produce a voter-verifiable paper trail that would enable recounts and audits, and we already know that some of those states are actively discussing their options. The majority of states have switched to optical scanning systems in which the voter marks a paper ballot that also serves as evidence for later verification.

Many states and localities are also working to upgrade their voting equipment. In 2016, 43 states used voting machines that are more than ten years old. Election officials have been approaching their state and county lawmakers about replacing or updating these systems to bolster their cybersecurity poster by 2018 or 2020.

In addition, the U.S. Election Assistance Commissions (EAC) Voluntary Voting System Guidelines (VVSGs) are being updated to reflect new ways to increase security and resiliency in voting machines and related technologies.

If I have one major request to Congress and the Administration other than rescinding the critical infrastructure designation for elections or placing clear parameters on the Executive Order, it would be to help election officials get access to classified information-sharing. We need this information to take appropriate actions to defend state elections from foreign interference and respond to threats.

According to a 2017 survey by the Center for Strategic and International Studies, fewer than half of respondent organizations are using unclassified government information as a source of information in making decisions about cybersecurity.[2] More than three-quarters believe that faster access to security clearances would be the most effective way to improve their cybersecurity posture, and 66% want greater access to threat intelligence. States see cooperation with our national intelligence agencies as an important part of their cybersecurity strategy, and with the right threat information-sharing info, an important part of increasing both the physical and the digital elements of their systems.

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. States continue to increase protection for their own systems, as evident by the already common trend of re-implementing handwritten ballots. With increased cooperation and diversity, and not expanded top-down regulation, elections systems will become more resilient and protected.

To quote a letter sent to election directors on September 28, 2016 by Senate Majority Leader McConnell, Senate Minority Leader Reid, House Majority Leader Ryan and House Minority Leader Pelosi:

"The local authorities who bear the responsibility cannot now, and should not in the future be able to, point the finger of blame at some distant, unaccountable, centralized bureaucracy.... For over 200 years states have overcome every challenge to ensure the smooth functioning of our democracy. We trust now that you will take the steps necessary to meet the challenges of the 21st century by securing your election systems against cyberattacks."

I want to thank the Committee again for holding this hearing and for 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.

Thank you.

[2] *Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity*, Center for Strategic and International Studies, February 2017, pg. 17.