Nellie M. Gorbea
Secretary of State

Statement from

The Honorable Nellie M. Gorbea

Rhode Island Secretary of State

Presented to the

United States House of Representatives
Committee on Homeland Security

Hearing on "DHS's Progress in Securing Election Systems and Other Critical Infrastructure"

July 11, 2018
Washington, DC

Thank you, Chairman McCaul and members of the Committee, for the invitation to participate in this important discussion of how to best address cyberthreats to our elections.

I commend your Committee for holding this hearing to learn more about what is being done on the federal, state and local levels to protect our nation's elections systems and what can be done to improve upon this work. The advances in technology have brought with them a paradigm shift in elections administration. Addressing cybersecurity in elections has become an urgent and relevant matter. Cybersecurity is at the forefront of elections conversations taking place right now at every level of government across the country.

Before I continue, I want to recognize my Congressman, Jim Langevin, for his visionary leadership in elections administration in his past service as Rhode Island's Secretary of State. Two decades ago, then-Secretary Langevin led Rhode Island's early adoption of voting technology that replaced the ancient mechanical *Shoup Lever* voting machines with paper-based optical scanners.

In Rhode Island, we are proud of our role as an innovator in elections technology. In 1936, for example, Rhode Island was the first state to use voting machines at *every* polling place across the state, not just in major cities, as had been the practice at that time across the country.

As Secretary of State, I am building on that legacy of innovation and excellence despite the significant challenges that my state and almost all other states face. These challenges can be summarized as follows:

1. First, although this is not currently the case in Rhode Island, many elections across our country are being run on equipment that is either obsolete or near the end of its useful life.

2. Second, our public-sector employees and systems at the state, county and municipal levels are ill-prepared to handle the looming threat of cyberattacks.

3. Finally, our country is facing a very real threat presented by foreign actors and others who are conducting activities that serve to erode the public's trust in the integrity of our elections. These attacks are real and are focused on undermining our representative democracy.

Congress recently took an important step to help us address these challenges by providing $380 million for elections administration and security in additional Help America Vote Act (HAVA) funds in the Consolidated Appropriations Act. On behalf of my colleagues who oversee elections across the country I thank you for this important investment. I also want to emphasize that the challenges our democracy faces require an ongoing commitment of funds. Elections officials today, are tasked with preparing for threats that were nonexistent five years ago and are continuously evolving. Funds, training and improved communication are critical to ensuring that we continue to protect our democracy.

Actions addressing this new landscape of elections and cybersecurity have taken place in a variety of ways because elections are organized and run differently in every state. Nonetheless, I believe that our efforts in Rhode Island over the past three years offer valuable insight into the challenges and opportunities that elections officials face in this era of increased cyberthreats.

In Rhode Island, while I serve as chief state election official under HAVA, elections are run in coordination and collaboration between my office, the Rhode Island State Board of Elections and local elections officials with their boards of canvassers. My office, the Department of State, maintains the Central Voter Registration System (CVRS), a voter registration database and elections management system used by all local elections officials that was developed thanks to HAVA funding during Secretary of State Matthew A. Brown's administration. A separate agency, the Rhode Island State Board of Elections, oversees Election Day operations, is responsible for the security of the voting equipment and handles post-election disputes and audits. Meanwhile, local elections officials and their boards of canvassers run the polls on Election Day.

Our collaboration is a key ingredient to successfully running elections. Over the past year, we have strengthened relationships with our federal partners, specifically the Election Assistance Commission (EAC) and the Department of Homeland Security (DHS). We have also taken advantage of state resources such as the cyber unit at the Rhode Island National Guard and the expertise of faculty members at Salve Regina University and Brown University.

So how has Rhode Island handled the three challenges I described above?

First, we addressed the topic of equipment. When I took office in 2015, our voting equipment, purchased in 1997, was on the brink of total failure. Thankfully, when I confronted them with the problem, the leadership of our state took this issue seriously – Speaker Nicholas Mattiello, then Senate President Teresa Paiva Weed and the membership of the General Assembly, along with Governor Gina Raimondo, all supported the purchase of new paper-ballot optical scanning machines. This translated into an investment of nearly $10 million over the next 7 years. The EAC was instrumental in providing us with key advice and counsel in the development of the Request for Proposals for the new voting equipment. Because of these efforts Rhode Island entered the 2016 election cycle with new, secure voting machines that have four layers of security and encryption.

We have also modernized many other aspects of the electoral process and infrastructure. Over the past two years we have implemented online voter registration, acquired electronic poll books and recently implemented automated voter registration. These advancements make both voting and the administration of elections more efficient for all involved.

While modernizing the electoral process and infrastructure, we also leveraged resources offered by the Department of Homeland Security under their critical infrastructure designation, to further protect our Central Voter Registration System. Recently, DHS performed external penetration testing and vulnerability scanning to assess any cybersecurity concerns with regard to our voter registration system. This Risk and Vulnerability Assessment provided my office with areas that needed to be improved to ensure our system is as secure as possible. In addition, the Rhode Island National Guard provided a security analysis of the electronic poll books (e-poll books), used during a recent election, to assess possible security vulnerabilities.

But investments in hardware and software cannot be used effectively if government does not have the human resources that can manage and operate them. Our second challenge is one of building the capacity of the public sector to manage and respond to cyberthreats in our elections.

In Rhode Island, I have increased my office’s IT staff by 40% to ensure that we have the technical expertise in-house necessary to respond to the ever-shifting landscape that technology presents. This investment in our state workforce has also allowed us to deploy online tools and resources that not only make our elections infrastructure more secure, they make it easier for voters to participate in elections.

It is important to note that security breaches can come through any connection within a governmental office, even those that may be physically removed from elections-related infrastructure. That is why over the past year we have conducted social engineering training, where our own IT team sends phishing emails to employees to test their awareness of potentially harmful emails. In addition, all our employees participated in cybersecurity awareness and threat mitigation training. These tools teach employees about the dangers of methods that online hackers commonly use to attempt to infect our network.

However, having technically proficient state and local technology professionals is not enough if we do not have a well-developed communications structure between DHS and our country's Chief State Election Officials. Being able to quickly disseminate information on potential threats and respond effectively is critical to safeguarding our elections. The National Association of Secretaries of State was able to persuasively present this issue to the Department of Homeland Security and, as a result, DHS initiated the process of providing Chief State Election Officials like myself with the required security clearance to effectively manage the cybersecurity of elections systems. While this process of communicating cyberthreat information between DHS and Chief State Election Officials was admittedly rocky at first, it is now much improved and will be an important mechanism to share cyberthreat information. At this time, I would like to commend DHS for bringing on former EAC Chairman Matt Masterson to work with states on cybersecurity issues. In my experience working with former Chairman Masterson I have found him to be a consummate professional, and his thorough knowledge of our country’s complex elections systems gives DHS critically important knowledge for more effective policy making.

Additionally, local elections officials are on the front lines and must have the information and resources necessary to identify and mitigate emerging threats. For this reason, in Rhode Island we are members of the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). In addition, by the end of next week I expect all our cities and towns to be signed-up with EI-ISAC. These organizations provide elections officials with cybersecurity products and services as well as best practices that enhance the overall strength of our election systems. For example, the Albert sensor is a device provided by MS-ISAC that monitors and analyzes all traffic that comes into our network. The information it collects is scanned and if something malicious is detected, we are notified.

In Rhode Island, we are also taking steps of our own to ensure full preparedness. Last month, my office and the State Board of Elections hosted a seminar for local elections officials that included a comprehensive tabletop exercise presenting potential scenarios on Election Day. Elections officials were forced to make quick decisions under pressure and practice how to handle such situations. The exercise was based on a similar program my team attended at Harvard University's Belfer Center.

Last year, I convened more than a hundred of Rhode Island's local elections officials and IT staff for a summit on elections cybersecurity. Several industry and academic experts in the field of cybersecurity, as well as Congressman Langevin, provided briefings during the summit. One important message that we focused on that day with local elections officials is that cybersecurity is not a destination; it is a continuous process of assessment, improvement of our systems and mitigation of risk.

This is why we must bring together all stakeholders, regardless of political affiliations, to continually identify threats and work on solutions. This is not a far-fetched ideal. In fact, IT leaders from Google and Facebook have commented that the top technology companies in our country regularly collaborate on cyberthreat information facing their companies despite being fierce competitors. We must develop a similar protocol in the public sector to share information on cyberthreats. In Rhode Island, I have focused on ensuring that our elections officials and staff at every level have the information necessary to minimize cybersecurity threats.

Investment in training of our public-sector employees has become a critical need. As cyberthreats continue to evolve and become more sophisticated, states need additional funding and resources dedicated to the security of elections systems. These funds are necessary for third-party assessments, testing procedures and strengthening IT capacity. The HAVA funds approved by Congress in the recently passed Appropriations Act are an important initial investment in such systems.

Using Rhode Island as an example, I would like to take a minute to discuss some of the critical initiatives that we are investing in with the new HAVA funds.

- One of our key priorities is to secure the registry of voters. Prior to the 2018 election we plan to invest over $500,000 in cybersecurity enhancements to our CVRS.

- The new funds also enable us to rewrite our CVRS application, originally developed in 2004 and 2005, to current industry best-practice standards and help us protect against penetration attempts.
- Understanding that trust in elections results is critical, we will fund the first-ever post-election audits in Rhode Island. This law was passed by our legislature in 2017 and is another step in ensuring the integrity of our elections.
- Ensuring that municipalities also improve their systems and help protect our elections, we will initiate an Elections Administration Improvement Grant Program for cities and towns to make election security enhancements on a local level.

In conclusion, I would like to make the following suggestions:

- Congress can play a critical role by providing ongoing funding to the states so that we remain prepared to face any cybersecurity challenge. As I mentioned above, the additional HAVA funds approved earlier this year are welcome and much needed by jurisdictions across the country. However, sustained funding is necessary for elections officials to modernize their systems to enhance the integrity and security of our elections.

- Federal agencies must continue to provide important training and resources to support the work being done on a state and local level to protect our elections systems.

- Congress also can formalize clear communication channels between federal agencies and state and local governments to share cyberthreats and information to assist in preparing for any outside interference in our elections. The federal government should recognize that it can play a critical advisory and support role in securing elections infrastructure while respecting the fact that elections are the responsibility of state and local elections officials. It is my firm belief that improving the integrity of elections systems can be achieved while simultaneously improving access to voting.

- Finally, Congress must also provide oversight of federal intelligence and security agencies recognizing the important balance that must be kept between security measures needed to safeguard our democracy and the transparency and access to information that preserve our ability to have open government and elections that can be trusted.

Thank you again for the opportunity to present testimony on the work we are doing in Rhode Island and how the federal government can work with states to ensure our nation’s elections systems are secure and our democracy safeguarded.