Nellie M. Gorbea
Secretary of State

Testimony of Rhode Island Secretary of State Nellie M. Gorbea presented to the Congressional Task Force on Election Security

October 24, 2017

Thank you, Congressman Thompson and Congressman Brady, for the invitation to discuss what Rhode Island is doing to protect against cyberthreats to our elections.

I commend you and Minority Leader Pelosi for your leadership in creating this task force that focuses on the health and security of our nation's elections.

I would be remiss if I did not, of course, recognize my Congressman, Jim Langevin, who as you know, before coming to Congress served as Secretary of State in Rhode Island. Nearly two decades ago, then Secretary Langevin led Rhode Island's early adoption of voting technology that replaced the ancient *Shoup Lever* voting machines with state of the art paper-based optical scanners.

Interestingly, Rhode Island's small size and rich history of civic engagement has facilitated its role as an innovator in elections technology. As early as 1936, Rhode Island was the first state to use voting machines at *every* polling place across the state, not just in major cities as was the practice in other states.

Right now, throughout the United States, our elections infrastructure faces several challenges:

- First, although this is not 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.

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

- Finally, our country is facing a very real threat presented by foreign actors 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.

These challenges to our elections have been handled a variety of ways because elections are organized and run differently in every state. Nonetheless, I believe that

what we have done in Rhode Island over the past three years can provide valuable insight into the challenges and opportunities that elections officials face in this era of increased cyber threats.

In Rhode Island, while I serve as chief state election official, elections are run in coordination and collaboration between my office, the Rhode Island Department of State, the Rhode Island Board of Elections and local election officials with their boards of canvassers. My office, the Department of State, maintains the Central Voter Registration System (CVRS). The CVRS is a singular voter registration database used by all local election officials across the state. A separate agency, the RI State Board of Elections, oversees Election Day operations and is responsible for the security of the voting equipment. Meanwhile, local election officials and their boards of canvassers run the polls on Election Day. Our collaboration and cooperation are a key ingredient to successfully running elections. Over the past year, we have developed new collaborations to include federal partners, specifically the Election Assistance Commission (EAC) and the Department of Homeland Security (DHS).

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 was on the brink of total failure. Thankfully, when I confronted them with the problem, the leadership of our state took this issue seriously – Governor Gina Raimondo, Speaker Nicholas Mattiello, Senate President Teresa Paiva Weed and the membership of the General Assembly all supported the purchasing 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. As a result of all of these efforts Rhode Island entered the 2016 election cycle with new, secure voting machines that have four layers of security and encryption.

Similarly, we invested in more secure data storage and cloud based systems. We signed up for the assistance to states under the critical infrastructure designation by the Department of Homeland Security to further protect our Central Voter Registration System.

But investments in hardware and software cannot be used effectively if government doesn't have the human resources that can manage and operate them. My 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 the process. Over the past two years we have implemented online voter registration, acquired electronic poll books and

have just started the implementation of automatic voter registration. It is my firm belief that improving the integrity of elections systems can be achieved while simultaneously improving access to voting.

At this time, I would like to stress how important it is to have better communication between the Department of Homeland Security and our country's Chief State Election Officials. Being able to quickly disseminate information on potential threats and respond effectively is critical. The National Association of Secretaries of State was able to persuasively present to the Department of Homeland Security this issue and, as a result, DHS has begun the process of providing Chief State Election Officials like myself with the required security clearance to effectively manage the cybersecurity of elections systems.

It is important to acknowledge the significant paradigm shift in elections that the issues of cybersecurity have made us face over the past couple of years. Cybersecurity is at the forefront of elections conversations at every level of government across the country.

Just last week, I convened more than a hundred of Rhode Island's municipal election officials and IT staff for a summit on elections cybersecurity. Congressman Langevin provided a briefing during the summit. One important take-away from that meeting, which we should all be mindful of, is that cybersecurity is not a destination but rather a continuous process of assessment, improvement of our systems and mitigation of risk.

This is also a problem that requires us as elections officials to bring together all stakeholders, regardless of political affiliations, to continually identify threats and work on solutions. At a recent workshop I participated in organized by Harvard University's Belfer Center, IT leaders from Google and Facebook discussed cyberthreats. They commented that the top technology companies in our country regularly collaborate on cyberthreat information despite being fierce competitors.

They have realized in the private sector what we need to in the public sector - our elections are only as strong as the weakest link in the chain. Thus in Rhode Island, I have focused on ensuring that our elections officials and staff at every level have the information and support necessary to minimize cybersecurity threats.

As cyber threats continue to evolve and become more sophisticated, states need additional funding and resources dedicated to the security of elections systems. These funds are critically needed for third-party assessments, testing procedures and strengthening IT capacity.

In addition to federal-state collaboration, investment in our public sector IT employees, and much-needed equipment upgrades, Rhode Island also took an important step forward when the General Assembly passed legislation providing for risk-limiting random post-election audits to verify results. These will ensure that Rhode Island

randomly reviews the results of elections to ensure the integrity of the voting machines and the entire process.

In order for our elections to work, Americans need to trust in the integrity of our elections systems. Since our founding, the United States has been a beacon of democracy in the world. We cannot allow the public's trust in our government to deteriorate.

This is particularly important as we seek to strike a balance between life in a free and open society and responding to new cyber threats in this world of big data and eroding privacy. Add to this, the delicate balance between states' rights and federal involvement, and we begin to describe the complexity of the task at hand.

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 election officials.

Congress can play a critical role by providing resources to the states so that we are prepared to face any cybersecurity challenge. It can also serve to provide oversight on the challenge between security measures that are needed to safeguard our democracy and the need to preserve transparency and access to information to protect our open government.

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.