Elections Cybersecurity
in Rhode Island

Nellie M. Gorbea
Secretary of State

April 2018

State Update

Cybersecurity is the practice of ensuring the integrity, confidentiality and availability of information that is created, stored and transmitted in the digital realm. This includes the ability to defend, detect and recover from accidents and intentional attacks. Over the past three years we have modernized our elections infrastructure to improve the security and integrity of Rhode Island elections.

The cybersecurity of elections is a quickly evolving space. Since the 2016 Election, there has been a paradigm shift in the conversation around cybersecurity as it relates to the administration of elections at the local, state and federal level. The national discourse on cyberattacks and elections security has the potential to undermine Rhode Islanders' trust in our electoral process. As Rhode Island's Chief State Elections Official, Secretary Gorbea has been working hard with local, state and national stakeholders to protect the security of electionß systems so that Rhode Islanders can be confident in the integrity of their elections.

Elections are a community endeavor with multiple levels of stakeholders. In 2017, the Rhode Island Army National Guard joined a cybersecurity working group that evaluates the voting systems in the state. Working with the Board of Elections, they performed a cybersecurity assessment of the electronic poll book system at a recent election to identify and evaluate the security of the system.

Everyone involved needs to have not only a basic understanding of the security measures in place for our elections systems, but also be equipped with the latest information to be vigilant against cybercrimes. Secretary Gorbea convened a cybersecurity summit, in collaboration with the State Board of Elections, that brought together more than 100 local elections and IT officials to highlight national conversations around elections and cybersecurity. The 2017 CyberSummit also provided an overview of how our new elections systems work in Rhode Island and trained attendees on best practices to help keep these systems secure.

Below: Secretary Gorbea addresses local elections and IT officials at the 2017 CyberSummit

National Update

In addition to the work at the local and state level, strong communication between the Department of Homeland Security and our country's Chief State Election Officials is important to improving the security of our election systems. Being able to quickly disseminate information on potential threats and respond effectively is critical. The National Association of Secretaries of State (NASS) was able to persuasively present to the Department of Homeland Security (DHS) this issue and, as a result, DHS has begun the process of providing Chief State Election Officials with the required security clearance to effectively manage the cybersecurity of elections systems.

Earlier this year, Secretary Gorbea met with Secretary of Homeland Security Kirstjen M. Nielsen to discuss DHS' efforts to assist state election officials on cybersecurity for the 2018 elections. She also participated in a classified briefing from senior DHS, Office of the Director of National Intelligence, and Federal Bureau of Investigation (FBI) officials in Washington. The briefing described the tactics employed by Russia to influence the 2016 Presidential Election. Of note, intelligence officials stressed that no votes or voter records were tampered with in 2016, but that efforts from foreign actors would likely be employed again in 2018 and beyond.

Rhode Island is working hard to protect the integrity of our elections systems and our efforts have gained national recognition. **Recently, Rhode Island was among 11 states receiving the highest grade for elections security in a new report published by the Center for American Progress.** The report touted Rhode Island as "leading the states in election security, receiving 'good' scores for the three most important categories due to its statewide use of paper ballots, its adherence to minimum cybersecurity best practices, and its new risk limiting audit law."

This report outlines the initiatives Rhode Island has undertaken over the past three years to enhance the security in three areas of critical importance: *online systems, Election Day operations*, and *human resources*. This work has been a partnership of the Secretary of State, the General Assembly, Governor, Board of Elections and local elections officials across our state.

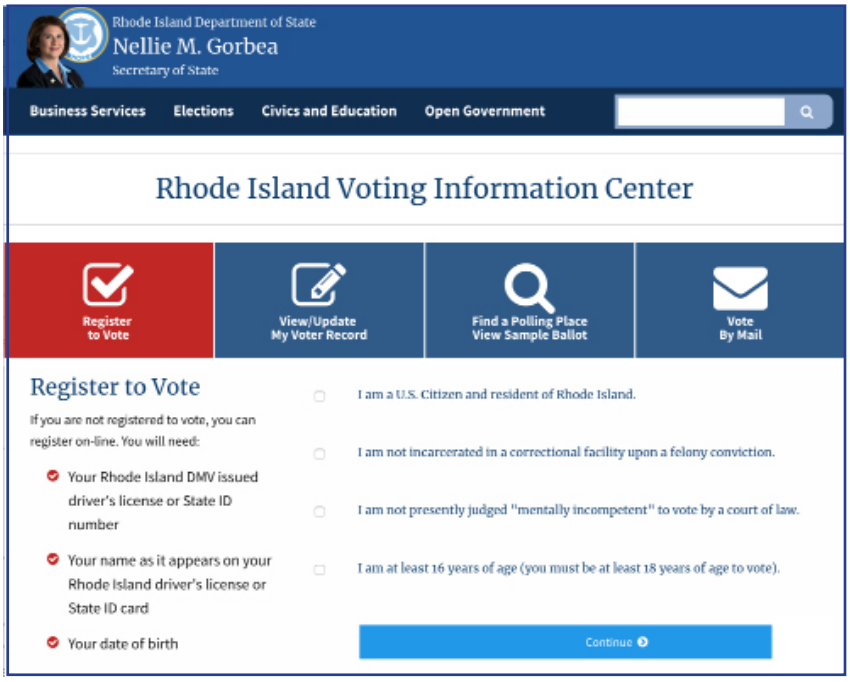
Left: Secretary Gorbea and fellow NASS executive committee members meet with Secretary of Homeland Security Kirstjen M. Nielsen.

Photo courtesy of Vermont Secretary of State.

Securing Online Systems

Protecting our online systems is an ongoing process of risk mitigation. The experience of the private sector has shown that even top companies are vulnerable. The RI Department of State has taken a variety of measures to greatly reduce and mitigate the threat of a cyberattack.

- Rhode Island continues to invest in more secure data storage and cloud based systems with advanced encryption and more rigorous security protocols for all access points.
- Rhode Island has **partnered with the Department of Homeland Security under the critical infrastructure designation to further protect our Central Voter Registration System (CVRS)** by testing for vulnerabilities, sharing cyber security information, threat/incident reporting and receives ongoing risk and vulnerability assessments that include penetration testing, web application testing and social engineering.



Above: Rhode Island's Voting Information Center

- Rhode Island has joined the Center for Internet Security (CIS) and the Multi-State Information Sharing & Analysis Center (MS-ISAC), a consortium created to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.
- Rhode Island has adopted nationally-recognized best practices around cybersecurity threat assessments and vulnerability scanning, including National Institute of Standards and Technology (NIST) and ISO standards.
- The RI Department of State is looking at local higher education institutions with robust computer science and cybersecurity programs to help us continuously assess and protect our elections systems. The Department of State has already benefited from the cybersecurity and computer science expertise of the faculty at Salve Regina University and Brown University.
- The RI Department of State has also reached out and started collaborating with the State's Cybersecurity Officer and the RI National Guard's cybersecurity experts to further test and protect our systems on an ongoing basis.

Securing Election Day

One of Secretary Gorbea's first initiatives was procuring new voting equipment to replace machines that were nearly two decades old. She involved local and state stakeholders in the process. The Rhode Island National Guard has assisted the Board of Elections in performing cybersecurity assessments of the new equipment.

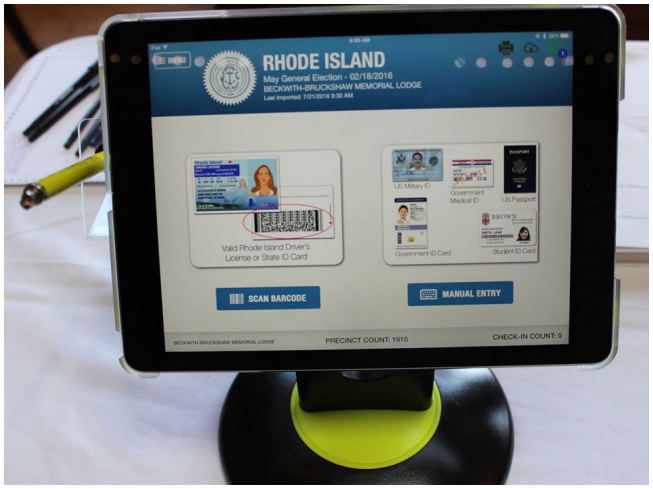
DS200 Voting Machines

Rhode Island purchased new voting equipment ahead of the 2016 state primaries and general election. **The new equipment is a state-of-the-art, paper ballot system. The voting system has four layers of security**:

1. Unofficial results are encrypted and sent in on election night,
2. Thumb-drive containing unofficial results and event logs,
3. Printed results tape for each precinct, and
4. The paper ballots.

Electronic Poll Books

- Rhode Island's new electronic poll books utilize a proprietary encrypted application running on Apple's iOS, which meets the security requirements for the Federal government's secure networks, including classified Department of Defense (DoD) and Department of Justice (DoJ) data applications.
- These electronic poll books use the highest level of data encryption for all data. The use of secure data transfer and 256-bit encryption has been built into the hardware, operating system and Poll Pad application. This is the same standard used by most banks and financial institutions.



Top: DS200 voting machine deployed in 2016. Bottom: Electronic poll books to be fully deployed in 2018.

Post-election Audits

- Rhode Island passed post-election audits legislation in 2017. A post-election audit is a check on the voting machines to ensure their accuracy.
- Rhode Island's law calls for risk-limiting audits, which is an audit of an election contest that provides strong statistical evidence that the outcome of the election is correct.
- Risk-limiting audits require more scrutiny in closer races. If the margin of victory is close, a risk-limiting audit requires manually examining a larger number of ballots.

Securing Human Resources

Secretary Gorbea has been working to ensure that all elections officials at the state and local level are knowledgeable enough to prevent threats or assess problems. Local municipalities have a variety of technological expertise. It is imperative that local elections officials can speak articulately about election security and help us prevent against foreign attacks.

Statewide Cybersecurity Summit

In October 2017, Secretary Gorbea convened local election and IT officials to discuss cybersecurity and how it relates to elections. This event, at Salve Regina University, was attended by more than 100 people who heard from experts in cybersecurity and elections.

The day's agenda covered:

- A National Perspective on cybersecurity issues
- A cybersecurity 101 discussion
- Rhode Island Congressman James Langevin talked about Congressional activities regarding cybersecurity and elections
- An overview of the security protections for Rhode Island's voting systems.

Secretary Gorbea will host cybersecurity summits for local elections officials twice a year. In addition, cybersecurity has been incorporated into all elections trainings by the Department of State.

Department of State Staffing

Secretary Gorbea has used turnover vacancies to increase the Department's IT staff 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 – developed in-house - that not only make our elections infrastructure more secure, they make it easier for voters to participate in the process.

In 2017, the IT division began a "Phishing Campaign" to test and educate all Department of State staff on phishing attempts and scams. These phishing tests are ongoing and will culminate in a "Secure the Human" training that will be taken by all Department of State employees. The training will focus on best practices to identify and mitigate cyberthreats.

In 2018, our **entire Department of State staff will be certified in cybersecurity awareness** relative to topics such as social engineering, data security, personally identifiable information (PII), HIPAA, FERPA, passwords, and physical security.

The Path Forward

Democracies cannot allow cyber threats to election systems—real or perceived—to undermine the role voting plays in our society. Despite the progress made over the past three years, it is important to remember that cybersecurity is not a destination, but a continually evolving road that **requires constant attention to mitigate risk. We must always strive to do better for voters because the single act of casting a ballot is fundamental to our democracy and fundamental to making government accountable to the people it serves.** This will require a continued commitment – and the corresponding dedication of resources – to ensuring the integrity of our voting systems.