



GOV. PHIL MURPHY | LT. GOV. SHEILA OLIVER | DIR. JARED MAPLES

NJOHSP

OFFICE OF HOMELAND SECURITY AND PREPAREDNESS



Joint Release Concerning the Cybersecurity of New Jersey's Election Systems

April 12, 2018 – Press Release

Press Contact: Patrick R. Rigby
communications@njohsp.gov | 609.584.4392

Press Contact: Timothy J. Carroll
communications@sos.nj.gov | 609.414.5041

TRENTON, N.J. – The New Jersey Department of State, through its Division of Elections, and the New Jersey Office of Homeland Security and Preparedness, through its New Jersey Cybersecurity and Communications Integration Cell, released the following statement reasserting continued confidence in the state's election security measures.

“As the state's chief election official, I am working with our team to reaffirm New Jersey's commitment to election security. We are engaging in vital training sessions, constructing interagency communication channels, and helping to integrate best practices downstream to strengthen the security of elections here in New Jersey,” **said New Jersey Secretary of State Tahesha Way**. “The Division of Elections has been and continues to work with federal partners at the Department of Homeland Security, the New Jersey Office of Homeland Security and Preparedness, and other third-party security experts to continuously improve our security posture as the threat landscape evolves. The Department of State is working to ensure that every individual able to cast a ballot in November can do so knowing the state affords a safe and secure system.”

“We are committed to providing cybersecurity assistance to state and local officials throughout this election cycle and beyond,” **said New Jersey Office of Homeland Security and Preparedness Director Jared Maples**. “We are working with county and municipal election officials to offer security services and continuously monitor our systems. To that end, the New Jersey Cybersecurity and Communications Integration Cell provides near real-time awareness of cyber threats and analysis, shares information on sound digital resilience and risk mitigation practices, and acts as a resource for cybersecurity incident reporting.”

State officials are increasing deterrence, detection, and response resources and making relevant upgrades to the State's election systems.

The New Jersey Statewide Voter Registration System (SVRS) has been upgraded and modernized, and rollout is scheduled for after this year's Primary Election. The State is conducting training and working with the U.S. Department of Homeland Security to conduct a Risk and Vulnerability Assessment prior to the rollout.

Distinct from the voter registration system are the voting machines found in each polling place. New Jersey law requires voting machines never connect to the internet; making this a discussion of physical security, not cybersecurity. New Jersey enhances voting machine security procedures through:

- Use of seal-use protocols—steps taken to ensure the physical machine is impenetrable— for tamper-evident seals on all voting machines;

-
- Use of pre-election testing protocols;
 - Requiring a seal-use protocol and voting machine security training class;
 - Requiring all those working on the voting machines to undergo criminal and security background checks; and
 - Hardening and installation of anti-virus software on all election management computers.

The New Jersey Office of Homeland Security and Preparedness (NJOHSP) is responsible for leading and coordinating the State's counterterrorism, cybersecurity, and emergency preparedness efforts while building resiliency throughout the State across all levels of government and the private sector. Through its New Jersey Cybersecurity and Communications Integration Cell (NJCCIC)—an information-sharing and analysis center established to exchange cyber threat intelligence—the NJOHSP continuously works with the New Jersey Secretary of State's Office, its Division of Elections, and the New Jersey Office of Information Technology to proactively assess and enhance other controls that protect New Jersey's election processes. This includes providing advice and guidance to state and local election officials on:

- Monitoring systems for signs of suspicious activity;
- Conducting risk and vulnerability assessments and penetration tests;
- Implementing network hardening controls;
- Providing security awareness training;
- Ensuring continuity of operations plans are in place.

We encourage state and local officials to contact the NJCCIC for assistance at njccic@cyber.nj.gov or by visiting its website at www.cyber.nj.gov.

###

The New Jersey Office of Homeland Security and Preparedness (NJOHSP), a Cabinet-level agency, was created in 2006. The Director serves as the Governor's Homeland Security Advisor, and is responsible for leading and coordinating the State's counterterrorism, cybersecurity, and emergency preparedness efforts while building resiliency throughout the State across all levels of government and the private sector. NJOHSP oversees and distributes discretionary State and federal homeland security and emergency preparedness funds on behalf of New Jersey. More information about NJOHSP can be found at www.njhomelandsecurity.gov

In addition to overseeing the orderly conduct of elections, the New Jersey Department of State's Division of Elections is the filing office for state and federal elective offices, state ballot questions, and bond issues placed on the ballot. The Division also assists county election officials, county clerks, and the public on matters of election administration. It also certifies and publishes election results, certifies voting machines, and manages the statewide voter registration system to ensure compliance with the National Voter Registration Act of 1993. For more information on the Division of Elections, please visit www.elections.nj.gov or follow the Department of State on Twitter at @NJStateDept.