



2020 Election Security Planning Snapshot State of New Jersey

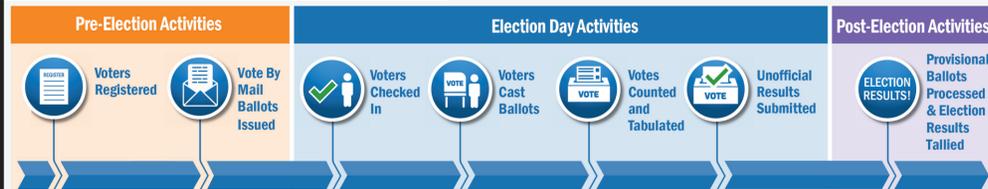


SAFEGUARDS / RESILIENCY MEASURES

THREAT MITIGATION

2020 ELECTION INITIATIVES

New Jersey Election Process



Pre-Election Safeguards

Voters Registered

- Statewide voter registration system protected using administrative, physical, and technical controls.
- Authorized access to statewide voter registration system safeguarded using advanced authentication mechanisms.
- Suspicious activity monitoring and vulnerability testing conducted continuously.
- All system users receive regular security training.
- Continuity of Operations Plans (COOP) regularly reviewed and updated.

Election Day Safeguards

Voters Checked In

- Voter eligibility confirmed through the use of poll books.
- Signature verification for mail-in ballots.
- Failsafe measures protect eligible voters' right to vote.

Voters Cast Ballots

- Emergency ballots available if voting machines fail.
- Mail-in ballots option.
- Voters who return ballots electronically must also submit hard copy of completed ballot via mail.

Voting, Tallying and Reporting Systems

- Electronic and physical security measures ensure voting system integrity on Election Day.
- All voting machines undergo testing by a federally accredited laboratory before purchase.
- Logic and accuracy tests conducted before each election; test results are open to the public.
- Voting systems are not connected to the internet.
- All ballots are securely stored with extensive chain of custody records.

Post-Election Safeguards

Election Results Tallied

- All ballots accounted for at the precinct level.
- Provisional ballot voter eligibility is researched prior to counting ballot.
- Chain of custody records maintained.

Election Results Website

- Access to results database is restricted to authorized users.
- Website results server and election system are securely separated.

Specific Threats / Mitigation

- Social Engineering** refers to bad actors who manipulate their target into performing a given action or divulging certain information (often a login or password). "Spear-phishing" (sending an email attachment or link to infect a device) is the most common. **Mitigation:** Education and training on threats and types of targeted information; conducting phishing campaign assessment.
- Information Operations** include propaganda, disinformation, etc., to manipulate public perception. Methods include leaking stolen information, spreading false information, amplifying divisive content, and/or interrupting service. **Mitigation:** Clear and consistent information including accurate cybersecurity terminology; relationship building with the media and open dialog with the public.
- Hacking** refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access. **Mitigation:** Incident response planning, penetration testing, two factor authentication, recovery planning, active system monitoring and current security updates, along with physical security measures.
- Distributed Denial of Service (DDoS)** attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access with excessive traffic, causing the service to crash. **Mitigation:** Business continuity and incident response planning, anti-virus software and firewall, good security practices for distributing email address and email filters.
- Insider Threat** is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes. **Mitigation:** Background checks for all election workers and contractors, insider threat training, vigorous chain-of-custody records, strict access controls based on need and updated as access needs change.

Definitions from The State and Local Election Cybersecurity Playbook / Defending Digital Democracy (www.belfercenter.org/D3P)

Recognizing and Reporting an Incident

Definition of an Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (NIST Pub. 800-61).

If you suspect a Cybersecurity Incident has occurred, contact—

- New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), 1-833-4-NJCCIC or NJCCIC@cyber.nj.gov
- National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870 or NCCIC@hq.dhs.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or soc@cisecurity.org

In the event of a Data Breach, notify—

- NJCCIC, 1-833-4-NJCCIC or databreach@cyber.nj.gov

For Additional Information or Questions

- New Jersey Division of Elections:** elections.nj.gov or njelections@sos.nj.gov
- U.S. Cybersecurity and Information Security Agency:** www.dhs.gov/cisa/election-security
- Rich Richard, Region II Cybersecurity Advisor, richard.richard@hq.dhs.gov
- John Durkin, Region II Director for Infrastructure Protection, ipregion2outreach@hq.dhs.gov

State Overview



Election Districts: 6,348
Registered Voters: 6,052,483 (as of August 16, 2019)
Website: elections.nj.gov

2020 Activities Checklist

- Initiative 1:** Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.cisecurity.org/ei-isac-registration.
- Initiative 2:** Install Albert intrusion detection system to monitor the statewide voter registration database.
- Initiative 3:** Conduct a free Vulnerability Scanning (formerly known as Cyber Hygiene scanning) through DHS of internet-accessible systems for known vulnerabilities.
- Initiative 4:** Perform a free Risk and Vulnerability Assessment through DHS to receive risk-prioritized actionable remediation recommendations.
- Initiative 5:** Conduct a free Phishing Campaign Assessment through DHS to evaluate susceptibility to phishing emails.
- Initiative 6:** Conduct physical and cyber security assessment.
- Initiative 7:** Update Continuity of Operations Plan (COOP) for elections.
- Initiative 8:** Participate in an election-related exercise, including the DHS' National Election Cyber Exercise and the NJ Statewide Election Security & Preparedness Tabletop Exercise.