## 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.

### Post-Election Safeguards
- Election Results Tally
  - 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.

### Information Operations
- Include propaganda, disinformation, etc., to manipulate public perception.
- Methods include leasing stolen information, spreading false information, amplifying divisive content, and/or intimidating service.

### 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.

### Insider Threat
- Refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access.

### Hacking
- Refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access.

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

### Insider Threat
- Military operations, protective security or vetting, and/or background checks for all election workers and contractors.

### Hacking
- Related 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.

## For Additional Information or Questions
- New Jersey Division of Elections: elections.nj.gov
- U.S. Cybersecurity and Information Security Agency: www.dhs.gov/cisa/election-security
  - Rich Richard, Region II Cybersecurity Advisor, richard.richard@dhs.gov
  - John Durkin, Region II Director for Infrastructure Protection, john.durkin@dhs.gov

---

## Threat Mitigation

### 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. 800-41).

#### If you suspect a Cybersecurity Incident has occurred, contact—
- New Jersey Cybersecurity and Communications Integration Cell (NJCICC), 609-657-0800 or njcicc@nj.gov
- National Cybersecurity and Communications Integration Center (NCCIC), (888) 252-0870 or nccic@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—
- NJCICC, 609-657-0800 or njcicc@nj.gov
- NCCIC, 1-888-4-NCCIC or nccic@dhs.gov

## State Overview

<table>
<thead>
<tr>
<th>Election Districts: 6,348</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Voters: 6,052,483 (as of August 16, 2019)</td>
</tr>
<tr>
<td>Website: elections.nj.gov</td>
</tr>
</tbody>
</table>

## 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 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 assessments.
- **Initiative 7:** Update Continuity of Operations Plan (COOP) for elections.
- **Initiative 8:** Participate in an election-related exercise, including the DHS’ National Cyber Exercise and the NJ Statewide Election Security & Preparedness Tabletop Exercises.