**Election Day Safeguards**

- **Voters Checked In**
  - Voters are matched to precinct register and present identification at the time of voting.
  - Voter registration lists are available.
  - Questioned ballot voting protects a voter’s right to vote.
- **Voters Cast Ballots**
  - Voters use either paper ballots or if using a voting tablet, a paper ballot is printed of each voter's ballot for verification before casting.
  - The paper or printed ballot is the official record.
  - Absentee and Questioned ballots are tracked and kept in a secure location.

**Post-Election Safeguards**

- **Ballots Used to cast votes on Election Day at polling places are accounted for at the precinct level. Absentee and questioned ballots are reviewed by a bipartisan board to determine voter’s eligibility before the ballots are counted.**
- **Results are not certified until auditing is complete at the State level and shows no discrepancies.**

**State Election Data**

- **Precincts:** 401
- **Active Voters:** 595,387 (as of June 2022)
- **Election Day Results:**
  - Vote Counting Processes: Precinct
  - Touch Screen Voting Tablet
  - Voter Verified Paper Audit Trail
  - Hand Count
- **Website:** [www.elections.alaska.gov](http://www.elections.alaska.gov)

**2022 Initiatives Checklist**

1. **Initiative 1:** Implement Intrusion Prevention Systems (IPS) for the Online Voter Registration System (OLVR) and Online Absentee Ballot Application (OABA).
2. **Initiative 2:** Employ communication encryption tools and practices to reduce risk of losing voter data during transmission.
3. **Initiative 3:** Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at [learn.cisecurity.org/ei-isac-registration](http://learn.cisecurity.org/ei-isac-registration).
4. **Initiative 4:** Conduct a vulnerability scan, such as CISA’s free Cyber Hygiene Scanning.
5. **Initiative 5:** Hold cybersecurity trainings, including training on phishing, email, and web browsing security, for all State employees.
6. **Initiative 6:** Conduct logic and accuracy testing of voting machines.

**For Additional Information or Questions**

- **Alaska Division of Elections:** Gail Furutani, Director of Elections, (907) 465-4611, gail.furutani@alaska.gov
- **Cybersecurity and Infrastructure Security Agency:** [www.cisa.gov/election-security](http://www.cisa.gov/election-security)
- **Mark Breunig, Region X Cybersecurity Advisor:** mark.breunig@cisa.dhs.gov
- **Patrick Massey, Region X Director for Infrastructure Protection:** patrick.massey@alaska.gov
- **Thomas Koloski, Region X Protective Security Advisor:** thomas.koloski@cisa.dhs.gov

---

**2022 Election Security Planning Snapshot**

**State of Alaska**

**SAFEGUARDS / RESILIENCY MEASURES**

<table>
<thead>
<tr>
<th>Alaska Election Process</th>
<th>Threat Mitigation</th>
<th>2022 Election Initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre-Election Activities</strong></td>
<td><strong>Specific Threats / Mitigations</strong></td>
<td><strong>2022 ELECTION INITIATIVES</strong></td>
</tr>
<tr>
<td>Voters Registered</td>
<td>Social Engineering refers to bad actors who manipulate their target into performing a given action or divulging certain information (often a login or password). &quot;Phishing&quot; (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.</td>
<td><strong>Initiative 1:</strong> Implement Intrusion Prevention Systems (IPS) for the Online Voter Registration System (OLVR) and Online Absentee Ballot Application (OABA).</td>
</tr>
<tr>
<td>Election Officials</td>
<td>Information Operations include propaganda, disinformation, etc., to manipulate public perception. Methods include leaking stolen information, spreading false information, amplifying divisive content, and/or disrupting service. Mitigation: Clear and consistent information, including accurate cybersecurity terminology, relationship building with the media, open dialogue with the public.</td>
<td><strong>Initiative 2:</strong> Employ communication encryption tools and practices to reduce risk of losing voter data during transmission.</td>
</tr>
<tr>
<td><strong>Election Day Activities</strong></td>
<td>Hacking: refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access. Mitigation: Incident response and recovery planning, penetration testing, strong passwords and two-factor authentication, especially for admin access; encrypted password storage and transmission; active system monitoring; current security updates; upgrades to supported OS and applications; physical security measures.</td>
<td><strong>Initiative 3:</strong> Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at <a href="http://learn.cisecurity.org/ei-isac-registration">learn.cisecurity.org/ei-isac-registration</a>.</td>
</tr>
<tr>
<td><strong>Post-Election Activities</strong></td>
<td>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 addresses; email filters.</td>
<td><strong>Initiative 4:</strong> Conduct a vulnerability scan, such as CISA’s free Cyber Hygiene Scanning.</td>
</tr>
</tbody>
</table>

**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).

**Mitigation:**
- Alaska Office of Information Technology: (907) 465-2230 or [ocuisupport@alaska.gov](mailto:ocuisupport@alaska.gov).
- Cybersecurity and Infrastructure Security Agency (CISA): (888) 282-0870 or [cisa@nasac.nhs.mil](mailto:cisa@nasac.nhs.mil).
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or [sec@isac.org](mailto:sec@isac.org).

**For Additional Information or Questions**

- **Alaska Division of Elections:** Gail Furutani, Director of Elections, (907) 465-4611, [gail.furutani@alaska.gov](mailto:gail.furutani@alaska.gov).
- **Cybersecurity and Infrastructure Security Agency:** [www.cisa.gov/election-security](http://www.cisa.gov/election-security).
- **Mark Breunig, Region X Cybersecurity Advisor:** [mark.breunig@cisa.dhs.gov](mailto:mark.breunig@cisa.dhs.gov).
- **Patrick Massey, Region X Director for Infrastructure Protection:** [patrick.massey@alaska.gov](mailto:patrick.massey@alaska.gov).
- **Thomas Koloski, Region X Protective Security Advisor:** [thomas.koloski@cisa.dhs.gov](mailto:thomas.koloski@cisa.dhs.gov).

---

**Developed by the Alaska Division of Elections**

**With Support from the Cybersecurity and Infrastructure Security Agency**

**#TrustedInfo2022**