2020 Election Security Planning Snapshot
State of Alaska

SAFEGUARDS / RESILIENCY MEASURES

Alaska Election Process

Pre-Election Activities
- Voters Registered
- Voters Checked In
- Ballots 
- Tabulated
- Election Results Tallied

Election Day Activities
- Voters Cast Ballots
- Voting Tablets
- Results Communicated in a Secure Manner

Post-Election Activities
- Election Results Certified

Pre-Election Safeguards
- Voters Registered
  - Alaska’s Online Voter Registration System (OLVR) is protected by firewalls and Intrusion Prevention Systems (IPS).
  - Access Control listing (whitelisting) and two-factor authentication restrict access to OLVR database.
- OLVR database backups and contingency plans in place to recover corrupted data.
- Election officials receive cybersecurity training and follow strict security protocol.

Election Day Safeguards
- Voters Checked In
  - Voters either matched to precinct register or present proof of voting eligibility.
- Backup voter registration lists are available.
- Fairball measures protect voter’s right to vote.
- Voters Cast Ballots
  - Voters use either paper ballots or voting tablets to cast ballots.
  - Ballots print each voter’s ballot for verification before casting.
  - The paper or printed ballot is the official record.
  - Absence of ballots tracked and kept in a secure location.
- Voting, Tabulating, & Reporting Systems
  - Voting system creates verifiable paper audit trails and is not connected to the internet.
  - Independent functionality and thorough logic and accuracy testing on all equipment before each election.
  - Hash code verification performed on vote tabulation system to meet National Institute of Standards and Technology (NIST) standards and protect against tampering.
  - Intrusion detection processes and practices quickly notify election officials of what within the voting system was compromised.
  - Physical security measures ensure voting system integrity.

Post-Election Safeguards
- Election Results Tallied
  - 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 bi-partisan board to determine voter’s eligibility before the ballots are counted.
  - Election results are not certified until auditing is complete and shows no discrepancies.
- State Ballot Review Board selects and conducts an audit on one precinct that accounts for at least 5% percent of the votes cast in the district to ensure accuracy.

Election Day Security Guidelines
From Alaska’s Statutes Title 15
All official ballots, voting materials, and tabulation equipment is kept secure by the election officials in accordance with law.

TREATMENT / MITIGATION

Specific Threats / Mitigations

- 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. Includes stealing state information, spreading false information, distributing disinformation, and/or disrupting public service. Mitigation: Clear and consistent information, including accurate cybersecurity terminology; relationship building with the media; open dialogue with the public.
- Hacking refers to attacks that exploit or manipulate a target system to obtain 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; application system monitoring; current security updates; updates to supported OS and applications; physical security measures.

State Election Data

2020 Initiatives Checklist

Initiative 1: Implement Intrusion Prevention Systems (IPS) for the Online Voter Registration System (OLVR).
Initiative 2: Employ communication encryption tools and practices to reduce risk of losing voter data during transmission.
Initiative 4: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.cisecurity.org/ea-isac-registration.
Initiative 5: Conduct a vulnerability scan, such as CISA’s free Cyber Hygiene Scanning.
Initiative 6: Hold cybersecurity trainings quarterly, including training on phishing, email, and web browsing security, for all State employees.
Initiative 7: Conduct logic and accuracy testing of voting machines.

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

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

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—
- Alaska Office of Information Technology (907) 465-2220 or @hotspot@alaska.gov
- Cybersecurity and Infrastructure Security Agency (CISA), (888) 282-0870 or @cisa@alaska.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or cisco@eisecurity.org

For Additional Information or Questions

Cybersecurity and Infrastructure Security Agency: www.cisa.gov/election-security
- Ron Watts, Region X Cybersecurity Advisor, rwatts@cisecurity.gov
- Patrick Massey, Region X Director for Infrastructure Protection, pmassey@cisecurity.gov
- Tom Wilder, Region X Protective Security Advisor, twilder@cisecurity.gov

Mitigation:
Clear and consistent information, including accurate cybersecurity terminology; relationship building with the media; open dialogue with the public.

If you suspect a Cybersecurity Incident has occurred, contact—
- Alaska Office of Information Technology, (907) 465-2220 or hotspot@alaska.gov
- Cybersecurity and Infrastructure Security Agency (CISA), (888) 282-0870 or cisa@alaska.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or cisco@eisecurity.org

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

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—
- Alaska Office of Information Technology, (907) 465-2220 or hotspot@alaska.gov
- Cybersecurity and Infrastructure Security Agency (CISA), (888) 282-0870 or cisa@alaska.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or cisco@eisecurity.org

State Election Data

2020 Initiatives Checklist

Initiative 1: Implement Intrusion Prevention Systems (IPS) for the Online Voter Registration System (OLVR).
Initiative 2: Employ communication encryption tools and practices to reduce risk of losing voter data during transmission.
Initiative 4: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.cisecurity.org/ea-isac-registration.
Initiative 5: Conduct a vulnerability scan, such as CISA’s free Cyber Hygiene Scanning.
Initiative 6: Hold cybersecurity trainings quarterly, including training on phishing, email, and web browsing security, for all State employees.
Initiative 7: Conduct logic and accuracy testing of voting machines.

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

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—
- Alaska Office of Information Technology, (907) 465-2220 or hotspot@alaska.gov
- Cybersecurity and Infrastructure Security Agency (CISA), (888) 282-0870 or cisa@alaska.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or cisco@eisecurity.org

For Additional Information or Questions

Cybersecurity and Infrastructure Security Agency: www.cisa.gov/election-security
- Ron Watts, Region X Cybersecurity Advisor, rwatts@cisecurity.gov
- Patrick Massey, Region X Director for Infrastructure Protection, pmassey@cisecurity.gov
- Tom Wilder, Region X Protective Security Advisor, twilder@cisecurity.gov

Knowing your assigned role is a key component of a well-developed Incident Response Plan (IRP). Your role may include activities such as: reporting an incident, acting as an incident manager, or serving on a cross-functional team. The IRP should be written in a way that is accessible and easily understood by all team members. A well-written plan can help ensure that everyone knows what to do when an incident occurs and that the organization is better equipped to mitigate the impact of an attack.