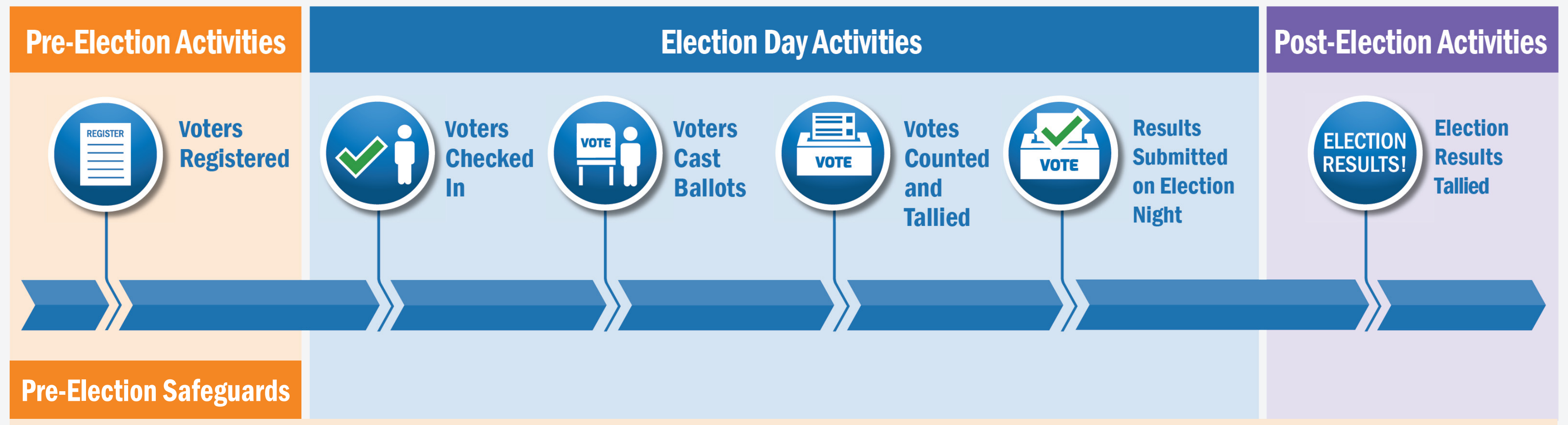
2020 Election Security Planning Snapshot
State of Alaska

SAFEGUARDS / RESILIENCY MEASURES

Alaska Election Process



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 are either matched to precinct register or present proof of voting eligibility.
- Backup voter registration lists are available.
- Failsafe measures protect voter's right to vote.

Voters Cast Ballots

- Voters use either paper ballots or voting tablets to cast ballots.
- Voting tablets print each voter's ballot for verification before casting.
- The paper or printed ballot is the official record.
- Absentee ballots tracked and kept in a secure location.

Voting, Tallying, & 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 then 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.

THREAT 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. 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; open dialogue with the public

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

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

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—

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

For Additional Information or Questions

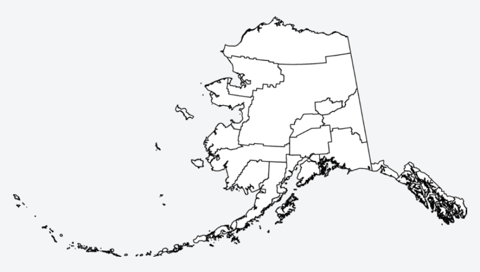
Alaska Division of Elections: Gail Fenumiai, Director of Elections, (907) 465-4611, gail.fenumiai@alaska.gov

Cybersecurity and Infrastructure Security Agency: www.cisa.gov/election-security

- Ron Watters, Region X Cybersecurity Advisor, ronald.watters@cisa.dhs.gov
- Patrick Massey, Region X Director for Infrastructure Protection, ipregion10outreach@cisa.dhs.gov
- Tom Wilder, Region X Protective Security Advisor, thomas.wilder@cisa.dhs.gov

2020 ELECTION INITIATIVES

State Election Data



Precincts: 441

Active Voters: 585,377 (as of June 2020)

Ballot Counting Processes: Optical Scan Units, Direct-Recording Electronic Touch Screen Units, Hand Count

Website: www.elections.alaska.gov

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 3:** Attend CISA's Tabletop the Vote 2020: National Election Cyber Virtual Tabletop Exercise.

☑ **Initiative 4:** Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.cisecurity.org/ei-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.

#TRUSTEDINFO2020
Election Officials are your trusted sources for election information

DEVELOPED BY THE ALASKA DIVISION OF ELECTIONS
WITH SUPPORT FROM THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

#PROTECT2020
CISA.gov