SAFEGUARDS / RESILIENCY MEASURES

THREAT MITIGATION

2018 ELECTION INITIATIVES

2018 Election Cybersecurity Planning Snapshot
State of Alaska

Alaska Election Process

Pre-Election Safeguards

Election Officials will ensure the physical security of tabulation equipment and software.

Post-Election Safeguards

OLVR database backups and contingency plans in place to recover corrupted data.

Voting, Tallying, & Reporting Systems

Voting, tallying, and reporting systems

Pre-Election Activities

Election Officials receive cybersecurity training and follow strict security protocol.

Election Day Safeguards

Voters who signed in at the polling place.

Election Results Tallied

Election results are not certified until auditing is complete and shows no discrepancies.

Election Officials receive cybersecurity training and follow strict security protocol.

State Election Data

Precincts: 441
Active Voters: 569,940 (as of October 2018)
Ballot Counting Processes: Optical Scan Units, Direct-Recording Electronic Touch Screen Units, Hand Count
Website: www.elections.alaska.gov

Election Day Safeguards

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

Executive Order 31

Intrusion detection processes and practices quickly notify election officials of what within the voting system was compromised.

Voters Cast Ballots

• Touch screen units print each voter's ballot for verification before casting.
• The paper or printed ballot is the official record.

Post-Election Safeguards

• Absentee ballots tracked and kept in a secure location.

Defining terms:

• Pre-Election Activities: activities before an election.
• Election Day Activities: activities on Election Day; activities occurring during Election Day.
• Post-Election Activities: activities after an election.

Election Day Security Guidelines

Voting, tallying, and reporting systems

• Voting system creates verifiable paper audit trails and is not connected to the internet.
• Independent and thorough logic, functionality, 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.

Confidentiality

Physical security measures ensure voting system integrity.

Electronic Voter Registration System (OLVR)

The OLVR database is protected by firewalls and Intrusion Prevention Systems (IPS).

For Additional Information or Questions

Alaska Division of Elections: Josie Bahne, Director of Elections, (907) 466-4611 elections@alaska.gov
Ron Walters, Region X Cybersecurity Advisor, ron.walters@dhs.gov
Patrick Massay, Region X Director for Infrastructure Protection, massay.p@hq.dhs.gov
Tom Wilder, Region X Protective Security Advisor, tom.wilder@hq.dhs.gov

2018 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: Hold cybersecurity table-top exercise for election staff.

Initiative 4: Attend DHS’s Tabletop the Vote 2018 National Election Cyber Exercise.

Initiative 5: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.esiscy.org/ei-isac-registration

Initiative 6: Conduct a vulnerability scan, such as DHS’s free Cyber Hygiene Scanning.

Initiative 7: Hold cybersecurity trainings quarterly, including training on phishing, email, and web browsing security, for all State employees.

SAFEGUARDS

Pre-Election Activities: activities before an election.

Election Day Activities: activities on Election Day; activities occurring during Election Day.

Post-Election Activities: activities after an election.

Election Day Safeguards

Voters are either matched to precinct register or present proof of voting eligibility.

Election Results Tallied

Election results are not certified until auditing is complete and shows no discrepancies.

Post-Election Safeguards

OLVR database backups and contingency plans in place to recover corrupted data.

Voting, Tallying, & Reporting Systems

Voting, tallying, and reporting systems

Pre-Election Activities

Election Officials receive cybersecurity training and follow strict security protocol.

Election Day Safeguards

Voters are either matched to precinct register or present proof of voting eligibility.

Executive Order 31

Intrusion detection processes and practices quickly notify election officials of what within the voting system was compromised.

Voters Cast Ballots

• Touch screen units print each voter's ballot for verification before casting.
• The paper or printed ballot is the official record.

Post-Election Safeguards

• Absentee ballots tracked and kept in a secure location.

Defining terms:

• Pre-Election Activities: activities before an election.
• Election Day Activities: activities on Election Day; activities occurring during Election Day.
• Post-Election Activities: activities after an election.

Election Day Security Guidelines

Voting, tallying, and reporting systems

• Voting system creates verifiable paper audit trails and is not connected to the internet.
• Independent and thorough logic, functionality, 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.

Confidentiality

Physical security measures ensure voting system integrity.

Electronic Voter Registration System (OLVR)

The OLVR database is protected by firewalls and Intrusion Prevention Systems (IPS).

For Additional Information or Questions

Alaska Division of Elections: Josie Bahne, Director of Elections, (907) 466-4611 elections@alaska.gov
Ron Walters, Region X Cybersecurity Advisor, ron.walters@dhs.gov
Patrick Massay, Region X Director for Infrastructure Protection, massay.p@hq.dhs.gov
Tom Wilder, Region X Protective Security Advisor, tom.wilder@hq.dhs.gov

2018 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: Hold cybersecurity table-top exercise for election staff.

Initiative 4: Attend DHS’s Tabletop the Vote 2018 National Election Cyber Exercise.

Initiative 5: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.esiscy.org/ei-isac-registration

Initiative 6: Conduct a vulnerability scan, such as DHS’s free Cyber Hygiene Scanning.

Initiative 7: Hold cybersecurity trainings quarterly, including training on phishing, email, and web browsing security, for all State employees.