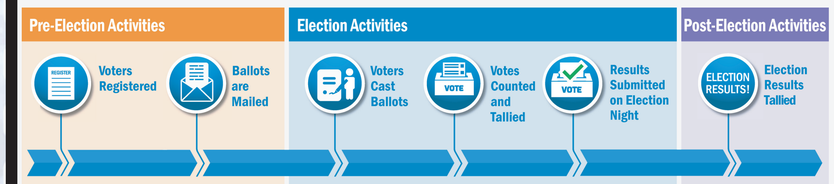
2018 Election Cybersecurity Planning Snapshot
Pierce County

SAFEGUARDS / RESILIENCY MEASURES

Washington Election Process



The Voter Registration Database (VRDB) and results reporting systems are secured by highly skilled Office of the Secretary of State (OSOS) IT staff, using state of the art equipment and following IT industry best practices.

Network Security
- Voter Registration database is protected by firewalls and Intrusion Prevention Systems (IPS).
- Only authorized Internet Protocol (IP) system access.
- Network that is only used by authorized partners and servers isolated on network demilitarized zone (DMZ).

Physical Security
- Secure single tenant modern facility with dual redundant alarms, security cameras, and FM200 protection.
- Access restricted to 3 authorized OSOS IT staff members.
- Data center located next door to police station.

Log Review
- Firewall logs reviewed 4 times a day and system event logs reviewed twice a day.

Security Audit
- Regular security scans by OSOS IT staff and periodic 3rd party scans to test/verify firewalls, IPs, and servers.

Election Safeguards

Verification
- Verification of signatures on ballot envelopes.
- Voter signature is compared to voter's registration record.
- Failsafe measures protect voter's right to vote.

Voters Cast Ballots
- Votes are cast on human readable paper ballots and tabulated electronically. The paper ballot is the official record.
- Ballots are kept in secure location.

Voting, Tallying, & Reporting Systems
- County-specific security protocols in formalized policy.
- Counties conduct logic and accuracy tests before each election. Tests are open to public observation.
- Voting systems are not connected to the internet.
- Security measures to ensure physical security and detect inappropriate access (WAC 434-261-045).
- County maintains continuity of operations (COOP) plans and participated in DHS's Cyber Resilience Review (CRR).

Post-Election Safeguards

Election Results Site
- Hosted in Microsoft Azure cloud with server & geographic redundancy.
- Results data retrieved from secure location provided by results reporting system at specified times (intervals).
- Parsed and presented to users in read-only and compact web files (HTML).
- Graphic representation of results not connected to results reporting system or network after data transmittal.

Election Results Tallied
- Results are unofficial until the canvass of votes.
- Canvass compares printed report from precincts to number of ballots scanned before certifying results as official.
- Vigorous chain of custody records maintained.
- Post-election audit preformed on random selection of all precincts.

THREAT MITIGATION

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. ***Mitigation:*** Education and training on threat and types of targeted information. Washington participated in DHS vulnerability assessment on social engineering

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 and open dialog with the public

Hacking refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access. ***Mitigation:*** Incident response planning; penetration testing (DHS RVA); two-factor authentication; recovery planning; active system monitoring; up-to-date security updates along with 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:*** Maintain organization's essential functions through business continuity plan and implementing a security incident response plan

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—
- Washington Security Operations Center, SOC@sos.wa.gov, 509-235-7500 ext. 711
- National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870 or NCCIC@hq.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 impacting more than 500 people, notify—
- Washington State Office of the Attorney General, securitybreach@atg.wa.gov

For Additional Information or Questions

Washington Secretary of State's Office: Lori Augino, Director of Elections, lori.augino@sos.wa.gov

U.S. Department of Homeland Security: www.dhs.gov/topic/election-security
- Ron Watters, Region X Cybersecurity Advisor, ronald.watters@hq.dhs.gov
- Patrick Massey, Region X Director for Infrastructure Protection, patrick.massey@hq.dhs.gov

2018 ELECTION INITIATIVES

Pierce County Overview

Precincts: 518
Active Voters: 484,111
Voting System/Model: ClearBallot
Accessible Voting Unit: ClearAccess
COOP: Yes
Website: piercecountyelections.org

2018 Activities & Timeline Checklist

Initiative 1: Completion of DHS Risk Vulnerability Assessment (RVA)
(Target Completion: June 2018)

Initiative 2: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.cisecurity.org/ei-isac-registration
(Target Completion: July 2018)

Initiative 3: Schedule Cyber Hygiene Scanning. Contact nccicustomerservice@hq.dhs.gov and reference "Washington Cyber Hygiene Initiative" to obtain this service free through DHS
(Target Completion: August 2018)

Initiative 4: Conduct a Phishing Campaign Assessment. Contact nccicustomerservice@hq.dhs.gov and reference "Washington Phishing Campaign Assessment" to obtain this service free through DHS
(Target Completion: September 2018)

Initiative 5: Formation of the Office of Secretary of State Security Operations Center
(Target Completion: October 2018)

Initiative 6: Addition of Albert monitoring system for each county
(Target Completion: January 2019)

Revised as of October 2, 2018