OFFICE OF THE SECRETARY OF STATE

BEV CLARNO
SECRETARY OF STATE

A. RICHARD VIAL
DEPUTY SECRETARY OF STATE

ELECTIONS DIVISION
STEPHEN TROUT
DIRECTOR

255 Capitol Street NE
Salem, Oregon 97310
Information (503) 986-1518

Fax 503-373-7414
sos.oregon.gov/elections

Election Security Report

September 2019

To protect the integrity of Oregon's elections and other systems, The Office of Oregon Secretary of State (SOS) has multiple layers of defense controls in place, including hardware and software designed to prevent cybercriminals from gaining access or misusing our systems. We closely monitor our systems for suspicious activity and frequently test for vulnerabilities. We also routinely train and remind all staff how to appropriately handle email and other threats in order to prevent unauthorized access or tampering.

More specifically, we have programs, policies, and plans in place to address and mitigate the unlikely event of a breach and stop any potential damage. We work with partners such as the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED), and others to ensure we are implementing the best practices in protecting our elections and their supporting systems.

Routinely approximately 28 million attempts per day are blocked from reaching systems and information, including our elections systems. We utilize Defense in Depth with administrative, technical and managerial security controls. Layers of security provide multiple ways of examining activity attempting to access or accessing systems. Any successful access of systems has typically been reviewed by multiple security systems prior to access.

We routinely perform threat analysis and risk assessments on our systems. Assessments are done by internal staff as well as third parties contracted to perform assessments. As a result of these assessments, we continue to improve security processes and protections for all systems.

We use preventative and detection measures including:

- Patch and vulnerability management
- Firewalls
- Continuous monitoring of systems
- Incident management planning and tools
- Security training

Over the past year we increased our security efforts with respect to elections. We completed:

- Upgraded network firewalls
- Requiring a VPN to access the SOS network remotely
- Upgraded antimalware solution with enhanced monitoring and alerting for unusual activity
- A third party risk assessment, including controls assessment, physical security testing, social engineering testing, and network penetration testing
- Third party penetration testing of ORESTAR
- Upgraded log collection and monitoring system to handle increased amounts of system and application data in order to increase our visibility and understanding of system activity.
- Nearly doubled the amount of security dashboards used to monitor and audit security data from the SOS network and systems.
- Mitigated identified application security vulnerabilities
- Provided Oregon Counties secured upload platforms from which to transfer SOS Elections data.

We also work closely with federal partners at the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). In partnership we developed a cybersecurity tabletop exercise focused on Oregon's vote by mail process for Oregon's 36 counties at their annual summer conference. Election and IT representatives from the counties participated in the exercise and then shared best practices. Additionally, our Protective Security Advisor-Oregon District from CISA and DHS is conducting security assessments at each of Oregon's 36 county election offices.

We created an Oregon TIGER Team (Threat Information Gathering and Election Resources). The TIGER team is made up of representatives from the Oregon Elections Division, Oregon Office of Emergency Management, Enterprise Security Office in the Oregon CIO's Office, Oregon National Guard, FBI, and at the federal level DHS and CISA. We meet regularly to share information, coordinate activities, and plan and prepare for threats.

All 36 Oregon counties are members of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). The EI-ISAC was established to support the cybersecurity needs of the elections subsector. Through the EI-ISAC, election agencies gain access to an elections-focused cyber defense suite, including sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices.

Security systems are never finished and need to continue to be improved and modernized. We continue to evaluate and make improvements. We are currently implementing:

- Inspection of encrypted traffic

- Network access control – detection and blocking of unauthorized devices attempting to access the SOS network.
- Ongoing phishing campaigns to test and educate staff.
- Ongoing testing and scanning for application security vulnerabilities

We are also in the planning phase of the following projects that will be completed before the 2020 Primary Election:

- Multi-factor authentication for county elections staff
- Election system disaster recovery
- Increased monitoring and log collection for OCVR
- Install agents on high value targets' workstations to collect and forward log data. This includes workstations for security, information systems, and elections staff, as well as management.

We will continue efforts to protect the integrity of our elections. We successfully blocked attempted cyber-attacks by the Russian Government in 2016 and our systems today are much more robust than those systems in place in 2016. We will continue our efforts to secure our election and other systems and implement best practices as we continue forward in this battle.