Oregon Secretary of State

Information Technology Security Report

Mary Krehbiel, Chief of Strategic Initiatives

Chris Molin, Director of Information Systems Division

Dan Thiems, Chief Information Security Officer

SOS Information Security Program

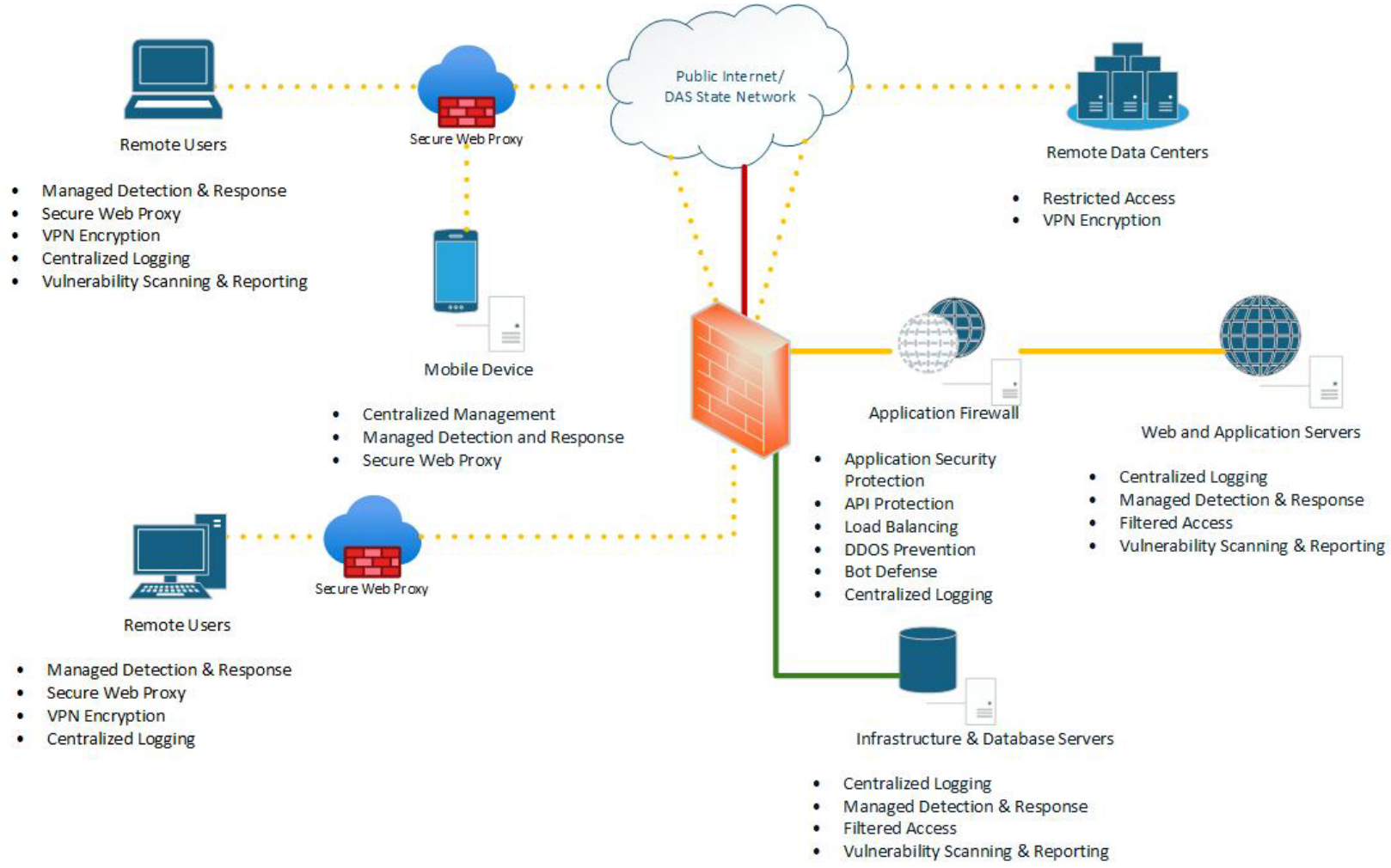
Mission Statement

"Protecting the Work of the Oregon Secretary of State's Office and the People it Serves Through Strong Cybersecurity."

Top Risks in Cybersecurity 2025

- **State-Sponsored Threats and GeoPolitical Risks**
  - Increase State-sponsored physical and cyberattacks on critical infrastructure
  - Mis- and disinformation campaigns
- **AI – Offensive and Defensive Uses**
  - Cybercriminals leveraging AI for phishing, automation, deepfakes, and bypassing security control
- **Cyber Hygiene and Basic Security Controls**
  - Unpatched vulnerabilities and weak credentials
  - Misconfigurations and unused services
  - Shadow IT makes it difficult to enforce security policies and increase attack surface.
- **Legacy Systems and Technical Debt**
  - Relying on older infrastructure due to operational and financial constraints
  - Inability to patch legacy systems and relying on compensating controls that increase complexity and risk.
- **Workforce & Talent Scarcity**
  - Shortage of skilled cybersecurity professionals remains acute.
  - Scarcity of trained cybersecurity professionals
  - Insufficient automation
- **Third-Party & Supply Chain Risk**
  - Attacks targeting vendors as weak links
  - Large attack surface and complex vendor ecosystems

High Level Diagram of SOS Environment



Audits & Assessments

Current Internal Efforts

- Performing regular internal vulnerability scans on infrastructure.
- Scanning web applications, both internal and public facing, for vulnerabilities.
- Ongoing self-assessments of high-value systems to ensure alignment with cybersecurity best practices.

In Progress: Strengthening Assessment Framework

- Identifying and developing a structured assessment model with defined cadence.
- Establishing standards for assessments, including risk scoring, tracking, and post-assessment review.

Strategic Focus Areas

- Formalizing a vulnerability assessment program.
- Preparing to engage with third parties for future independent assessments or penetration tests.
- Aligning internal assessments with NIST 800-53 and CIS Controls to support continuous improvement.

Accomplishments 2024

Workforce is more secure

- Implemented tools to help individuals be secure.
- Deployed MFA and other physical improvements.
- Increased required training on security.

Technology is more secure

- Expanded mobile and hardware policies.
- Updated plans and procedures.
- Applied access limitations and monitoring.

Resilient Security Processes

- Improved reporting and dashboarding.
- Expanded device monitoring.
- Maintained updated documentation and procedures.

Cybersecurity Strategy for 2025

Continued Utilization of CIS Controls to Improve Cybersecurity Posture

Expanding Zero Trust Network Access (ZTNA) Deployment

Formalize Cybersecurity Program with Policies and Procedures

Implement Full Static Code Analysis in CI/CD Pipeline

Oregon Secretary of State

Questions?

Ricardo Lujan Valerio

Deputy Chief of Staff – Government Relations

(503) 779 – 5451 | ricardo.lujanvalerio@sos.oregon.gov