SECRETARY OF STATE

Information Technology Overview

Joint Legislative Committee on Information Management and Technology

May 31, 2023

CIO: Chris Molin
CISO: Dan Thiems

Information Systems Division (ISD) Program Overview

$3,160,199 (GF); $16,863,393 (OF); 42 FTE

- **Application Development**: Develops custom applications for business partners
- **Information Security**: Protects and defends critical infrastructure, applications, and data from all threats
- **Infrastructure Operations**: Operates and maintains all SOS IT infrastructure and systems
- **Service Delivery**: Ensures effective, efficient delivery of technology solutions to business divisions

ISD Partners

Our Internal Partners

- **Chief Elections Officer** ensuring election integrity
- **State Auditor** of public funds ensuring maximum value of tax dollars
- **Chief Business Adv**ocate building a prosperous Oregon economy
- **State Archivist** preserving Oregon public records and shared his

Our External Partners

- County Elections Offices
- State CIO
- State CISO & Security Council
- SOS Trusted Vendors
- E-Gov Boards
- Federal/Local Law Enforcement
- DHS/CISA

SOS Information Security Program

Mission Statement

"Securing and Reducing Cyber Risk for Secretary of State Services provided to Oregonians"

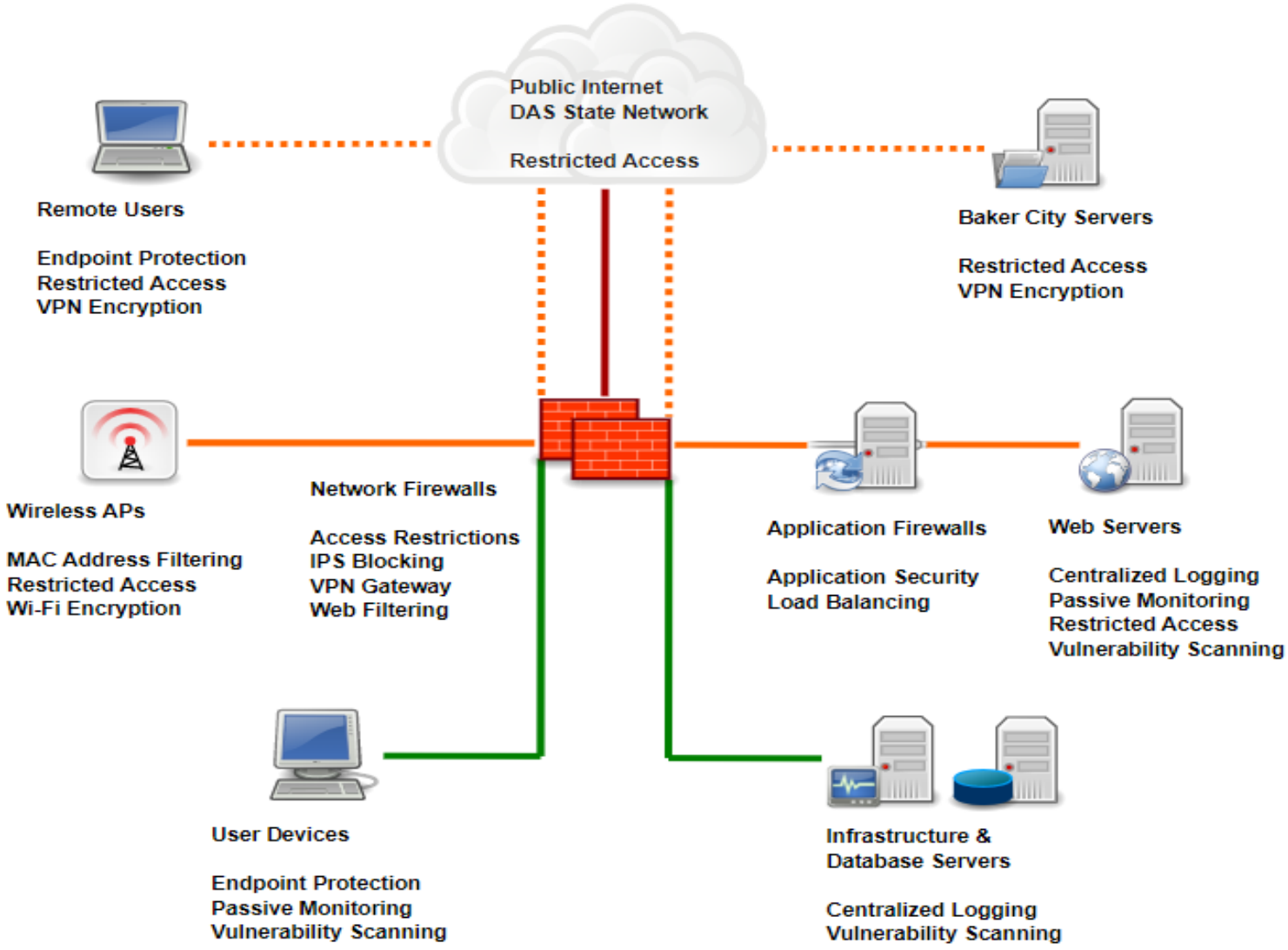
Top Risks in Cybersecurity 2023

February 2023
Bipartisan Policy Center

- **Evolving GeoPolitical Environment**
  - Increase State-sponsored physical and cyberattacks on critical infrastructure
  - Mis- and disinformation campaigns
- **Accelerating Cyber Arms Race**
  - Criminals leveraging consumer technology
  - Attacking human factor strong controls (MFA)
- **Lack of Investment, Preparedness and Resilience**
  - Lack of crisis preparedness, disaster recovery and business continuity planning
  - Vendor and 3rd Party Risk management
  - Poor cyber hygiene and security awareness
- **Vulnerable Infrastructure**
  - Trustworthy operation of essential government services.
  - Unpatched and outdated code and legacy systems.
- **Talent Scarcity**
  - Scarcity of trained cybersecurity professionals
  - Insufficient automation

https://bipartisanpolicy.org/report/top-risks-cybersecurity-2023/ ** Selected points from Report*

High level Diagram of SOS Environment



Audits & Assessments

- Governance, Policy & Training - Ongoing
- Cerium – Information Security Risk Assessment – Dec 2018
- SOS / InfoTech – Guided Risk Assessment – Dec 2019
- FireEye / Mandiant – MAZE Ransomware Assessment – Nov 2020
- Cybersecurity & Infrastructure Security Agency (CISA) – OCVR Assessment – Dec 2020
- CISA – BERI Application Assessment – Jan 2021
- CIS – Nationwide Cybersecurity Review – Current 2023
- CISA – Physical Security Assessment - TBD
- Application Vulnerability Assessment – Apr 2024

Accomplishments 2022

Elections

- Increased monitoring and reporting of Elections and SOS systems (CIS, DHS, Local law enforcements, Albert sensors , 24/7 monitoring)
- Advisory and consulting review of Oregon Votes
- Expanded communications and cyber advisory work with Counties
- Implemented DDOS and Web Application Firewall for Election Night Reporting

Archives

- Physical security improvements

Corporation

- Increased email security protection
- Secured Internet Egov domains

BSD

- Reviewed and updated security procedures

HRD

- Policies review and updates
- Refreshed New Employee and increased security awareness training
- Audit of Sensitive data Access procedures.

Agency

- Enhanced endpoint protection and monitoring
- Mobile Device Management Implementation

Mission Statement

"Securing and Reducing Cyber Risk for Secretary of State Services provided to Oregonians"

Accomplishments 2022 - continued

Executive

- Updated polices and procedures

ISD

- Major security hardware upgrades to existing systems
- Systemic User and Access reviews of all critical systems
- Updated Phishing detection and reporting, and scheduled Phishing campaigns
- Implementations of 8 cybersecurity services to improved and upgrade SOS security posture
- User and access audit review of systems

Cybersecurity Strategy for 2023

- **Utilize CIS Controls to Improve and Update our cybersecurity posture**
  - Continue All CIS Controls across SOS services
  - Asset Management (CIS1/2)
  - Network Infrastructure Management (CIS12):
    - Network Switches
    - Firewall security improvements
    - Web Application Firewall and Load balancer
  - Endpoint protection
  - Configuration and Changing Monitoring (CIS4)
  - Privileged Access Management (CIS 6)
  - Static and Dynamic code scanning solutions (CIS16)
  - Risk Management

- **Top Risks for 2023 response**
  - Improvements to CIS 9 Email/Web browser protections
  - CIS 10 Malware Defenses
  - CIS 14 Security Awareness and Skills training

QUESTIONS?

CHRIS MOLIN, CIO
Information Systems Division,
Oregon Secretary of State
chris.l.molin@sos.oregon.gov

DAN THIEMS, CISO
Information Systems Division,
Oregon Secretary of State
Daniel.Thiems@sos.oregon.gov