Information Technology Overview

Joint Legislative Committee on Information Management and Technology

March 1, 2023

CIO: Chris Molin
CISO: Leo Cuellar
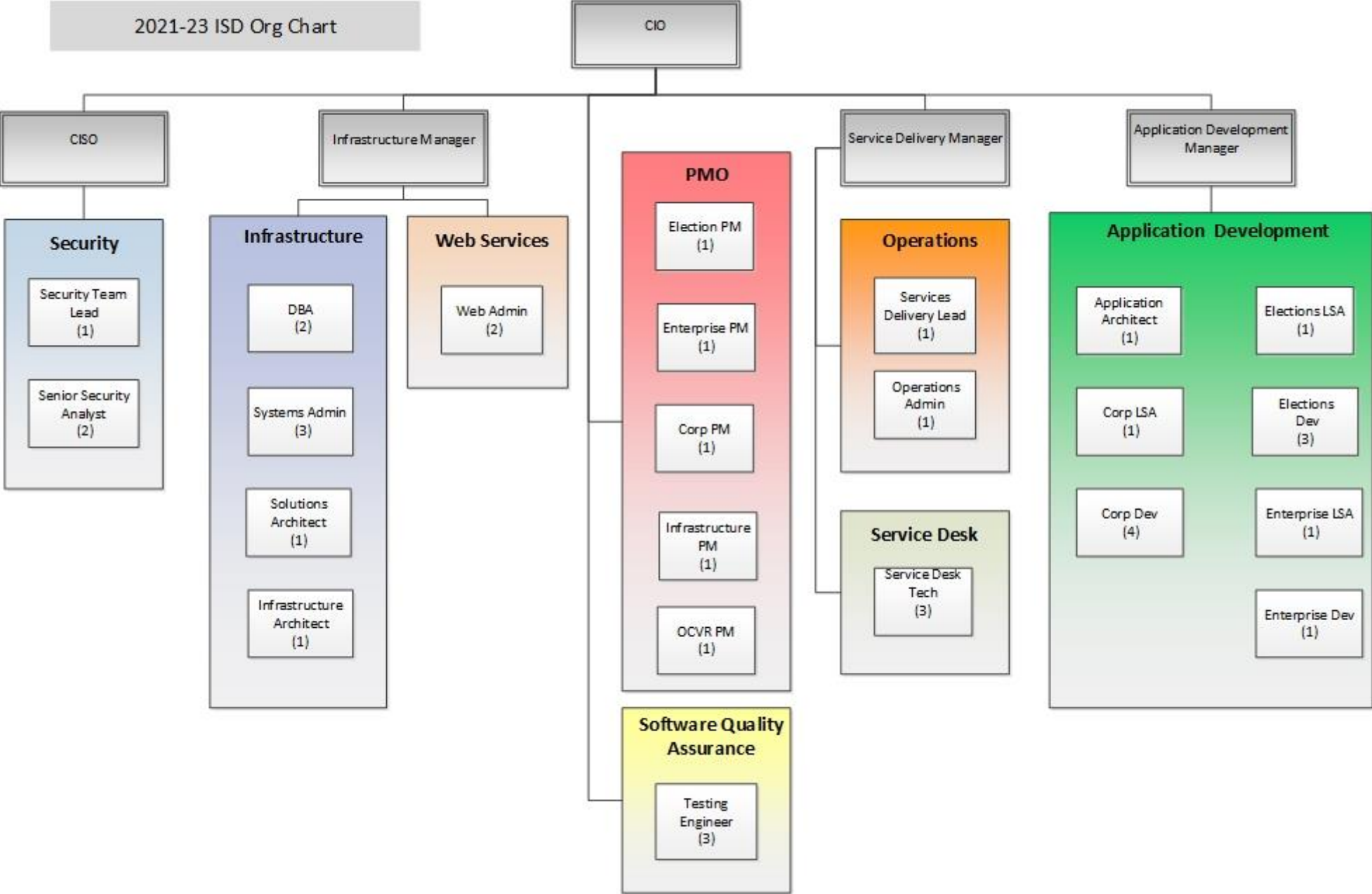
CIO Background

- 30 + years federal, state, and local experience

- 22 Years Federal
  - 8 Years Active-Duty Air Force
  - 14 Years w/ Department of Defense (Civilian)
    - Supporting Fighter Wing, Space Systems, Intelligence, Command and Control, Logistics w/ full-suite of IT services

- 11 Years w/ Oregon State Government
  - Secretary of State and State Treasury

- Appointed to E-Gov Portal Advisory Board (EPAB) and currently serve as Chair

- 3 years Municipal
  - Served on Stayton City Council

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

2021-23 ISD Org Chart

CIO

CISO

Security
- Security Team Lead (1)
- Senior Security Analyst (2)

Infrastructure Manager

Infrastructure
- DBA (2)
- Systems Admin (3)
- Solutions Architect (1)
- Infrastructure Architect (1)

Web Services
- Web Admin (2)

PMO
- Election PM (1)
- Enterprise PM (1)
- Corp PM (1)
- Infrastructure PM (1)
- OCVR PM (1)

Software Quality Assurance
- Testing Engineer (3)

Service Delivery Manager

Operations
- Services Delivery Lead (1)
- Operations Admin (1)

Service Desk
- Service Desk Tech (3)

Application Development Manager

Application Development
- Application Architect (1)
- Corp LSA (1)
- Corp Dev (4)
- Elections LSA (1)
- Elections Dev (3)
- Enterprise LSA (1)
- Enterprise Dev (1)

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
- Oregon Tyler / NIC
- E-Gov Boards
- Federal/Local Law Enforcement
- DHS/CISA

SOS – CUSTOM BUILT APPLICATIONS

ELECTIONS:
- Oregon Votes (OCVR Replacement)
- Election Night Reporting
- Oregon Central Voter Registration
- Oregon Motor Voter
- Oregon Election System for Tracking and Reporting

CORPORATION:
- Oregon Business Registry
- Business Entity Registration Information
- Notary
- Uniform Commercial Code
- Business Information Center

ISD

ARCHIVES:
- Oregon Administrative Rules Database
- Oregon Historical Records Index
- Public Records Search

AUDITS:
- Municipal Filing Application

ADMINISTRATION:
- Deposit Interface System
- Oregon Identity Manager

2022 Major IT Accomplishments

- **Technical Work**:
  - Upgraded server infrastructure OS and VMWare stack
  - Post-pandemic IT support in agency re-opening/consolidation
  - Laptop/PC technology refresh
  - Implemented new website analytics functionality

- **Business/IT Projects**
  - Mis/Dis/Mal-Information Program Rollout
  - Online Certificate of Existence w/ Corporation
  - HB 3021 – Translation Services and Translation Advisory Council Website
  - HB 3291 – Required ballots by mail to have postal indication showing ballot was mailed NLT date of election
  - Archives Oregon Admirative Rules Database Remote Hearings Enhancement
  - File interchange protocol implementation between DMV and Oregon Votes

Current/Major Business and IT-Driven Projects

Agency Priorities	
1	Oregon Votes
2	Server Room HVAC
3	Oracle 19c Upgrade
4	Municipal Filing System Replacement
5	Identity & Access Management
6	Project Portfolio Governance
7	Legacy Hardware Decommission
8	Active Directory Migration
9	Data Categorization and Cleanup Tool
10	Windows 11
11	Core Switch Replacement
12	Continuity of Operations Plan (COOP)

Service Delivery "Health"

- **To establish priorities and initiatives toward a strategy, we needed to better understand our operational pain points and risks.**

  - We conducted a third-party customer service assessment with all our divisions.

  - We also performed a third-party CIO/CXO alignment survey.

  - We developed a business-value scorecard for ideas to approved projects

  - Lastly, we assessed our service catalogue <u>MATURITY</u>, <u>BENCH STRENGTH</u>, and <u>RISK</u>.

Service Delivery "Health" (Example)

Ownership	Service	Maturity	Bench Strength	Risk	Health
AppDev	Requirements	1	1	1	3
Infrastructure	Networking	1	2	3	6
Service Delivery	Change Management	1	2	2	5
CIO	Customer Engagement	3	3	3	9

Green (3-5)	Yellow (5-7)	Red (7-9)

ISD Strategic Goals

- Identify, document, and adapt technical capabilities to support the agency.

- Ensure technology security, resiliency, efficiency, and redundancy.

- Mature information technology governance.

- Overcome critical technical debt.

- Optimize delivery processes.

IT STRATEGIC INITIATIVES

Engage and Inform Partners

- Conduct monthly division leadership meetings
- Define overall communication plan
- Define service levels
- Identify team performance metrics
- Define app vs. Tech ownership

Modernize Architecture and Standards

- Implement enterprise architecture
- Define modernization efforts
- Define Lifecycle management
- Document systems (services & processes)
- Optimize Service Delivery
- Standardise dev toolset

Develop Workforce

- Develop career paths/ mentorship
- Implement cross training strategy
- Create training plans
- Team building

Ensure Technology Security and Resiliency

- Refresh the security strategy
- Implement Infrastructure Modernization Program
- Verify BC & DRP requirements
- Security health check
- Perform individual application risk assessment
- Implement risk management process

Optimize Delivery Process

- Define & enforce PM standards
- Redefine business case & intake process
- Define discretionary and non-discretionary balance with divisions
- Implement PPM

Policy Option Packages 23-25

Package 106 – System Modernization: $356,592 (GF), $2,615,015 (OF)

1. Addresses framework and interface improvements. Focus on user engagement and metrics to assess the effectiveness, usefulness, and accessibility of our data and online services through continuous improvement and a more agile approach to development.

2. Current IT staffing capacity, oversight, and capabilities are insufficient to support delivering targeted internal solutions that serve as adequate rebuilds, or replacements, that can also integrate with various external systems.

3. Roles will be focused on user experience, user interface development, and data management.

Policy Option Packages 23-25

Package 107 – Information Security: $218,211 (GF), $1,600,211 (OF)

1. This package requests $508k to fund permanent OPA3 (Asset Manager) and ISS-5 (Security Analyst) positions. This package also requests $1.3M in services and supplies funding aimed at managing delivery, security, performance, and availability of web applications, as well as monitoring the security of servers, cloud resources, storage devices, and other networking components.

2. This work is a continuation and commitment by our IT team and agency to ensure our systems and the data in our care are secured against an ever-changing threat landscape. Addresses and improves upon our information security planning, documentation, design, and innovation through processes, technology solutions, and new roles focused on our data, our assets, and our networks.

3. Additional roles will provide inventories, analytics, and reporting.

SOS Information Security Program

Mission Statement

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

Leo Cuellar, CISO

- Over **25 years of technical and strategic Information Technology and Cybersecurity experience in various industries and companies**

  - Nike, HP, Starbucks, financial, social media, education and MSSP.

  - Consulting CISO to SLTT in Boise ID area. Managed a team of consulting CISOs, VPs and Directors in client engagements across business organizations and market segments.

- **Master of Science, Applied Information Management**

  - UNIVERSITY OF OREGON – Eugene, Oregon
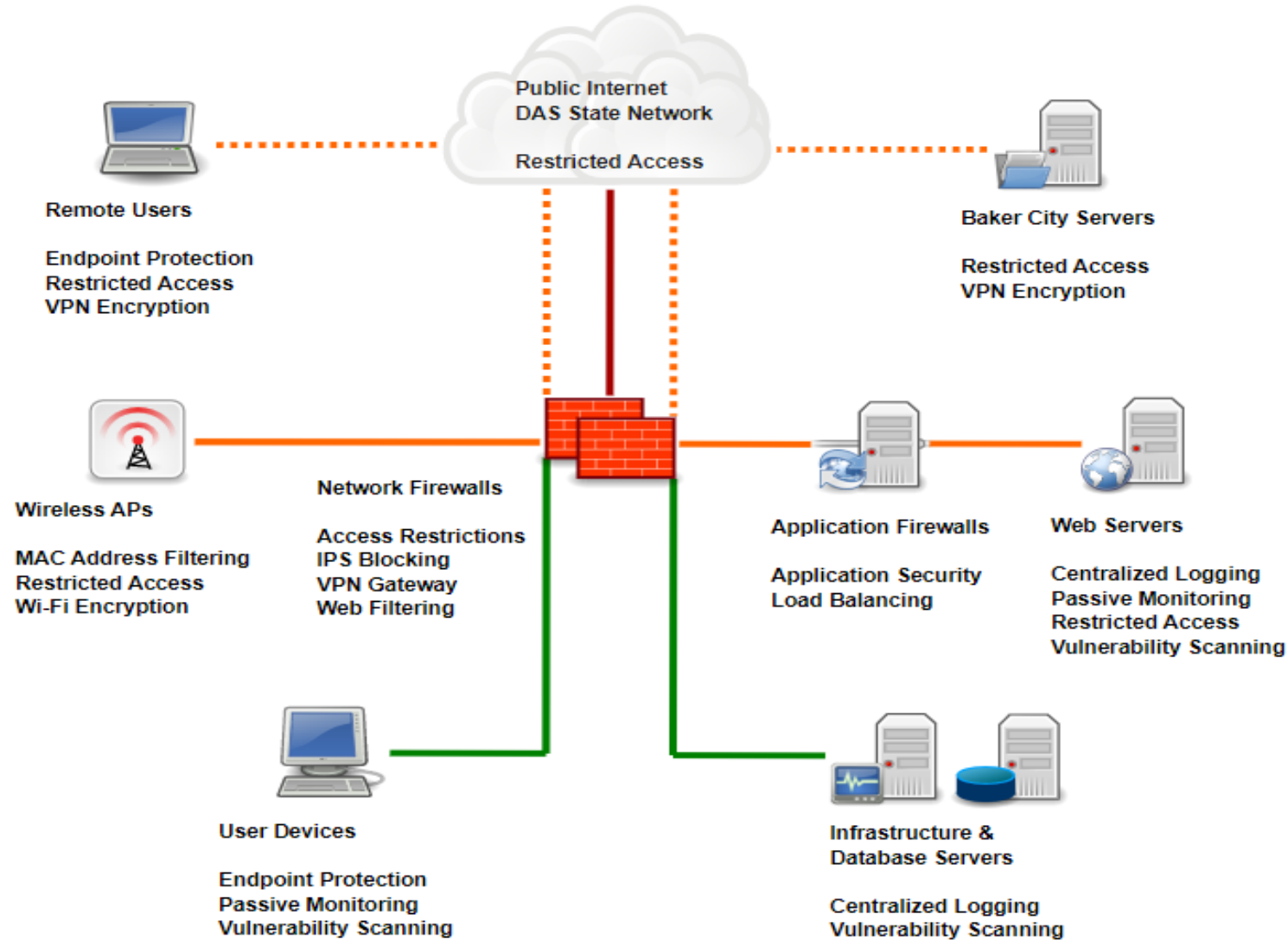
Top Risks in Cybersecurity 2023

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

Public Internet
DAS State Network

Restricted Access

Remote Users

Endpoint Protection
Restricted Access
VPN Encryption

Baker City Servers

Restricted Access
VPN Encryption

Wireless APs

MAC Address Filtering
Restricted Access
Wi-Fi Encryption

Network Firewalls

Access Restrictions
IPS Blocking
VPN Gateway
Web Filtering

Application Firewalls

Application Security
Load Balancing

Web Servers

Centralized Logging
Passive Monitoring
Restricted Access
Vulnerability Scanning

User Devices

Endpoint Protection
Passive Monitoring
Vulnerability Scanning

**Infrastructure &
Database Servers**

Centralized Logging
Vulnerability Scanning

Center of Internet Security (CIS) Controls vrs 8.0

- CIS Control 1:

    Inventory and Control of Enterprise Assets

- CIS Control 2:

    Inventory and Control of Software Assets

- CIS Control 3:

    Data Protection

- CIS Control 4:

    Secure Configuration of Enterprise Assets and Software

- CIS Control 5:

    Account Management

- CIS Control 6:

    Access Control Management

- CIS Control 7:

    Continuous Vulnerability Management

- CIS Control 8:

    Audit Log Management

- CIS Control 9:

    Email and Web Browser Protections

- CIS Control 10:

    Malware Defenses

- CIS Control 11:

    Data Recovery

- CIS Control 12:

    Network Infrastructure Management

- CIS Control 13:

    Network Monitoring and Defense

- CIS Control 14:

    Security Awareness and Skills Training

- CIS Control 15:

    Service Provider Management

- CIS Control 16:

    Application Software Security

- CIS Control 17:

    Incident Response Management

- CIS Control 18:

    Penetration Testing

Audits & Assessments

- Governance, Policy & Training

- 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

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

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.

[Mission Statement](#)
"Securing and Reducing Cyber Risk for Secretary of State Services provided to Oregonians"

Accomplishments 2022 - continued

Executive

- Updated polices and procedures

Audits

- User and access audit reviews

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

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

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
    - F5 Appliance
    - ISE (Identify Service Engine)/NAC (Network Access Control) Appliance upgrade
  - 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

LEO CUELLAR, CISO

Information Systems Division,
Oregon Secretary of State
Leo.Cuellar@sos.oregon.gov