SECRETARY OF STATE

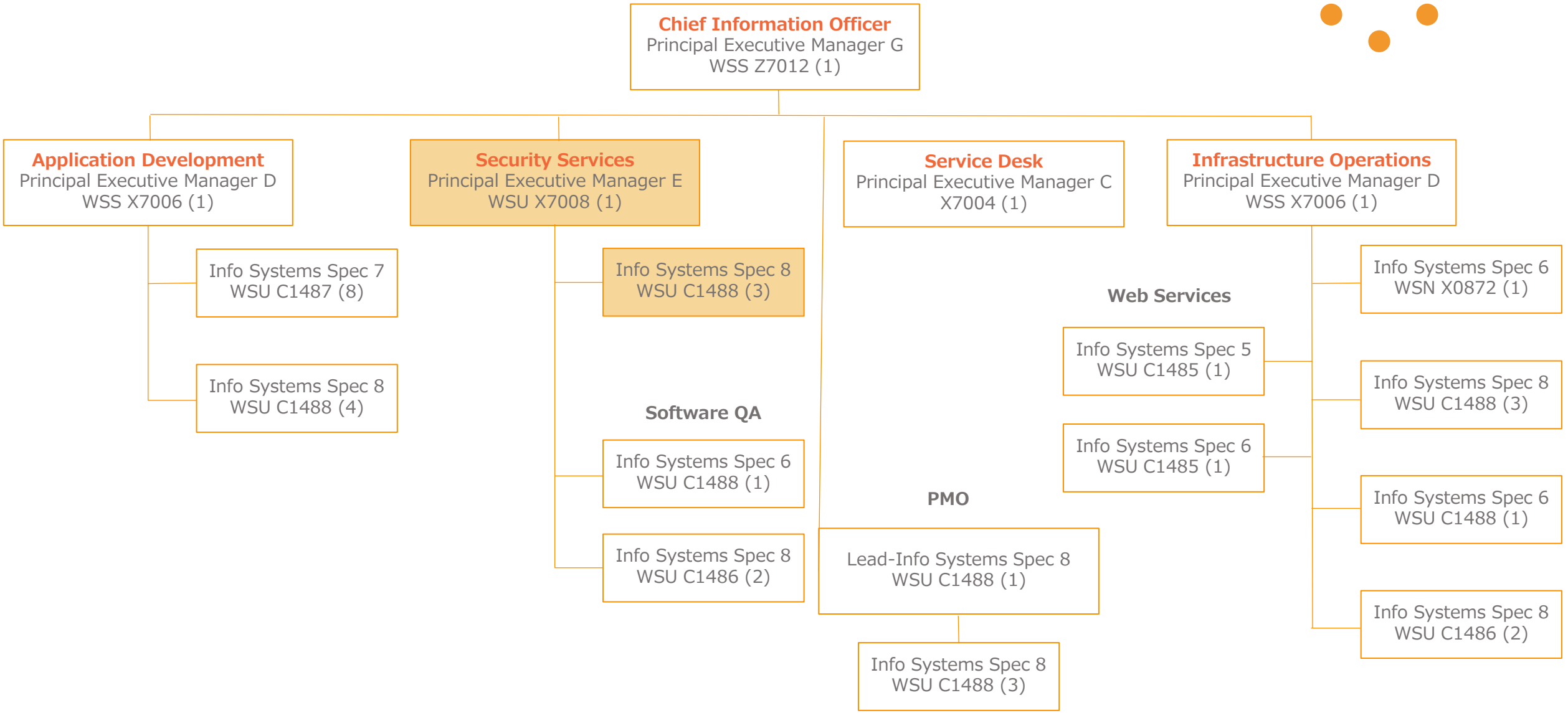
Information Security Report

Joint Legislative Committee on Information Management and Technology

June 2, 2021

A Sphere of Influence

Cybersecurity is a culture. We need to create a sphere of influence where everyone is an active/invested participant.


Chief Information Officer
Principal Executive Manager G
WSS Z7012 (1)
Application Development
Principal Executive Manager D
WSS X7006 (1)
Info Systems Spec 7
WSU C1487 (8)
Info Systems Spec 8
WSU C1488 (4)
Security Services
Principal Executive Manager E
WSU X7008 (1)
Info Systems Spec 8
WSU C1488 (3)
Software QA
Info Systems Spec 6
WSU C1488 (1)
Info Systems Spec 8
WSU C1486 (2)
Service Desk
Principal Executive Manager C
X7004 (1)
PMO
Lead-Info Systems Spec 8
WSU C1488 (1)
Info Systems Spec 8
WSU C1488 (3)
Infrastructure Operations
Principal Executive Manager D
WSS X7006 (1)
Web Services
Info Systems Spec 5
WSU C1485 (1)
Info Systems Spec 6
WSU C1485 (1)
Info Systems Spec 6
WSN X0872 (1)
Info Systems Spec 8
WSU C1488 (3)
Info Systems Spec 6
WSU C1488 (1)
Info Systems Spec 8
WSU C1486 (2)

ORG CHART

Overview

- Governance, Standards & Training
- Policy and Process
- Partnerships
- Security Architecture
- Assessments
- Network, Data, and Application Security
- Monitoring & Analytics
- Upcoming/Future Projects

Governance, Standards, and Training

- Security Plan
  - Strategic Security Plan (Drafted 4/19)
- Standards
  - National Institute of Standards and Technology (NIST)
  - Cybersecurity Framework 1.1
  - International Standards Organization (ISO)27000
- Annual Security Awareness Training
  - Formal, agency-wide
  - Newsletters/Internal messaging
  - Random phishing exercises

Policy and Processes (Last 12 months)

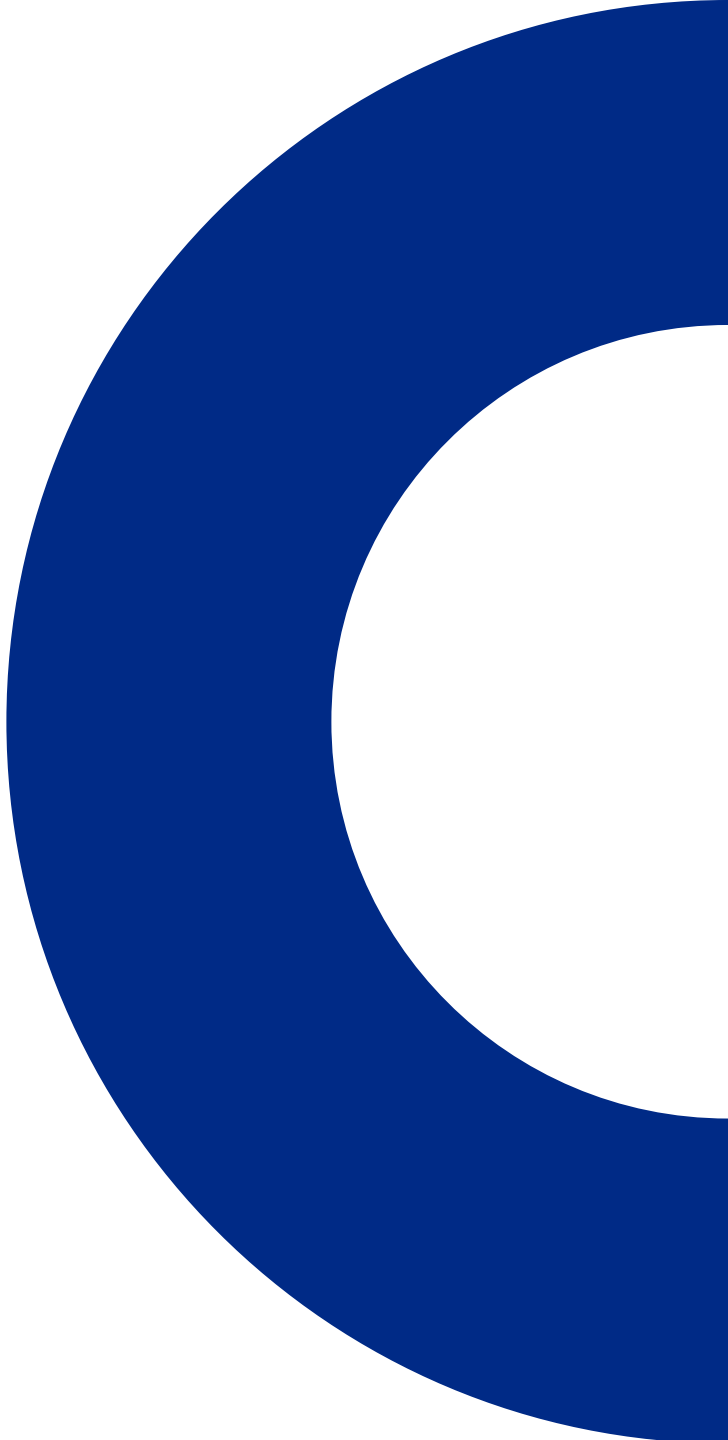
- Acceptable Use
- User Password
- Data Classification
- Security Awareness and Training
- Access Control
- Remote Access
- Electronic Commerce Services
- Criminal Justice Information Services (CJIS) Security

Collaborative Partnerships

- CIO Council
- State Information Security Council (ISC)
- Cyber Workgroup
  - National Guard, State and Local government
- Threat Information Gathering and Election Resources (TIGER) Team
  - DoD; State; and Federal legal, law enforcement, and intelligence agencies
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)

Security Architecture

- Next generation firewalls
- Web application firewalls (WAF)
- Endpoint Detection and Response (EDR)
- Data collection and analytics
- Network Access Control (NAC)



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

Network Security

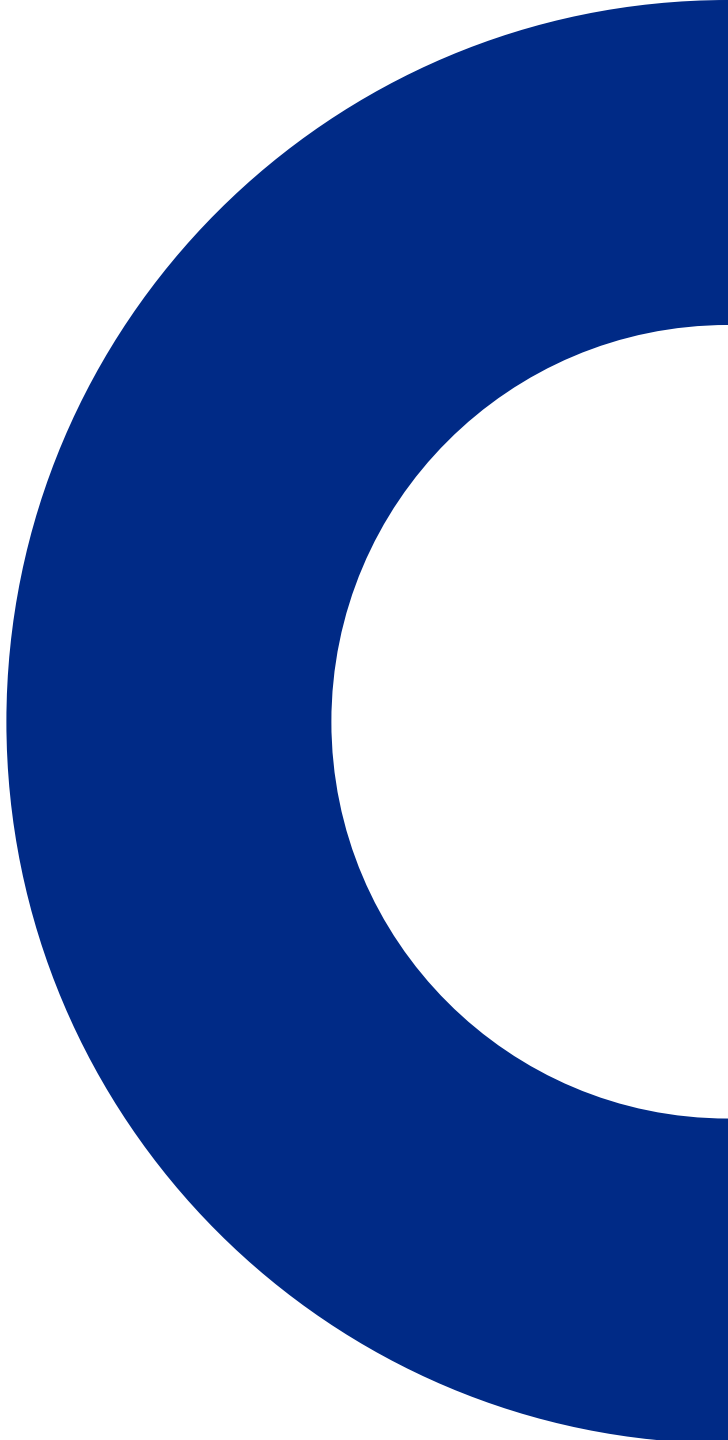
- Malicious Domain Blocking Reporting (MDBR)
- Website filtering blocking
- Log correlation monitoring and analytics
- Bot defense systems
- Incident Response
- 24-hour system monitoring and alerting – Crowdstrike and Albert Sensors

Data Security

- Enterprise application scanning
- COTS software scans
- Remote workstation scans

Application Security

- The WAF monitors, allows and blocks traffic
- Enterprise application scans
- Data collection & analytics system



Monitoring and Analytics

- Normal vs abnormal
- Threshold alerts
- Customizable Dashboards
- Investigations
- Identification of new/unauthorized devices

Upcoming/Future Security Projects

- Security Information and Event Management (SIEM)
- Upgrade EDR
- Expanding remote sensor and monitoring
- Penetration and Vulnerability assessments

QUESTIONS?

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