Oregon Department of Justice

Dan Rayfield, Attorney General

Information Security Report

2025 Joint Legislative Committee on Information Management and Technology

May 23, 2025

Judah Kelber, Interim Chief Information Officer

Herman Davis, Chief Information Security Officer

Information Security Governance

Security Partner Collaboration

Oregon DOJ Titan Fusion Cell Cyber Workgroup

- Monthly Meetings

Oregon Joint Agency Federal Tax Information Committee

- Monthly Meetings

Oregon Cyber Disruption Workgroup

- Quarterly Meeting

Cyber Security Services (CSS)

- Monthly Meetings with State CISO
- Monthly State Information Security Council

Enterprise Information Services (EIS)

- Monthly Meetings with State Deputy CIO for Public Safety

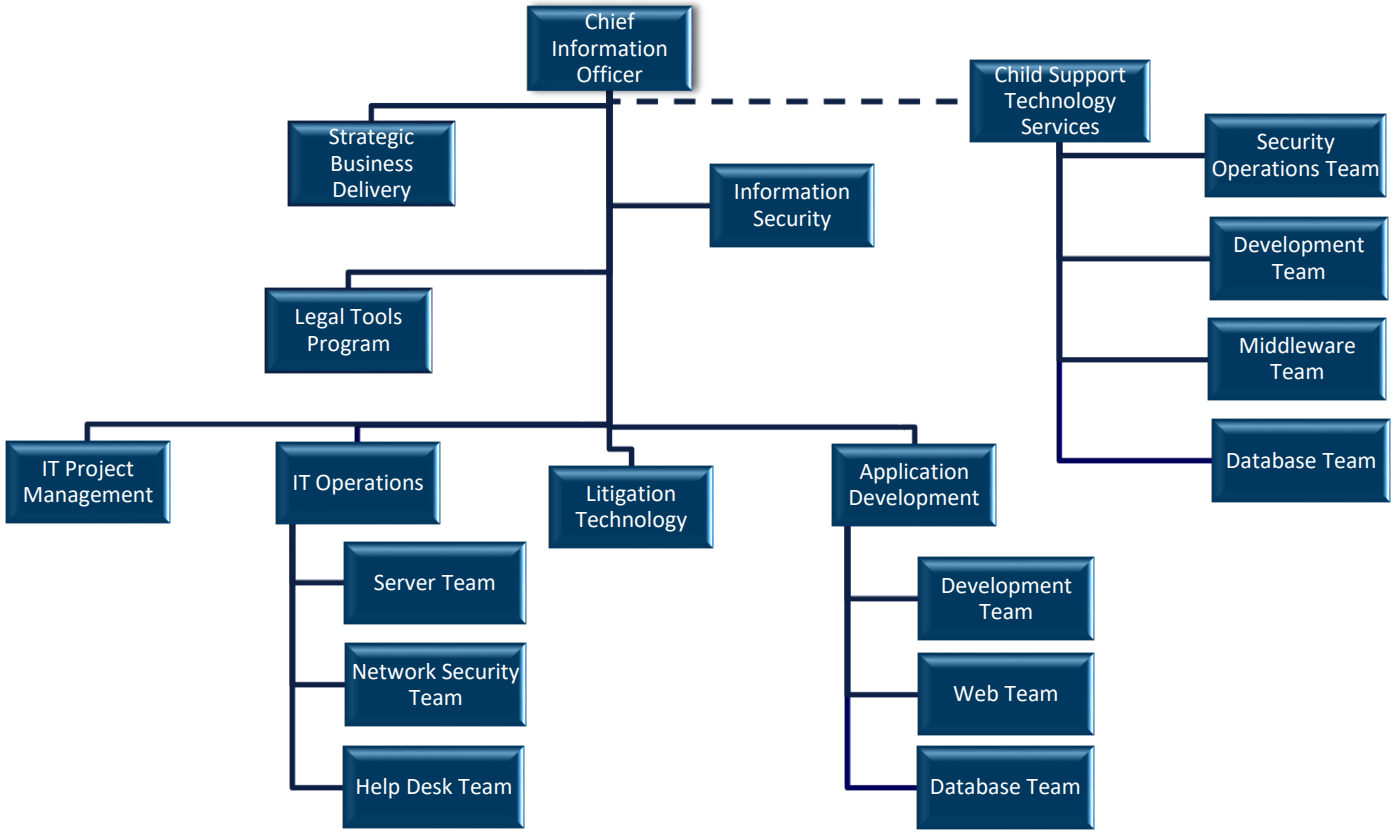
US DHS CISA

- Tabletop Exercises and Validated Architecture Design Review
- Cyber Hygiene and Web Application Scanning
- Penetration Testing and Vulnerability Assessments

Information Security and Privacy

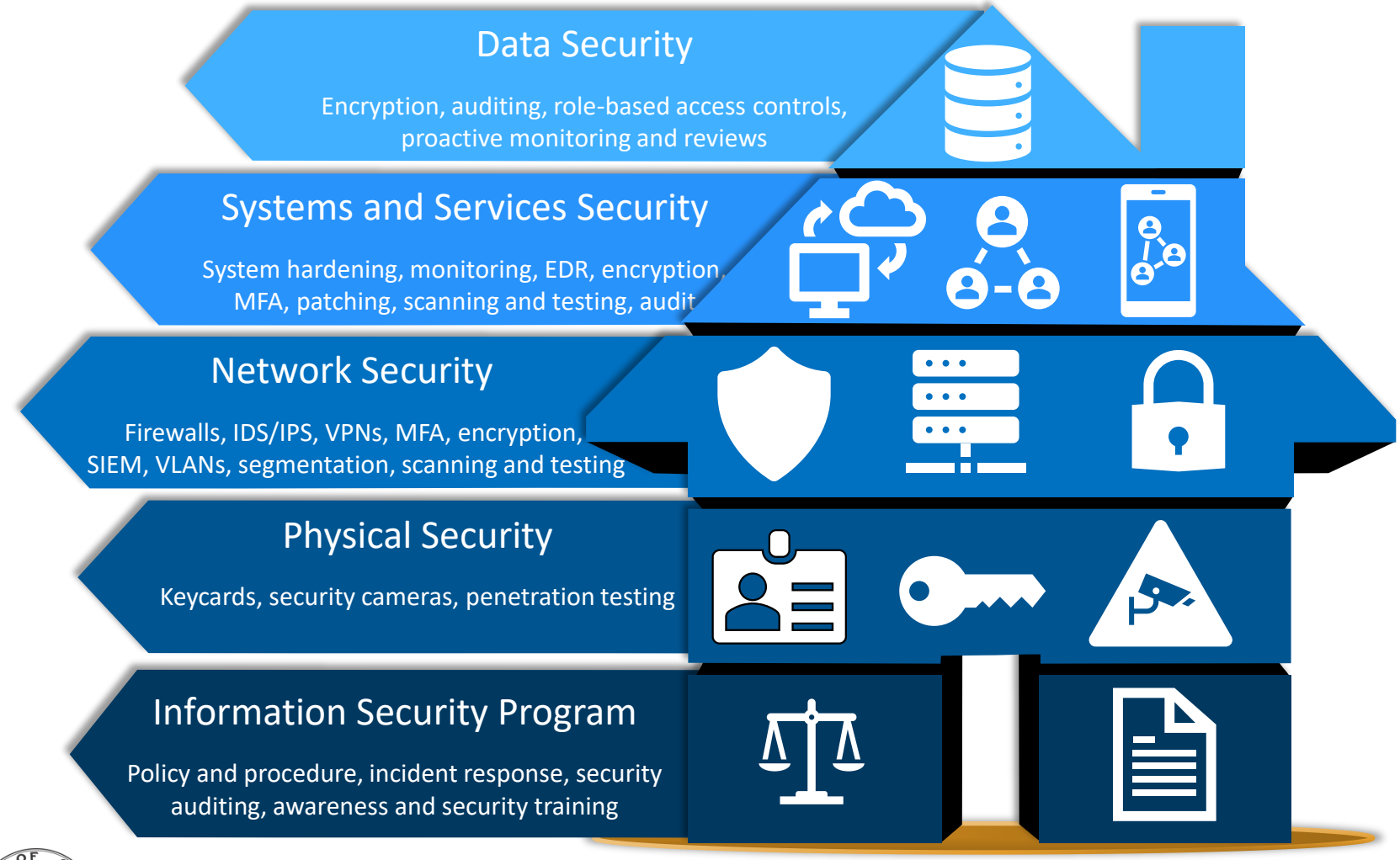
Statutory Regulatory	Standards	Policies	Process/ Procedure	Controls
• Regulatory requirements from Federal Agencies • OCIPA ORS 646A.600 • ORS 276A.303	• SP 800-53r5 Security and Privacy Controls • NIST 800-30 RISK • CJIS	• DOJ Policy Manual • CIO Policies • Oregon Statewide Information Security Standards	• NIST Guidelines • CIS Controls v8.1 • DOJ Process and Procedures	• Controls from NIST 800-53 and CIS Controls v8.1

Information Technology Overview



FTE: 88 with 22.7% eligible to retire within 5 years.

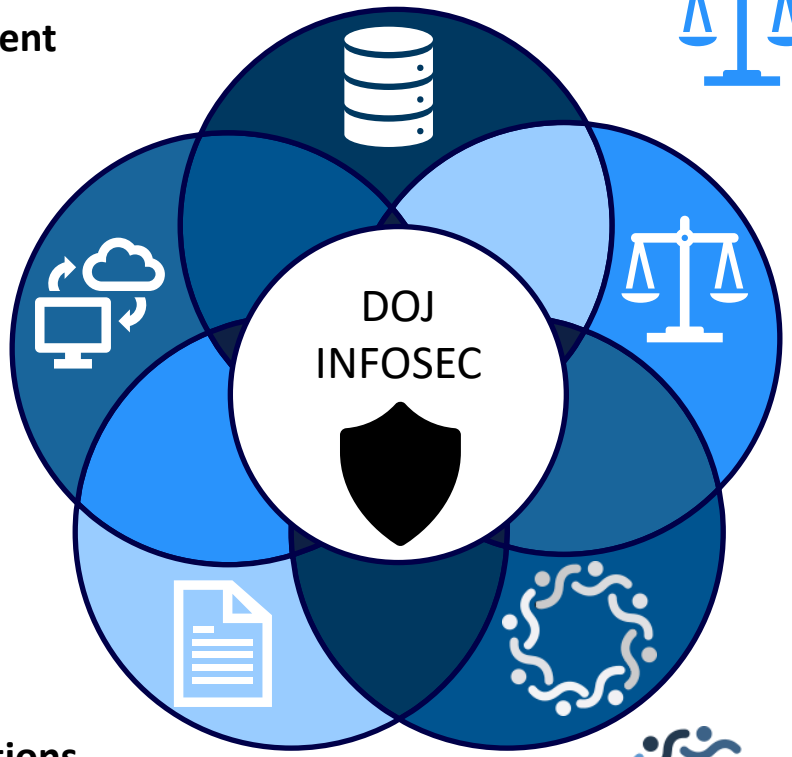
Value of Defense in Depth



DOJ Systems Protected

Enterprise Content Management
25 servers
21,922,188 files

Legal Case Management
134 servers,
1,129,630 case records



Enterprise Storage
5 Devices, 1246 TB

eDiscovery
10 servers, 52.5 TB
499 open cases, 8 TB

Web Applications
26 web domains,
44 web applications,
35,112,480 page views last year

Origin (Child Support System)
85 servers,
127,459 families served
Over a billion records

Security Statistics

Top Attacks

Phishing

DNS Poisoning

Distributed Denial of Service

Mail Security

Security Intel Blocks – 3.3 million

Phishing Attacks – 47,628

Perimeter Security

- Blocked - 768 million
- Security Intel Events – 11.7 million
- Targeted Intrusion Attempts - 146

Internal Systems

- Intrusion Attempts – 155,203
- Malicious Sites Blocked – 200 million
- Malware blocked – 42

Security and Privacy Values

There should be limits to the collection of data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes, should be accurate, complete, and kept updated.

Data should not be disclosed, made available, or otherwise used for purposes other than those specified.

Data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Business Systems - Protection

How do we provide the most value and protect critical business systems?

- Continuous vulnerability assessments
- Detailed System Security Plans
- Proactive auditing by third party trusted partners
- Proactive third-party vulnerability and penetration testing
- Collaboration with business units
- Collaboration with partners

Security Value Delivered 2023-2025

- Ongoing integration of MFA at every level of technology
- Security Awareness Training
- Quarterly Phishing Test at Level 5/6
  - 14.9 Phish-prone % (below industry average of 17.9%)
- Vulnerability and Penetration Tests – 18-24 months
  - Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) Engagement (no cost to the state)
  - Microsoft Security Assessment
- Continuity of Operations Testing
  - DHS/CISA Tabletop Exercise (no cost to the state)
- Advanced Threat Protection Deployment
- Advanced Security Incident Event Monitoring

Security – Looking to the Future

- Zero Trust Architecture Education and Plan Development
- Continue agency partnerships with a focus on security
- Continue biennial vulnerability and penetration testing with CISA and Third-Party vendors
- Continue to mature Third-Party vendor risk management
- Replace and retire legacy systems (e.g., Origin framework and legacy legal tools)
  - Independent code reviews
  - Security standards review
  - Vulnerability and penetration testing before go live approval
- Continue to mature and enhance capabilities
  - Create Incident Response playbooks for various scenarios
  - Test playbooks through CISA Tabletop Exercises

Information Security Investment

We must continue to invest in Information Security to:

- Combat malicious actors and to identify, protect, detect, respond, and rapidly recover from security incidents.
- Educate and expand awareness to reduce the attack surface.
- Advance the use of technologies such as trustworthy AI to identify trends and respond faster (e.g., do more with less).
- Achieve trustworthy computing through a zero-trust model.
- Leverage cloud and cloud security tools and capabilities.
- Develop knowledge and threat awareness sharing through alerts and statewide information sharing (e.g., Center of Excellence, Titan Fusion Cell Cyber Sharing).

Reminder – It's not IF but WHEN