



NCSL – Cybersecurity Task Force Meeting
April 21, 2017

**Oregon
Legislative Fiscal
Office**

Sean McSpaden
Principle Legislative
IT Analyst &
JLCIMT Committee
Administrator





Oregon Legislative Fiscal Office (LFO)

- Legislative Fiscal Officer (Ken Rocco) appointed by co-chairs of Joint Committee on Ways and Means (Senator Devlin and Representative Nathanson)
- **LFO is a permanent nonpartisan legislative service agency that:**
 - Provides comprehensive research, analysis, and recommendations on state's biennial budget
 - **Evaluates state expenditures, program administration, and agency organization**
 - **Assists in developing Legislature's adopted balanced budget**
 - **Prepares fiscal impact statements on legislative measures**
 - Publishes detailed analyses, summary documents, and briefs on budget-related topics
 - Performs other duties as directed by the Legislative Fiscal Officer

<https://www.oregonlegislature.gov/lfo>





Oregon Legislative Fiscal Office (LFO)

Provides Professional Staff Support

Emergency
Board
*(Legislative
Interim)*

Joint
Committee on
Ways and
Means

Joint
Legislative
Audits
Committee

Transparency
Oregon
Advisory
Commission

Joint
Legislative
Committee on
Information
Management
and
Technology

Other
Special
Committees
or Task
Forces





Oregon Legislative Fiscal Office (LFO)

Establish
Statewide IT
Goals and
Policy

JLCIMT
**Statutory
Committee**

(ORS 171.852 -
171.855)

Provide IT
Project and
Cybersecurity
Oversight
(Support JWM)

Conduct
Studies
IT & Cyber-
security

Introduce &
Oversee
IT &
Cybersecurity
Policy Bills

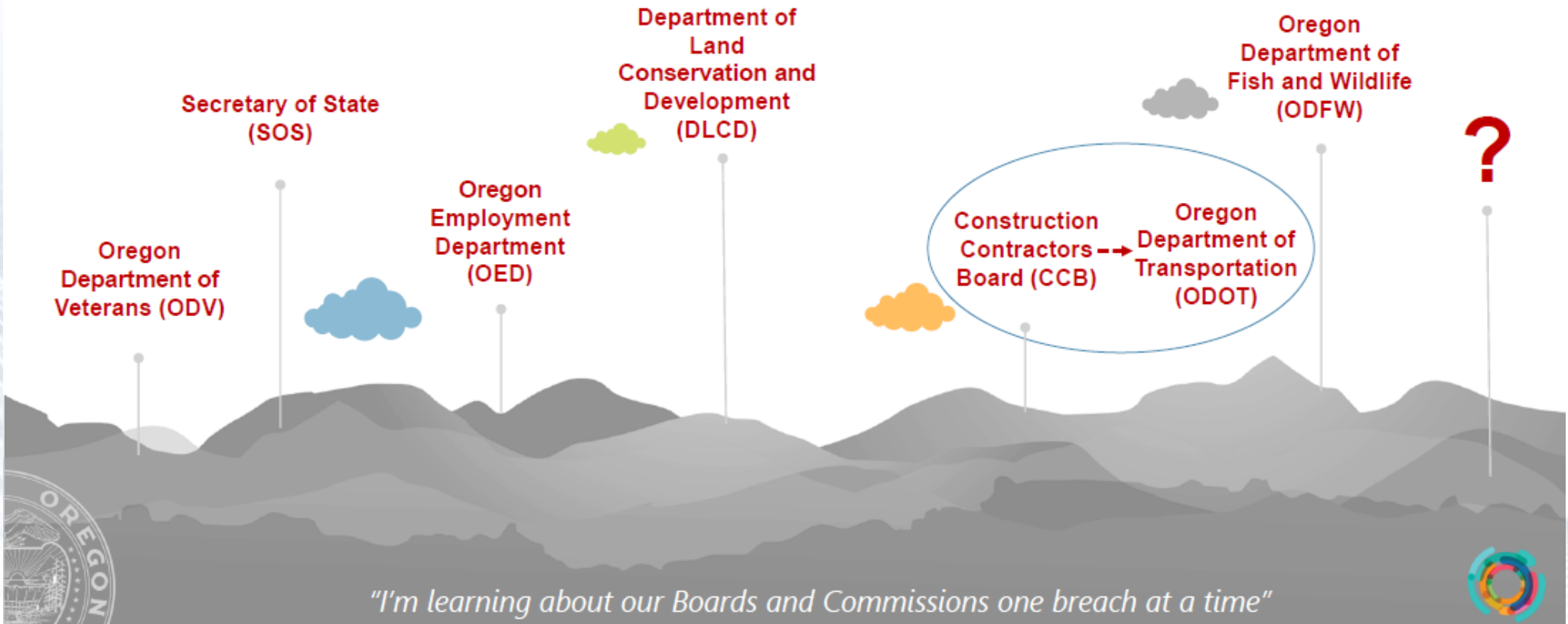
- https://www.oregonlegislature.gov/bills_laws/ors/ors171.html
- <https://olis.leg.state.or.us/liz/2017R1/Committees/JLCIMT/Overview>



Information Security Incidents - 2014-2016

IT Security

recent compromises, breaches and asymmetric risk





Key Actions – 2015

- **February 2015**, Legislature introduces **HB 3099** to transfer enterprise IT operations and information security oversight authority from DAS Director to State CIO
- **March 26th, 2015**. Governor Brown directs **State CIO** to take interim control of **State Data Center operations** in response to IT Security Incident and other issues
- **July 2015**. SB 5502, DAS Appropriation Bill – **adds 12 IT security positions**. Moves State CIO's Enterprise Security Office from **5 to 17 positions**
- **August 2015**. Secretary of State Audit 2015-20. State Data Center. Numerous findings, but progress being made. Indicate next audit will focus on agencies
- **August 2015**. Governor Brown **signs HB 3099 into law**
- **December 7th, 2015**. **Emergency Board** – DAS Rebalance & OSCIO Reorganization – **increased OSCIO Enterprise Security Office from 17-24 positions**

SOS Audit 2015-20 - <http://sos.oregon.gov/audits/documents/2015-20.pdf>

HB 3099 - <https://olis.leg.state.or.us/liz/2015R1/Measures/Overview/HB3099>



Key Legislative Action – 2016

JLCIMT Senate Bill 1538

- Introduced as JLCIMT bill in February 2016.
- **Requires state agencies – Executive, Legislative, Judicial Branch - to notify LFO of information security assessments and incidents**
- Requires heads of certain state agencies to provide annual report concerning information security to the JLCIMT
- Became operative July 1, 2016

SB 1538 - <https://olis.leg.state.or.us/liz/2016R1/Measures/Overview/SB1538>





Key Action – 2016

Secretary of State Audit: 2016-30

July/August 2016 – Preliminary Findings: state agency information security posture

- **“Security is not a priority.”** Security is not a priority within many agencies and the current model is probably hopeless.
- **“Empty promise of security.”** The state of Oregon does not effectively resource and coordinate IT security at an enterprise level.
- **Going it alone.** Some agencies refuse assistance and instead “circle the wagons.”
- **“Highly informal.”** Security controls in place are being carried out by IT line staff using whatever tools they happen to have at their disposal.
- **Genie out of the bottle.** Non-approved and unsecured “cloud applications” are deployed throughout the enterprise (along with other shadow IT)

November 2016. Secretary of State Audit 2016-30. Agency Information Security
<http://sos.oregon.gov/audits/documents/2016-30.pdf>



Key Executive Branch Action – 2016

Executive Order – 16-13

September 12, 2016. *Executive Order No. 16-13 “Unifying Cyber Security in Oregon”*



- **Unifies cybersecurity functions and personnel within the Executive department under the direction of the State CIO;**
- Requires Office of the State CIO to conduct a statewide agency-by-agency risk-based security assessment and remediation program; and
- Requires Office of the State CIO to conduct and document the completion of (IT) security awareness training by all state employees.
- Agencies billed for cost of tools, assessment services, and training

Temporary measure – must be codified by Oregon Legislature in 2017

EO – 16-13: http://www.oregon.gov/gov/Documents/executive_orders/eo_16-13.pdf



E.O. 16-13. Unifying cybersecurity to improve customer service for Oregonians while ensuring those systems are secure, resilient and ready for the future

| FOCUS |  Risk Assessments Determine Oregon's risk profile |  Vulnerability Mgmt. Reduce future exposure |  Awareness/Training Create insights and expertise |  Remediation Plan Enterprise functions enabling resilience |
|-------------------|---|---|---|--|
| IMPERATIVES | <ul style="list-style-type: none"> • NIST Maturity model • Information Handling • Secure Applications • Policy and Procedures | <ul style="list-style-type: none"> • Inventory and Scanning • Analysis and Reporting • Remediation • Governance | <ul style="list-style-type: none"> • Cyber-user awareness • Professional Expertise • Role based Expertise | <ul style="list-style-type: none"> • Enterprise Functions • Org Design • Resourcing the Plan |
| KEY PROGRAM GOALS | <ul style="list-style-type: none"> • Agency Surveys. Gather and analyze agency information to develop priorities • NIST Framework. Develop a set of risk evaluation standards for agencies • Security Assessments. Establish methods for large scale risk assessment activities • Analysis/Remediation. Address prioritized risk as discovered and document trends for Strategic priorities | <ul style="list-style-type: none"> • Scanning: Deliver scanning capabilities to in scope agencies • Analysis: Develop metrics and reporting that aid agencies in prioritizing remediation activities • Remediation: Collaborate with agencies on remediation priorities • Governance: Establish a recurring communication channel with agencies to monitor and discuss progress | <ul style="list-style-type: none"> • Awareness Training. Ramp up and roll out annual awareness training materials • Collaboration. Develop tools and campaigns for increasing awareness between annual training • Security Professionals. Increase expertise and experience through training and collaboration • SME Professionals. Increase security expertise in App Dev, Infrastructure and other IT professionals | <ul style="list-style-type: none"> • Security Functions: Prioritize security functions to be made Enterprise capable • ESO Design: Develop an organizational design capable of delivering security functions • Security Roles: Establish roles required to stand up new functions within the ESO • Enable the Future. Build plans that steadily increase the ESO capabilities over the next four years |

Focus on Executive Order but identifies some key budget categories for Cybersecurity



Current Actions

2017-19 Budget & Senate Bill 90

- **December 1, 2016.** 2017-19 Governor's Budget calls for
 - **Increase funding/staffing** for OSCIO Enterprise Security Office by **\$11,446,351 and 36 positions** or 35.75 FTE (a shift of budget/FTE out of other agency budgets)
 - If adopted by Legislature **will increase** OSCIO Enterprise Security Office **staffing from 24 to 60 information security professionals (funded via agency assessment \$)**
- **February 2017.** SB 90 – IT Security Unification and Cybersecurity Center of Excellence
 - **SB 90 codifies Executive Order 16-13 via statute**
 - Provides for unification of IT security within executive branch
 - **Establishes a Cybersecurity Fund** – account segmented from State IT Operating Fund
 - Establishes an Oregon Cybersecurity Center of Excellence (CCoE)
 - Public-private state-civilian interface for information sharing, coordination of cyber incident response, developing a statewide cyber strategy, identifying best practices and encouraging development of Oregon's cyber-security workforce.
 - **Currently working its way through various legislative committees w/amendments**

SB 90: <https://olis.leg.state.or.us/liz/2017R1/Measures/Overview/SB90>



Oregon Cybersecurity Challenges

- **Decentralized** agency operations model – program and IT services
- **Dispersed** authority/responsibility for Cybersecurity – agencies & State CIO
- **Uneven** staffing and funding levels, expertise & capability – Have/Have Not
- **Scarce** funding available (color of money) – uneven ability to address need
- **Limited** availability of Cybersecurity professionals willing to work for state pay ranges – agencies are competing with one another for cyber talent
- Propensity to **blame and shame** vs. community based/public health model
- All of this leads to **risk for the many from the few or the one... weakest link(s)**





Thank You





Contact Information

Sean McSpaden, PMP, CISM

Principal Legislative IT Analyst

JLCIMT Committee Administrator

Oregon Legislative Fiscal Office

Phone: (503) 986-1835

Email: Sean.L.McSpaden@state.or.us

