Oregon Legislative Fiscal Office

Sean McSpaden
Principle Legislative IT Analyst & JLCIMT Committee Administrator

NCSL - Cybersecurity Task Force Meeting
April 21, 2017
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)

JLCIMT
Statutory Committee
(ORS 171.852 - 171.855)

Establish Statewide IT Goals and Policy

Provide IT Project and Cybersecurity Oversight (Support JWM)

Conduct Studies IT & Cybersecurity

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

Secretary of State (SOS)
Oregon Department of Veterans (ODV)
Oregon Employment Department (OED)
Department of Land Conservation and Development (DLCD)
Oregon Department of Fish and Wildlife (ODFW)
Construction Contractors Board (CCB)
Oregon Department of Transportation (ODOT)

“I’m learning about our Boards and Commissions one breach at a time”
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**

HB 3099 - https://olis.leg.state.or.us/liz/2015R1/Measures/Overview/HB3099
Key Legislative Action - 2016

JLC IMT Senate Bill 1538

• Introduced as JLC IMT 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 JLC IMT
• Became operative July 1, 2016

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

**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

<table>
<thead>
<tr>
<th>Risk Assessments</th>
<th>Vulnerability Mgmt.</th>
<th>Awareness/Training</th>
<th>Remediation Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine Oregon's risk profile</td>
<td>Reduce future exposure</td>
<td>Create insights and expertise</td>
<td>Enterprise functions enabling resilience</td>
</tr>
</tbody>
</table>

### Imperatives

<table>
<thead>
<tr>
<th>NIST Maturity model</th>
<th>Inventory and Scanning</th>
<th>Cyber-user awareness</th>
<th>Enterprise Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Handling</td>
<td>Analysis and Reporting</td>
<td>Professional Expertise</td>
<td>Org Design</td>
</tr>
<tr>
<td>Secure Applications</td>
<td>Remediation</td>
<td>Role based Expertise</td>
<td>Resourcing the Plan</td>
</tr>
<tr>
<td>Policy and Procedures</td>
<td>Governance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Key Program Goals

<table>
<thead>
<tr>
<th>Agency Surveys</th>
<th>Scanning: Deliver scanning capabilities to in scope agencies</th>
<th>Awareness Training</th>
<th>Security Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gather and analyze agency information to develop priorities</td>
<td>Develop metrics and reporting that aid agencies in prioritizing remediation activities</td>
<td>Ramp up and roll out annual awareness training materials</td>
<td>Prioritize security functions to be made Enterprise capable</td>
</tr>
<tr>
<td>NIST Framework</td>
<td>Analysis: Develop metrics and reporting that aid agencies in prioritizing remediation activities</td>
<td></td>
<td>ESO Design: Develop an organizational design capable of delivering security functions</td>
</tr>
<tr>
<td>Develop a set of risk evaluation standards for agencies</td>
<td>Remediation: Collaborate with agencies on remediation priorities</td>
<td></td>
<td>Security Roles: Establish roles required to stand up new functions within the ESO</td>
</tr>
<tr>
<td>Security Assessments</td>
<td>Governance: Establish a recurring communication channel with agencies to monitor and discuss progress</td>
<td></td>
<td>Enable the Future: Build plans that steadily increase the ESO capabilities over the next four years</td>
</tr>
<tr>
<td>Establish methods for large scale risk assessment activities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis/Remediation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address prioritized risk as discovered and document trends for Strategic priorities</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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)
  - Currently working its way through various legislative committees w/ amendments

SB 90: https://olis.leg.state.or.us/liz/2017R1/Messages/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