OREGON | Office of the State
Chief Information Officer

2016

Implementation of E.O. 16-13, “Unifying Cyber Security in Oregon”

Written Testimony for the Joint Legislative Committee on Information Management and Technology | 12 December 2016

DAS | OFFICE OF THE STATE CIO | 155 COTTAGE STREET, NE, SALEM, OR 97301

Contents

Background. *IT Security in Oregon*

Until recently, the Office of the State CIO (OSCIO) and State Chief Information Security Officer (CISO) had neither responsibility for nor authority over the security of ETS operations—possessing only nominal authority over statewide security policy, given limited staffing and a lack of enforcement authority. In its 2015 audit report entitled "*State Data Center: First steps to address longstanding security risks, much more to do*" the Secretary of State's (SOS) Audit Division observed that "[o]ver the last nine years, security weaknesses at the state data center have put confidential information at risk. [Noting that] [t]he weaknesses continued because the state abandoned initial security plans, did not assign security roles and responsibilities, or provide sufficient security staff."[1] Under this model, responsibility for security at ETS was diffused amongst all staff, yet there was no corresponding accountability—much like the "bystander effect," when everyone is responsible no one is responsible.

Following the passage of HB 3099 (2015) and approval of *Policy Option Package 112: Security and IT Operations Audit Support* (SB 5502, 2105)—which provided 12 limited duration (LD) positions (12 months in duration)—the State CIO immediately moved to create the Enterprise Security Office (ESO). Given the immediacy of statewide security vulnerabilities and the SOS Audit findings, the ESO was formed with the 12 LD security positions (immediately filled with job rotations using existing ETS personnel), permanent ETS staffing and the original security policy group from the Chief Information Office. Consisting of 24 positions, the formation of the ESO increases total security staffing from 3 to 14 percent of ETS staffing.

Under the leadership of the State CISO, the ESO brought together all infrastructure security functions into a single organization—directly accountable for the security of ETS operations, real-time security monitoring of the state network and incident response, enterprise security policy, enterprise security architecture, and dissemination of best practices. Given its responsibility for ETS operations and the need to collaborate with ETS technical teams, the ESO was embedded within the state data center. However, in order to ensure clear accountability for the security for data center operations the State CISO continues to report directly to the State CIO. With the formation of the ESO, our Office took significant steps towards fixing the problems identified by the SOS's August 2015 audit, however, as the audit noted even them, "the solutions will take time, resources, and cooperation from state agencies."[2]

While working to address the security vulnerabilities of the statewide network and those related to IT infrastructure support is no small task, Oregonians personal data will remain at risk until we address the cyber security capacity gap amongst state agencies. State agencies are required to follow the policies and procedures established *("after consultation and collaborative development"*), however, they are ultimately responsible for securing their IT systems pursuant to ORS 182.122.[3] Recent IT security breaches, persistent vulnerabilities, non-compliance with IT security-related OARs and statute and the most recent audit findings demonstrate that the current decentralized model for IT security is not working. In the last year, agencies have refused to provide our Office with copies of a vulnerability assessment as required under ORS 182.122 (8)(b); attempted to purchase security software, hardware and services without prior authorization; been compromised by the same attack pattern that was used against the state over two years ago (potentially, the same individual depending on the veracity of self-attribution); and sought to actively conceal known security vulnerabilities. Given the sensitivity of IT security information (particularly, current

[1] Secretary of State Audit 2015-20. Available at http://sos.oregon.gov/audits/Documents/2015-20.pdf

[2] Ibid.

[3] ORS 182.122(8)(a) – *"State **agencies are responsible** for securing computers, hardware, software, storage media, networks, operational procedures and processes used in collecting, processing, storing, sharing or distributing information outside the state's shared computing and network infrastructure, following information security standards, policies and procedures established by the State Chief Information Officer and developed collaboratively with the agencies"* (emphasis added).

vulnerabilities) and our commitment to changing the discourse on IT security, our Office has no interest in naming and shaming individual agencies. These examples, merely underscore the failure of the current IT security model.

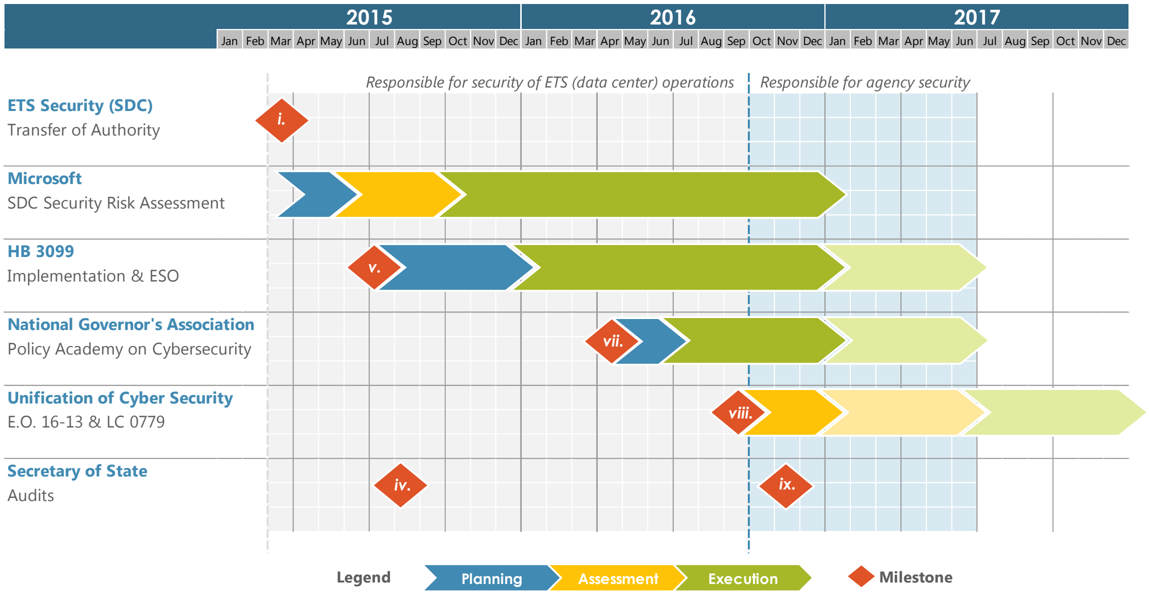
Just as it once was with the state data center, all agencies are collectively responsible for security—however, capacity is unevenly diffused across state government. In some agencies, there are clear capacity gaps, a legacy of disinvestment and an overly risk-tolerant approach to the cyber risks facing our state. More problematic however is the asymmetric nature of IT security risk, where the vulnerabilities of smaller and under-resourced agencies put larger state agencies and local government partners at risk; *e.g.*, the Construction Contractor's Board breach that compromised log-in credentials for the Oregon Department of Transportation and several County governments. Suffice to say, Oregon requires a long-term strategy for preventing future threats and building capacity across the state. The strategy our Office has proposed recognizes that IT security is a public good and that we are more resilient when we stand together—pooling our cyber security resources and shifting our approach from a model of risk transfer and assignment of blame to a proactive enterprise security approach.

IT SECURITY TIMELINE

Since coming into Office in February 2015, Governor Brown has brought focus on improving the state of Oregon's IT security posture, including: the reassignment of responsibility for the security of data center operations to the State CIO, Alex Pettit; the signing of HB 3099 (2015) into law; writing a letter in support of our Office's application to a national policy academy on cybersecurity; signing E.O. 16-13, *"Unifying Cyber Security in Oregon"*; and introducing legislation that will put E.O. 16-13 into law and establish a Cybersecurity Center of Excellence. Governor Brown's commitment to improving IT security is borne from personal experience. In February 2014, the Secretary of State's website suffered a breach that put state elections and business registry databases offline for nearly three weeks. Then and now, online security has remained a vitally important issue for the Governor's administration.

The timeline and list of key events below represents a fundamental shift in how the state of Oregon views and approaches IT security—a shift from isolated and ineffective interventions to an integrative, risk-based, multi-sector IT security model that works in partnership with its private-sector, education and local government partners to confront the cyber threat that our state faces.

Fig. 1. IT Security in Oregon. *A Timeline of Recent Events*



BACKGROUND. IT SECURITY IN OREGON

i. ***March 26th, 2015.*** *Governor Brown Addresses Recently Discovered I.T. Security Vulnerability*[4]

- Transfer of interim executive management responsibility for ETS to State CIO Alex Pettit
- State Chief Information Security Officer (CISO) assumes security responsibility for ETS operations

ii. ***May - October 2015.*** *Microsoft Security Risk Assessment*

- Initiated in May of 2015, completed in September of 2015 and immediately followed by a prioritization and remediation planning starting in October of 2015
- Focused on systemic risk and implementation of risk management as an ongoing program within ETS
- Key assessment findings, included: i) business leadership ***acceptance of risk***; ii) a lack of ***credential hygiene***; iii) insufficient ***security administration*** and definition of security zones; iv) insufficient ***security monitoring***; v) no ***enterprise risk assessment*** program was in place; and vi) a poor ***software development lifecycle*** and definition of boundaries between ETS and agencies.

iii. ***July 2015.*** *SB 5502, DAS Appropriation Bill*[5]

- 12 limited duration IT security positions were added through approval of a policy option package titled, ***"Package 112, Security and IT Operations Support"*** during a July 6th work session of the Ways and Means Subcommittee on General Government. The appropriation bill became effective on January 1st, 2016.

iv. ***August 2015.*** *Secretary of State Audit 2015-20. "State Data Center: First steps to address longstanding security risks, much more to do"*[6]

v. ***August 2015.*** *Governor Brown signs HB 3099 – "Relating to state information technology; and declaring an emergency"*[7]

- Governor Brown signed the bill on August 12th, 2015 and it became effective on January 1st, 2016.
- Our Office assumed permanent responsibility for the security of ETS operations and the state network.

vi. ***December 7th, 2015.*** *DAS Rebalance Request and OSCIO Reorganization*[8]

- In order to implement HB 3099 (2015) our Office immediately moved to reconstitute the Enterprise Security Office with 24 positions—increasing total security staffing from 3 to 14 percent of ETS staffing and providing for the security of ***ETS operations*** and monitoring of the ***state data center*** and incident response.

vii. ***March 2016 - present.*** *National Governor's Association (NGA), 2016 Policy Academy on Enhancing State Cybersecurity*

- With the full support of Governor Brown, our Office submitted an NGA proposal on March 18th, 2016 and was 1 of 5 states selected for the Policy Academy that had a two-day kick-off in Detroit, Michigan on June 6th and 7th 2016.[9]

[4] Press Release. Available at http://www.oregon.gov/newsroom/Pages/NewsDetail.aspx?newsid=636

[5] LFO Work Session Papers. Available at https://olis.leg.state.or.us/liz/2015R1/Downloads/CommitteeMeetingDocument/77884 -- *"**Package 112 Security and IT Operations Audit Support.** This package adds Other Funds expenditure limitation and limited duration positions to implement recent Secretary of State and independent auditor findings, as well as, accommodate growth in agency usage of IT services. Given the uncertainty involving which services ETS will offer in the future given the ongoing "IT Common Service Delivery" review currently underway and concerns over management of ETS which has led to numerous reviews and audits, the positions are approved as limited duration for 12 months only. DAS will return during the 2016 legislative session with recommendations on service lines provided, operational changes, and a revised funding methodology for ETS for the second year of the biennium as detailed in the budget note for ETS."*

[6] Secretary of State Audit 2015-20. Available at http://sos.oregon.gov/audits/Documents/2015-20.pdf

[7] LFO Work Session Papers. Available at https://olis.leg.state.or.us/liz/2015R1/Measures/Overview/HB3099

[8] LFO Work Session Papers. Available at https://olis.leg.state.or.us/liz/2015I1/Downloads/CommitteeMeetingDocument/82348

[9] The Oregon NGA Application to the Cybersecurity Policy Academy is available upon request.

- Our Office held a joint- Oregon Cybersecurity Policy Summit with the NGA on October 11th and 12th.[10]
- The NGA has continued to provide our Office with research assistance and will be hosting a series of IT security webinars over the next few months.

viii. ***September 12th 2016.*** *Executive Order No. 16-13 "Unifying Cyber Security in Oregon"*

- Unifies information technology (IT) security functions and personnel within the Executive department by putting them under the direction of our Office;
- Requires our Office to conduct a statewide agency-by-agency risk-based security assessment and remediation program; and
- Requires our Office to conduct and document the completion of (IT) security awareness training by all state employees.

ix. ***November 2016.*** *Secretary of State Audit 2016-30. "Improving State Computer Systems will take Time, Resources, and Cooperation[11]"*

x. ***December 1st 2016.*** *2017-19 Governor's Budget*

- Increases the funding and staffing for the Enterprise Security Office by $11,446,351 and 36 positions or 35.75 FTE (represents a shift of budget and FTE out of other agency budgets)
- Requesting additional resources was premature prior to the completion of the Enterprise Information Security Risk assessment being conducted pursuant to E.O. 16-13

xi. ***February 2015.*** *LC 0779 – IT Security Unification and Cybersecurity Center of Excellence*

- LC 779 provides for the unification of IT security within the executive branch and establishes a Cybersecurity Center of Excellence (CCoE), a public-private state-civilian interface for information sharing, coordination of cyber incident response, developing a statewide cyber strategy, identifying best practices and encouraging the development of the cyber-security workforce.

[10] In addition to our Office, the NGA and state agencies, the summit had 24 other attendees, including representatives from: Amazon, the Cascade Technology Alliance, Clackamas Community College, Hewlett Packard Enterprise, Intel, Microsoft, Mt. Hood Community College, Multnomah County, the Departments of Transportation and Education, Oregon State University and the Technology Association of Oregon (TAO). State Senator Chuck Riley and Lisa Howard, on behalf of the Governor's Office, were also in attendance.

[11] Secretary of State Audit, 2016-30. Available at http://sos.oregon.gov/audits/Documents/2016-30.pdf

E.O. 16-13. *“Unifying Cyber Security in Oregon”*

Governor Brown’s Executive Order 16-13, “Unifying Cyber Security in Oregon” (EO 16-13) represents a fundamental shift in how the state of Oregon approaches IT security. At a fundamental level, IT security is about trust—as public servants and custodians of public data, we owe Oregonians a duty to protect their personal information. Regardless of agency mission or size, Oregonians rightfully expect their government to use technology to improve customer service while ensuring those systems are secure and that personal information is subject to consistent protections. Citizen expectations of privacy, should not hinge on the agency with whom they are transacting—be it the Department of Motor Vehicles or Department of Fish and Wildlife (ODFW).

EO 16-13 is the first step towards addressing persistent IT security vulnerabilities and represents the next phase of Oregon’s IT security evolution. It will enable the implementation of a statewide agency-by-agency risk-based security assessment and remediation program that will inform the deliberations of the 2017-19 Legislative Session. While implementing change is inherently disruptive, our Office has made the continuity of IT security operations our first priority—keeping the majority of IT security personnel, protocols and tools in place while working to strengthen the statewide community of IT security professionals.

The planning and initial execution of EO 16-13 has matured substantially since the Secretary of State interviewed our Office, with definition of deliverables, timelines, and regular reporting of status and metrics all in place at this time. Unfortunately, given timing of EO 16-13, this information was not available to be included in audit findings. Our Office had two interviews with the Secretary of State in early September of this year, and the executive order was signed days later on September 12th 2016. The plan for implementation EO 16-13 includes four primary deliverables, developed in collaboration with agencies, boards and commissions, including:

- Completion of an Enterprise Information Security Risk (EISR) Assessment
- Publication and implementation of a new Enterprise Security Plan
- Implementation of an Enterprise Vulnerability Management Program
- Implementation of Enterprise Security Awareness Program

In support of these deliverables, our Office has conducted a statewide IT security survey, initiated public procurements to obtain third-party risk assessments and security awareness training. Additional details regarding these activities will be provided below—the EISR assessment in particular. Additionally, our Office has worked with the DAS Chief Human Resource Office and the Department of Justice to develop an Interagency Agreement (IAA) to facilitate the transfer of IT security functions and personnel from November 1, 2016 until June 30, 2017 (the end of the current biennium). As of December 5th 2016, our Office had executed 47 IAAs, covering all agencies that currently have IT security positions and the 20 agencies that are part of the first phase of the EISR assessment.

ENTERPRISE INFORMATION SECURITY RISK (EISR) ASSESSMENT

The Enterprise Information Security Risk (EISR) assessment is already well underway, with an enterprise-wide IT security survey completed, expert third-party assessment personnel procurement vehicles in place, an assessment approach established and a specific list of initial priority areas for assessment identified. The EISR assessment has four goals, including: i) the development of a risk-based enterprise security profile of the state of Oregon; ii) identification of specific vulnerabilities requiring immediate remediation; iii) the identification of systemic vulnerabilities that should inform the development of an IT security service catalog within the ESO; and development of an inventory and preliminary assessment of external-facing web applications. Web applications have been compromised in several of the most recent IT security breaches (*e.g.,* ODFW and the Construction Contractor’s Board), and up until EO 16-13, neither ETS nor our Office has had any visibility into the state portfolio of these applications.

EISR Assessment Approach

As previously mentioned, the first phase of the assessment includes 20 agencies. Given the sensitivity of IT security information, our Office is not publicly identifying these agencies. The selection of agencies was informed by the enterprise-wide IT security survey, and took into consideration agency size, the sensitivity of agency data and whether the agency had recently undergone a comprehensive IT security review. Taken together, the 20 agencies represent well over 30,000 FTE. In order to ensure cross-agency consistency and comparability, the assessment methodology is based on the NIST Cybersecurity Framework (a national standard that has been widely adopted by other states).[12] Additionally, given cross-agency variation in terms of IT systems, sensitive data and externa-facing applications, our Office has taken a modular approach to the assessment.

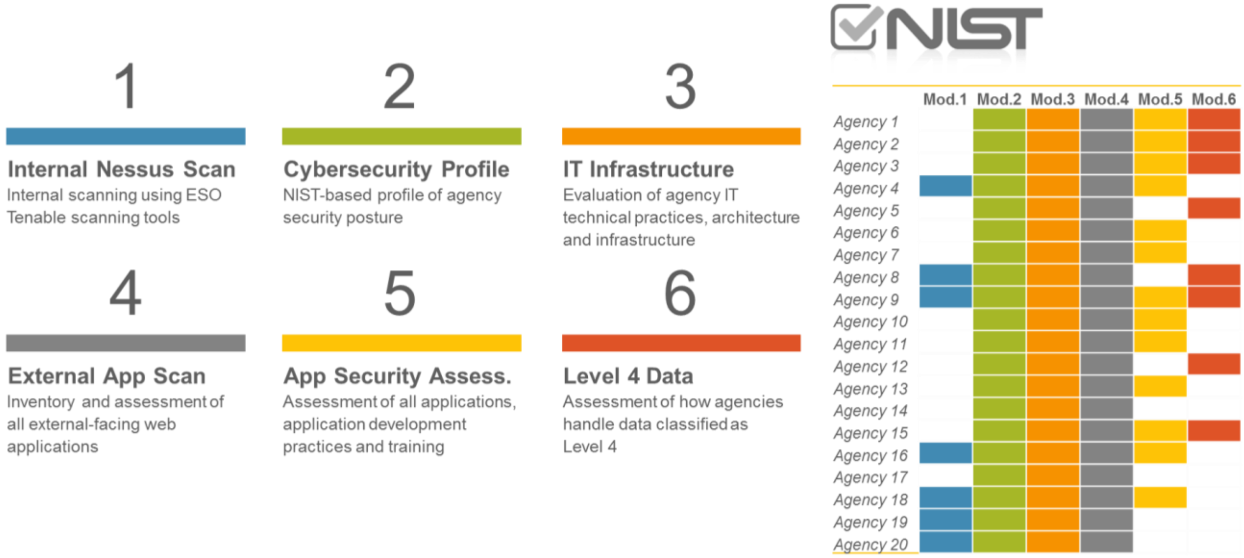
Our Office has developed six assessment modules, including:

1. **Internal Nessus scan.** Internal scanning will be performed with the ESO Tenable scanning tools or with compatible vendor tools
2. **Cybersecurity Profile.** Interview and assessment findings will inform NIST Cybersecurity Framework profile of agency security posture
3. **Infrastructure.** The technical architecture and practices assessment will evaluate agency IT infrastructure (*e.g.,* agency data-centers and servers) and may include internal credentialing scans
4. **External Web Application Scan.** The external application scan will provide an inventory and assessment of all external-facing web applications
5. **Application Security Assessment.** The assessment will include a security review of all applications, application development practices and training
6. **Level 4 Data Practices Assessment**. An assessment of how agencies handle data classified as Level 4 – Critical[13]

[12] National Institute of Science and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014. Available at https://www.nist.gov/cyberframework.

[13] Level 4 data, "Critical" is defined as *"Information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners, or cause major harm to the agency."* Examples would include the identities of law enforcement personnel working undercover or individuals with Hepatitis C—in the latter case, disclosure would pose reputational risks to the named individual.

Fig. 2. EISR Assessment. *Approach and Phase 1 Agencies*



1 **Internal Nessus Scan**
Internal scanning using ESO Tenable scanning tools

2 **Cybersecurity Profile**
NIST-based profile of agency security posture

3 **IT Infrastructure**
Evaluation of agency IT technical practices, architecture and infrastructure

4 **External App Scan**
Inventory and assessment of all external-facing web applications

5 **App Security Assess.**
Assessment of all applications, application development practices and training

6 **Level 4 Data**
Assessment of how agencies handle data classified as Level 4

NIST

	Mod.1	Mod.2	Mod.3	Mod.4	Mod.5	Mod.6
Agency 1		🟩	🟧	⬛	🟨	🟥
Agency 2		🟩	🟧	⬛	🟨	🟥
Agency 3		🟩	🟧	⬛	🟨	🟥
Agency 4	🟦	🟩	🟧	⬛	🟨	
Agency 5		🟩	🟧	⬛		🟥
Agency 6		🟩	🟧	⬛	🟨	
Agency 7		🟩	🟧	⬛	🟨	
Agency 8	🟦	🟩	🟧	⬛		🟥
Agency 9	🟦	🟩	🟧	⬛	🟨	🟥
Agency 10		🟩	🟧	⬛	🟨	
Agency 11		🟩	🟧	⬛	🟨	
Agency 12		🟩	🟧	⬛		🟥
Agency 13		🟩	🟧	⬛	🟨	
Agency 14		🟩	🟧	⬛		
Agency 15		🟩	🟧	⬛	🟨	🟥
Agency 16	🟦	🟩	🟧	⬛	🟨	
Agency 17		🟩	🟧	⬛		
Agency 18	🟦	🟩	🟧	⬛	🟨	
Agency 19	🟦	🟩	🟧	⬛		
Agency 20	🟦	🟩	🟧	⬛		

Vendor Alignment

While our Office is making every effort to leverage recently completed IT security assessments and the results of the enterprise-wide IT security survey, we are also drawing upon the expertise of the private-sector by procuring third-party assessment services. Our Office recently concluded a Request for Proposals (RFP), selecting 9 vendors to provide assessment services—all of whom, who have signed the contract. Under this larger agreement, we are developing individual statements of work that include the assessment modules required for each agency. However, for the sake of consistency, we have selected one vendor to perform all external web application scans. In terms of timing, the assessments will be conducted on a rolling basis—assessments beginning as soon as we have a signed vendor quote based on individual statements of work.

At this point, we have identified the assessment modules required for the first phase of the EISR assessment and assigned a vendor to each of the agencies. Our Office is currently working with agencies to develop agency-specific statements of work; *i.e.,* extent of review, cost and timing. Following execution and close-out of the assessment, we will determine whether immediate remediation is necessary.

ENTERPRISE SECURITY PLAN

The Enterprise Security Plan will identify the current and proposed ownership of all key security areas, be they enterprise or agency-specific. The new Enterprise Security Plan will address the following key areas, including:

- Enterprise security policy, standards, processes and oversight
- Enterprise standards-based controls framework
- Enterprise security tools & services (ex. vulnerability scanning)
- Agency security tools & services (ex. personnel investigations)
- Enterprise security programs (ex. security awareness)

Each area of focus identified in the Enterprise Security Plan will be prioritized based on risk and staffed accordingly, to the furthest extent possible given existing resources. Critical resource gaps that remain will be brought forward to the Governor and Legislature for consideration. Our Office is working to complete a substantial portion of this work in order to inform the 2017 Legislative Session and identify critical resource gaps.

ENTERPRISE VULNERABILITY MANAGEMENT

Our Office has been working to implement an Enterprise Vulnerability Management program since the completion of the Microsoft Security Risk Assessment just over a year ago. EO 16-13 has accelerated program implementation by realigning existing resources and bringing an enterprise focus to these efforts. Our Office will have regular scanning in place within most agencies, boards and commissions by mid-2017. Within the last month, our Office has doubled the number of available licenses for internal scanning equipment. At the same time, our Office is developing the infrastructure and processes necessary to make vulnerability scanning results actionable—moving from findings to fixes, with central oversight and accountability.

While monitoring is currently in place within several agencies and across much of the enterprise, there is little consistency in execution. Holistic centralized monitoring (deep packet analysis of ingress and egress traffic) is not possible due to the federated nature of our enterprise: each agency manages, configures, and maintains their own security solutions and architecture. Current minimum monitoring expectations and oversight are insufficient and will be addressed in the coming Enterprise Security Plan.

ENTERPRISE SECURITY AWARENESS PROGRAM

Our Office has already been working to procure new training for basic IT security awareness. With EO 16-13, our security awareness efforts have been expanded to include driving adoption and measuring compliance. New enterprise security awareness training will be acquired, deployed and tracked to completion by end of June 2017. Furthermore, during this timeframe our Office also plans on defining more rigorous training guidelines for individuals within sensitive job functions; *e.g.,* named individuals who handle Level 4 data.

LC 0771. *Unifying IT Security and CCoE*

With the implementation or EO 16-13 and completion of the EISR assessment, the state of Oregon will have a comprehensive view of its overall IT security posture for the first time. However, in the absence of legislative action, the executive order will expire on June 30th 2017. The executive order represents just the first step in the state of Oregon's IT security evolution. In February, our Office is seeking to introduce legislation, LC 0771, a bill that would make the unification of cybersecurity in Oregon permanent. Additionally, the LC would establish a Cybersecurity Center of Excellence (CCoE) through partnerships with the private-sector and universities.

Currently, Oregon lacks a state-civilian interface for coordinating cybersecurity information sharing and cross-sector incident response, performing cybersecurity threat analysis and remediation, and promoting shared and real-time situational awareness between and among the public- and private- sectors. The CCoE would fulfill this role and enable the state to draw on the expertise and capabilities of the private sector to develop a long-term multi-sector cyber strategy for preventing future threats, responding to cyber disruptions and building capacity across the state and with our local government partners and school districts. The LC would also establish a Cybersecurity Fund within the COoE, enabling it to accept federal and grant funds and enter into public-private partnerships.

ARTICULATING THE MODEL. *The Cybersecurity Center of Excellence*

The vision for the Oregon Cybersecurity Center of Excellence (CCoE) was developed through our partnership with the National Governor's Association (NGA) and informed by their research and continued participation in the Policy Academy on Cybersecurity. Much of the language contained in the LC itself and the CCoE governance model draws directly from HB 2996 (2015)—a bill that was introduced on behalf of the Technology Association of Oregon (TAO) that enjoyed the bipartisan support of sixteen legislators.[14] Our office has partnered with TAO and undertaken extensive stakeholder outreach.

In terms of the overall vision, our Office has embraced a model of collective impact for the CCoE that explicitly draws from public health literature. The CCoE would provide "backbone" support for the multi-sector initiative, act in a convening role to continue refining our common agenda, and provide communications and support, measure progress and work to coordinate mutually reinforcing activities among our higher education, private- and public-sector partners.[15]

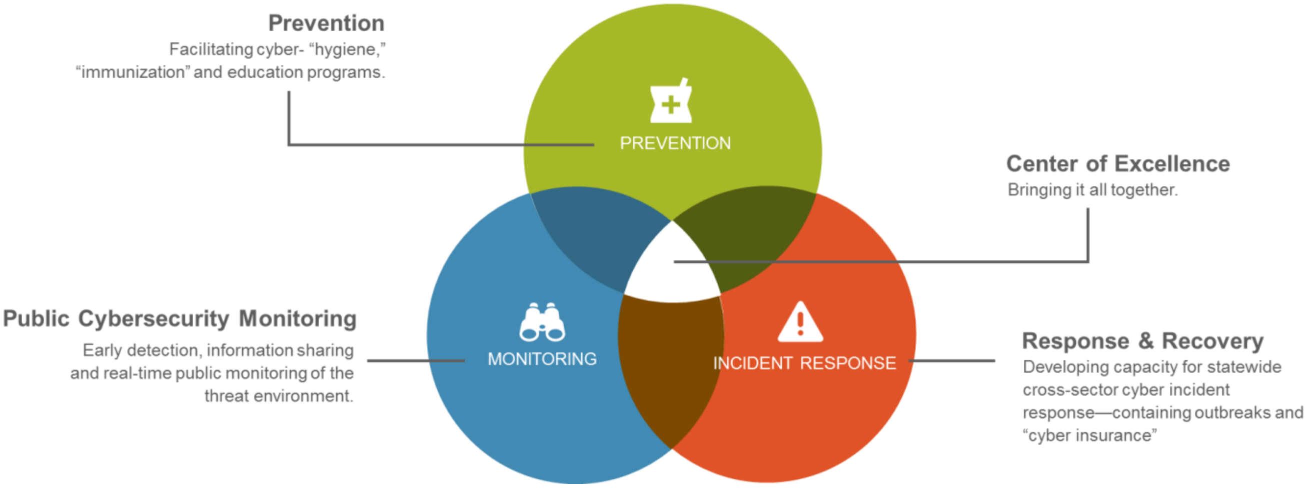
Our vision for enterprise IT security is to transform the culture of our state's IT security professionals to that of a public steward—focused on the seamless integration of security, solutions and personnel into a coordinated multi-sector approach that recognizes cyber security as a public good. While community institutions may fall outside the traditional ambit of state cyber security policy, our interdependence and shared information systems render individual and isolated interventions insufficient to stem the tide of cyber security threats—we are more resilient when we stand together.

[14] Given its fiscal impact and emphasis on workforce development, action on HB 2996 (2015) was deferred due to negotiations on whether to appropriate new funding for economic development. Additionally, the original CCoE was associated with the Department of Business and Consumer Services. LC 0079 unifies IT security within the Executive branch, broadens the scope of the original CCoE, establishes a clear link between the CCoE and the Office of the State CIO and is fiscally neutral. The LC text also draws inspiration from several recent Executive Orders on IT security issued in other states. These are available upon request.

[15] Mark R. Kramer and Marc W. Pfitzer, "The Ecosystem of Shared Value," Harvard Business Review, October 1, 2016, https://hbr.org/2016/10/the-ecosystem-of-shared-value.

While this idea may challenge conventional wisdom, it is part of an active research agenda on "public cybersecurity" and cyber-security as "public health."[16] Our Office has explicitly modeled the CCoE on the public health model proposed by Rowe, Levitt and Hogarth (2013). Their model includes three classes of interventions, including: prevention, public cybersecurity monitoring and response and recovery. These classes of interventions are further classified into either individual- and system-level interventions (summarized below). Individual-level interventions would include the deployment of end-point protection on particular devices such as antivirus, whereas the Enterprise Security Plan, Vulnerability Management Program and Security Awareness Trainings would fall under system-level interventions.

Fig. 3. Public Cybersecurity. *Classes of Interventions*[17]


Prevention
Facilitating cyber- "hygiene," "immunization" and education programs.
PREVENTION
Center of Excellence
Bringing it all together.
Public Cybersecurity Monitoring
Early detection, information sharing and real-time public monitoring of the threat environment.
MONITORING
INCIDENT RESPONSE
Response & Recovery
Developing capacity for statewide cross-sector cyber incident response—containing outbreaks and "cyber insurance"

[16] *See* Deirdre K Mulligan and Fred B Schneider, "Doctrine for Cybersecurity," *Daedalus* 140, no. 4 (2011): 70–92; Elaine M. Sedenberg and Deirdre K. Mulligan, "Public Health as a Model for Cybersecurity Information Sharing," *Berkeley Tech. LJ* 30 (2015): 1687–2073; and Jeff Rowe, Karl Levitt, and Mike Hogarth, "Towards the Realization of a Public Health System for Shared Secure Cyber-Space" (ACM Press, 2013).

[17] *Adapted from* - Jeff Rowe, Karl Levitt, and Mike Hogarth, "Towards the Realization of a Public Health System for Shared Secure Cyber-Space" (ACM Press, 2013).

Fig. 4. Public Cybersecurity. *Individual-level Interventions*[18]

✚ prevention
🔭 monitoring
⚠ response and recovery

Type of Intervention		Cybersecurity Threat: viruses and worms (*e.g., computer viruses and worms installed on a computer*)	poor behavior (*e.g., freely open e-mail attachments and trust all websites*)	distributed attacks (*e.g., DDoS attack aimed at shutting down a server*)
primary prevention—avoid threat	antivirus + endpoint protection	✚		
	firewall	✚		
	avoiding "high-risk" behavior	✚	✚	
	other primary prevention	✚	✚	
secondary prevention—address threat soon after onset to minimize damage	one-time or short –term interventions	⚠		⚠
	ongoing interventions	⚠	⚠	⚠
tertiary prevention—intervene to prevent fully present threat from worsening		⚠	⚠	⚠

Fig. 5. Public Cybersecurity. *System-level Interventions*[19]

✚ prevention
🔭 monitoring
⚠ response and recovery

Type of Intervention	Cybersecurity Threat: Communicable	Noncommunicable	Risky Behaviors	Coordinated
Educational information describing risk factors	✚	✚	✚	✚
High-priority patching	✚			✚
Mandatory individual-level interventions (e.g., network access control)	⚠		⚠	
Regulation of security of software	✚	✚	✚	✚
Secure configuration management				
Guidelines/recommendations for early detection	✚	✚	✚	
Monitoring of potential threat sources	🔭			🔭
Mandatory reporting of new cases for assessment of breaches/trends	🔭	🔭		🔭
Quarantine—isolation of affected individuals (by ISPs)	⚠			

[18] *Adapted from* - Brent Rowe, Michael Halpern, and Tony Lentz, "Is a Public Health Framework the Cure for Cyber Security?," *CrossTalk* 25, no. 6 (2012): 30–38.

[19] Ibid.

Cyber State of the States. Oregon in Context

Just as determining state of Oregon's current IT security posture and articulating a vision for the future are foundational, there is also value in contextualizing these efforts within a national context. While empirical cross-state comparative IT security studies are relatively limited, they provide key insights into how states are confronting cybersecurity challenges—to a large extent, this is a key role fulfilled by the NGA, NASCIO and similar organizations focused on sharing best practices.

In *State of the States on Cybersecurity,*[20] Spidalieri (2015) assesses the cybersecurity posture of ten states who are widely considered national leaders, most notably, the states of Virginia and Michigan. While Oregon was not included in the original analysis, our Office has added Oregon for comparative purposes. It is also worth noting that Governor Terry McAullife of Virginia recently became the Chair of the NGA and has made cybersecurity his signature initiative for 2016-17, entitling it *"Meet the Threat: States Confront the Cyber Challenge"*—particularly, given Oregon's participation in the NGA's Policy Academy on Cybersecurity.

In evaluating, the cybersecurity posture of the states, Spidalieri employs the "Cyber Readiness Index 1.0 (CRI) a comprehensive, comparative, experience-based methodology created to evaluate a country's maturity and commitment to cybersecurity."[21] While the CRI 1.0 may not be exhaustive with respect to cybersecurity best practices, it provides an objective overview of a state's commitment to securing its cyber infrastructure and its relative maturity.

Adapted for application at the state level, the CRI methodology defines the core components necessary for a state to demonstrate cyber readiness within five essential areas, including:

1. **"State Cybersecurity Strategic Plan** (that would include: specific cyber threats to the state and necessary steps, programs, and initiatives that should be undertaken to address identified cyber threats and increase resilience; competent authority—the responsible and accountable entity—that ensures the implementation and execution of the plan, and the adoption of well-established standards and policies; annual threat assessment to government agencies and critical infrastructure networks; adoption of well-known benchmarks, standards, and policies developed by nationally respected groups like NIST; and a strong linkage to the economic health of the state.[22])

2. **Incident Response** (state entity responsible for facilitating incident response in the event of a cyber incident—natural or man-made—that affects critical services and information infrastructure; published and regularly exercised incident response plan for emergencies and crisis that addresses continuity of operations and recovery mechanisms; role of the Homeland Security Advisor and integration with first responder community in the state; role of the state National Guard and/or local Fusion Center in the response to cyber incidents.)

3. **E-crime and Law Enforcement** (commitment to protect residents against cybercrime through laws, such as data breach notification law, and other regulatory governance mechanisms; established relationship with law enforcement officials to interdict and investigate events of fraud, crime, IP theft, privacy breach, and other cyber activities; state's ability to fight cybercrime, including training of law

[20] Francesca Spidalieri, "State of the States on Cybersecurity" (Pell Center for International Relations and Public Policy, November 2015).

[21] Spidalieri at 4.

[22] Melissa Hathaway, "Strategic Advantage: Why you should care about cybersecurity." (Presentation at the Pell Cener Cybersecurity Lecture Series, Newport, RI, November 6, 2013.)

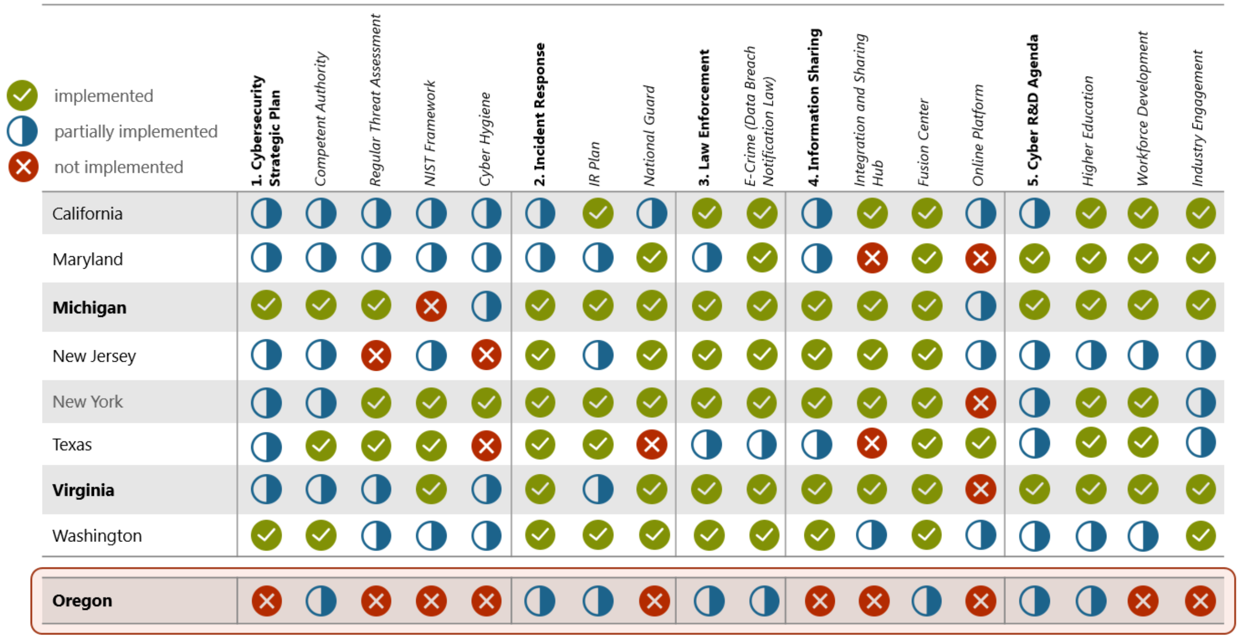
enforcement specialists, forensics specialists, judges, and legislators, and state law enforcement's ability to use tools at their disposal to combat cybercrime.)

4. **Information Sharing** (state information sharing and analysis center and/or mechanisms to enable the exchange of actionable intelligence/information between the state and critical industries; cross-sector and cross-stakeholder coordination mechanisms to address critical interdependencies, share situational awareness, and coordinate incident management; state Fusion Center's capability to collect, analyze, and disseminate timely cyber threat intelligence and information; official state platform/website available to its broader constituency to stay informed on latest cyber threats and other relevant Internet problems and possible solutions.)

5. **Cyber R&D, Education, and Capacity Building** (state investments in cybesecurity research and development; funding dedicated to universities offering degree programs in cybersecurity, information security or similar programs, and to K-12 cybersecurity programs and cyber challenges; partnerships between academia, public and private sectors to promote cyber innovation; state incentives (e.g. tax credit, scholarships, funds and innovation vouchers) to encourage cybersecurity training and workforce development, and to create jobs to serve the tech industry.)"[23]

In applying the CRI 1.0 methodology, Spidalieri (2015) assesses the presence and degree to which a state has implemented 18 separate measures—providing partial credit, where a state has initiated a program but it remains under development. Again while Oregon, was not included in the original evaluation it has been added to underscore the work that remains to be done.

***Fig. 5. Current Cyber Readiness**. Leading U.S. States and Oregon (adapted from Spidalieri, 2015)*



✓ implemented
◐ partially implemented
✗ not implemented

	1. Cybersecurity Strategic Plan	*Competent Authority*	*Regular Threat Assessment*	*NIST Framework*	*Cyber Hygiene*	**2. Incident Response**	*IR Plan*	*National Guard*	**3. Law Enforcement**	*E-Crime (Data Breach Notification Law)*	**4. Information Sharing**	*Integration and Sharing Hub*	*Fusion Center*	*Online Platform*	**5. Cyber R&D Agenda**	*Higher Education*	*Workforce Development*	*Industry Engagement*
California	◐	◐	◐	◐	◐	◐	✓	◐	✓	✓	◐	✓	✓	◐	◐	✓	✓	✓
Maryland	◐	◐	◐	◐	◐	◐	◐	✓	◐	✓	◐	✗	✓	✗	✓	✓	✓	✓
Michigan	✓	✓	✓	✗	◐	✓	✓	✓	✓	✓	✓	✓	✓	◐	✓	✓	✓	✓
New Jersey	◐	◐	✗	◐	✗	✓	◐	✓	✓	✓	✓	✓	✓	◐	◐	◐	◐	◐
New York	◐	◐	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	◐	✓	✓	◐
Texas	◐	✓	✓	✓	✗	✓	✓	✗	◐	◐	◐	✗	✓	✓	◐	✓	✓	◐
Virginia	◐	◐	◐	✓	◐	✓	◐	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Washington	✓	✓	◐	◐	◐	✓	✓	✓	✓	✓	✓	◐	✓	◐	◐	◐	◐	✓
Oregon	✗	◐	✗	✗	✗	◐	◐	✗	◐	◐	✗	✗	◐	✗	◐	◐	✗	✗

[23] Spidalieri at 7-8.

Based on the CRI, both Virginia and Michigan demonstrate substantial commitment and maturity. The only measure completely absent for either state, was the NIST framework for cybersecurity within Michigan. While increasingly viewed as the industry and national standard, a variety of other frameworks and standards exist, including: the International Organization of Standardization's (ISO) 27001 and 27002 and Control Objectives for Information Technology (CoBIT). However, Michigan is not alone, Oregon has historically employed the ISO standards itself, though it has transitioned to the NIST framework in implementing EO 16-13. Looking across the five areas, the state of Oregon lags within nearly every measure.

Beyond developing a state-by-state CRI scorecard, Spidialieri (2015) also contextualizes the cyber threat, provides overarching recommendations and provides a profile of each state—documenting successes, challenges and lessons learned. These overarching recommendations closely align with the "public cybersecurity" model that our Office has proposed to the NGA, including:

- ***Partnerships.*** *"[S]tates should work on building partnerships with the larger security community—including federal, state, and local stakeholders—to coordinate security efforts and equip state employees with the education and training necessary to understand their specific roles and responsibilities in protecting citizens information and maintaining the highest ethical standards.*[24]
- ***New Approaches Required. "****[States] have recognized that the traditional approach to managing security through preventive and risk-based protective measures, while important and necessary, is no longer enough. A handful of states are now leveraging state laws, regulation, standards, market incentives, and other initiatives to align state priorities with national priorities for critical infrastructure security; increase their situational awareness; lower cyber risks; improve their resilience, response, and recovery capabilities; and even turn the cybersecurity challenge into a business opportunity."*[25]
- ***Innovative Initiatives. "****Other more advanced and aggressive solutions have included the establishment of specific state cybersecurity offices or roles with authority over the other state agencies; the use of state National Guard units to combat cyber attacks and responds to cyber incidents; the creation of dedicated Computer Emergency Response Teams (CERTs) or integration centers for information sharing; and the launch of various partnerships among industry, academia, state and federal agencies to promote cyber industry growth, attract federal funding to local universities and companies, and train a new generation of cybersecurity professionals. In addition to state-sponsored initiatives, universities and research institutions around the country are taking advantage of federal grants and scholarships to grow their cybersecurity programs and advance cyber R&D, education, and capacity building in their respective states."*[26]

Furthermore, many of the examples cited within Virginia and Michigan align with the activities that would fall under the ambit of an Oregon CCoE. While there are an increasing number of states employing these non-traditional approaches, given our proximity to the Silicon Forest, the state of Oregon is uniquely positioned to shift the cybersecurity landscape and demonstrate national leadership.

[24] Spidialeri at 4.

[25] Spidialeri at 6.

[26] Ibid.