Secretary of State Audit Report

Jeanne P. Atkins, Secretary of State

Mary Wenger, Interim Director, Audits Division

Improving State Computer System Security will take Time, Resources, and Cooperation

Executive Summary

Most state agencies we reviewed do not have adequate security plans, processes, or staffing to carry out fundamental security functions that protect their information systems and data. The Office of the State Chief Information Officer is responsible for ensuring agencies carry out these critical functions, but has not yet provided sufficient standards and oversight to help agencies achieve appropriate information technology security. In September 2016, the Governor signed an executive order to unify cyber security in Oregon, but much work and cooperation remains to fulfill the requirements of the executive order and improve statewide security.

State agency security efforts fall short

We reviewed 13 state agencies' information security plans and a selection of security functions to determine if agencies were adequately protecting their systems and data. More than half of the agencies had security weaknesses in six of the seven fundamental security controls reviewed and all agencies had at least two weaknesses.

Security Functions Reviewed

Security Planning and Staffing

Vulnerability Management

Network Security

User Account Management

Security Patching and Anti-virus

Replacing Outdated Operating Systems

Security Awareness Training

These agencies represented a cross section of state government agencies. They process and store different types of information ranging from mostly public documents to highly sensitive tax, court, and medical records that require a higher level of protection to comply with federal law.

Overall, planning efforts were often perfunctory, security staffing was generally insufficient, and critical security functions were not always performed. These weaknesses collectively increase the risk of a security incident at one or more of the agencies.

Office of the State Chief Information Officer not fully prepared to centrally administer the state's security function

State law gives the state Chief Information Officer responsibility for planning statewide security, setting security standards and policies, and ensuring remedial actions are undertaken to correct known security weaknesses. However, the Office of the State Chief Information Officer (OSCIO) has not yet provided state agencies with sufficient and appropriate information technology security standards and oversight. In addition, the OSCIO does not have processes to ensure that agencies comply with the published statewide standards and the regulations imposed by federal requirements.

Recent executive order shifts security functions from the agencies to the Office of the State Chief Information Officer but much work remains

In September 2016, the Governor signed Executive Order No. 16-13 *Unifying Cyber Security in Oregon.* This directive outlines a process to unify information technology security, including a process to transfer state agency security functions and staffing into the OSCIO until June 30, 2017. In addition, it directs agencies to work with the OSCIO's newly formed security group to develop and implement security plans, rules, policies, and standards. The directive also requires agencies to fully cooperate with the OSCIO to implement a statewide agency-by-agency risk-based security assessment and remediation program.

However, the executive order may not fully resolve the state's information technology security weaknesses. The need to securely operate information systems competes for resources with the needs of the agencies to provide services to Oregonians. The executive order transfers security functions but does not add additional resources or describe how agency security staff will work with the OSCIO while remaining under agency management direction for day-to-day activities. In addition, at the time of this report, the OSCIO has not yet developed plans detailing how the OSCIO and agencies will achieve the requirements of the executive order.

Ultimately, the Governor, the OSCIO, agency directors, and the Legislature must cooperate to create, fund, endorse, and implement a statewide security plan. Without full cooperation of these key stakeholders, it is unlikely that the state's security posture will significantly improve.

Recommendations

We recommend that the Office of the State Chief Information Officer:

- Collaborate with state agencies to develop detailed plans in order to fully implement the requirements of Executive Order No. 16-13.
- Develop sufficient statewide standards and processes for oversight to ensure security of agency computer systems.
- Collaborate with state agencies to ensure remediation of the specific weaknesses communicated to state agencies in separate management letters.

- Work with the Governor, Legislature, and agency directors to ensure staffing and resources are available to implement agency security measures.

Agency Response

The Office of the State Chief Information Officer generally agrees with the findings and recommendations in this report. The full agency response can be found at the end of the report.

Background

State computer systems contain a wide variety of private and public information

Oregon state government is comprised of more than 300 separate agencies, boards, and commissions operating hundreds of computer applications. Each entity has a specific mission to support the citizens and businesses of the state. The range of services these entities provide is broad and diverse.

Many of the services involve collecting, processing and storing sensitive citizen information and collecting money in the form of taxes, fees, and grants. Agencies use mission critical systems to obtain and store this information, which includes personal income tax data, Social Security numbers, driver license information, and confidential education and medical records.

Internet connectivity makes computer systems more vulnerable to attack

Many of Oregon’s computer applications were designed and implemented before the Internet became an integral part of business activities. As state agencies began connecting to the Internet, they allowed the public to connect to them. The proliferation of devices that can access online sites has grown exponentially. In addition, we now have state workers teleworking from their homes.

The amount of state information and services available to citizens and businesses online has exploded, making it easier to find and use state services. A few examples of the many state services available online include vehicle registration renewals, unemployment insurance claims, and applications for various business-related licenses. These services can be accessed from any computer allowing citizens to do business with the state without leaving their home or office.

The growth of online services increases the risk of hackers breaching state systems. The number of data breaches occurring across all industries and government has grown worldwide. In addition, the state faces organized groups of hackers with a wide range of motives. Some want to make money by selling confidential information, others want to make political or social statements, and others may want to embarrass or weaken government.

With the wide variety of motives comes a wide variety of attacks (see Figure 1). Many of the attacks today are elaborate and not easy to detect. As a result, finding security solutions is difficult.

Figure 1: Examples of Internet Attacks

Type of threat	Description
Phishing	Emails with hyperlinks that direct the user to provide sensitive information such as usernames and passwords through a fake, but realistic looking, website.
Ransomware	Malicious software that encrypts a computer system's files preventing access without paying a ransom to unlock the files.
Viruses, Worms, and Trojans	Malicious software that infects computer systems or networks so attackers can gain access to systems and files.
Exploiting software weaknesses	Outdated software often has known vulnerabilities that could allow hackers to gain access to computer systems and files.

Allowing the right people into state computers and keeping the wrong people out is not only an expectation, it is required by law. Federal laws require state agencies to protect much of the information they routinely use and store. Examples include tax information, Social Security numbers, minors' criminal information, and medical records.

To counteract ever-growing threats to citizens' personal information, the Oregon Legislature passed Senate Bill 583 in 2007, requiring all organizations to protect citizens' personally identifiable information by implementing robust security controls. As a result, agencies entrusted with personally identifiable information must develop and maintain a security framework of policies, procedures, and technical strategies based on the business needs of its customers as well as current risk and vulnerability assessments. This framework should clearly define security roles and responsibilities, including governance of security functions. Management should also ensure technical controls are in place to protect the computing environment by providing a layered defense against internal and external threats.

IT security requires agencies' cooperation

State law places the state Chief Information Officer, who reports directly to the Governor, in a central position of leadership and accountability for security for most state agencies. The state Chief Information Officer's statutorily defined responsibilities include planning for statewide security, setting security standards and policies, and ensuring remedial actions are undertaken to correct known security weaknesses. In addition, the office is charged with collaborating with state agencies to achieve information technology security.

The Office of the State Chief Information Officer (OSCIO) provides centralized computer services to many state agencies, including operation of the state's data center. To cover operating costs, the state data center charges for services according to a predetermined rate schedule. The data center provides Internet service and networking for the majority of state agencies. It also hosts the majority of computer systems for 11 agencies that rely on the data center to provide a secure environment for their computer applications.

The state data center generally controls the infrastructure where computer applications operate and data is stored. Its staff also manage the networking that connects agency staff with central processing, mainframe computers or servers, and to the Internet, which is the door to the outside world.

State agencies have only limited ability to control or see into this environment but retain responsibility for operating and securing their computer applications. Agencies also are responsible for updating middleware, which is software needed as a bridge between the operating system and a computer application. Because security is no stronger than its weakest link, agencies and the state data center must ensure their individual security responsibilities are adequately performed.

Audit Results

Most state agencies we reviewed do not provide adequate security for computer programs and data. Their planning efforts were often perfunctory, security staffing was generally insufficient, and critical security functions were not always performed.

In addition, the Office of the State Chief Information Officer (OSCIO) is not yet prepared to provide needed standards or oversight to ensure security of the state's computer systems.

In September 2016, Governor Brown signed Executive Order No.16-13 *Unifying Cyber Security in Oregon* (see Appendix A). This order directs most state agencies within the executive department to consolidate security functions and staffing into the OSCIO. In order for these efforts to improve statewide security, the OSCIO and the agencies must be unified in a concerted effort to identify, prioritize, and resolve statewide security issues. In addition, complex governance issues and competition for staffing and other resources need to be resolved.

Longstanding security weaknesses remain at the state data center and agencies

For more than 15 years, audits of state agency systems and controls have identified significant security weaknesses with computer systems and controls at state agencies. Examples of these security weaknesses include inadequate software development and user account management. Many of these weaknesses remain unresolved because agency missions focus on serving citizens and partners, not securing information systems.

In addition, agencies rely on the state data center to perform critical security functions. However, as we found in a 2015 audit of the state data center, nearly all security weaknesses identified in previous audits remained unresolved. These weaknesses have persisted since the inception of the state data center because management did not follow through with plans to assign responsibility and provide sufficient staff to implement and maintain security systems.

Since then, the state Chief Information Officer changed the organizational structure of the state data center. The changes increased management's focus on security at the state data center. Still, the weaknesses will take time, perseverance, and significant resources to resolve.

Agency security efforts fall short

To provide adequate security, each agency needs an entity wide information security management program. Agency management should create a documented plan based on an IT risk assessment that identifies the agency's specific business needs, requirements, and related technology threats and vulnerabilities. Security plans should also be a roadmap for maintaining security infrastructure and defining the necessary resources to accomplish critical objectives.

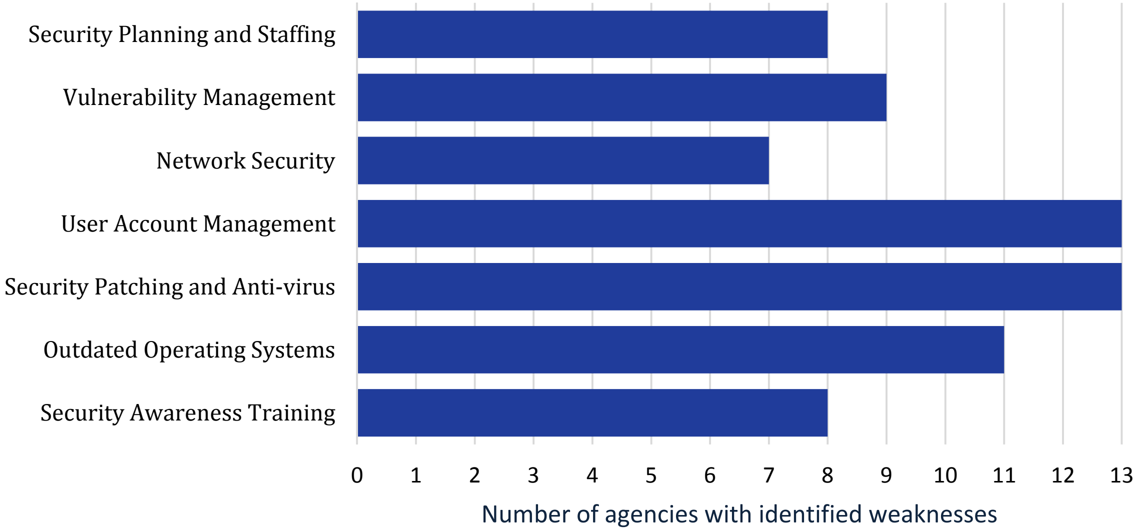
One important objective for information security is controlling who can access state IT systems and networks. Key control points include monitoring networks for telltale signs of attack and ensuring access to state networks is granted to only authorized users. In addition, network accounts should be reviewed periodically to ensure ongoing access remains authorized.

In order to ensure that computer servers and user workstations remain secure against known vulnerabilities, agencies should have processes to identify and correct technical weaknesses that could allow a system to be compromised. These weaknesses include missing security updates for operating systems or middleware, outdated or disabled anti-virus software, and insecure system configurations. In addition, agencies should ensure that operating systems on servers and user workstations remain current because vendors generally stop releasing security updates for older software after a specified amount of time, potentially leaving outdated systems vulnerable to attack.

Best practices also call for employees to participate in mandatory security awareness training, since employees can be one of the weakest links in information security. These trainings should occur on a recurring basis to help protect against threats such as phishing attempts where employees unwittingly share usernames and passwords with unauthorized people.

We reviewed information security at 13 state agencies and found that many have not implemented all the necessary information technology security programs and controls to protect their computer systems and data (see Figure 2 below).

Figure 2: Summary of Security Weaknesses



Agencies Reviewed

Department of Consumer and Business Services (DCBS)

Department of Corrections (DOC)

Oregon Department of Education (ODE)

Oregon Employment Department (OED)

Oregon Department of Forestry (ODF)

Oregon Department of Fish and Wildlife (ODFW)

Oregon Health Authority (also provides IT services to the Department of Human Services) (OHA|DHS)

Department of Justice (DOJ)

Oregon Parks and Recreation Department (OPRD)

Department of Revenue (DOR)

Oregon State Police (OSP)

Oregon Department of Transportation (ODOT)

Oregon Youth Authority (OYA)

A few agencies had only one or two weaknesses, but more than half had weaknesses in six of the seven areas reviewed. Some agencies were missing only a part of a control, while others had significant deficiencies. Some agencies have much less risk because their computing systems are not as complex and may not contain critical or sensitive information. Other agencies have enormous challenges with complex payment systems that have highly sensitive citizen information that is required to be protected under federal regulations.

Because of the sensitive nature of security, we communicated detailed information about security weaknesses to each agency in separate confidential letters according to ORS 192.501 (23).

Security planning and staffing is insufficient

Most agency security planning documents were inadequate because they were not based on an IT risk assessment designed to identify the unique security needs and risks of the agency. In addition, two agencies did not have security plans.

Without sufficient planning, security managers are less able to acquire sufficient staff dedicated to security functions and critical security roles and duties may not be assigned. In this respect, we noted three of the agencies reviewed did not have a dedicated security officer and one agency assigned part of the security officer’s time to network functions. In addition, we noted that agency management did not always provide the necessary staff to implement security measures identified in the planning documents.

Agency efforts to resolve vulnerabilities are inadequate

The OSCIO purchased software that agencies can use to perform vulnerability scans across their network. These scans report missing patches and other configuration issues that make systems susceptible to compromise. Of the 13 agencies reviewed, 11 performed vulnerability scans. Nine of the 11 were using the system provided by the OSCIO.

However, we noted that six of the agencies using scanning software had not yet developed processes to follow up on the vulnerabilities identified. Agencies reported that vulnerabilities could not always be corrected timely because the vulnerable software or operating system was needed to provide a critical business function. Without these processes, agencies have an increased risk that unauthorized users may gain access to critical information systems.

Network monitoring efforts are not robust

Most agencies we reviewed rely on the state data center to manage their networks, including monitoring network traffic for signs of attack. Although the state data center provides some network monitoring, these efforts are not designed to provide the detail necessary to adequately protect agency systems. In addition, of the five agencies that managed their own networks, three did not have sufficient network monitoring tools in place to identify potentially malicious traffic.

The absence of robust network traffic monitoring tools weakens an agency's overall ability to provide security because dangerous network traffic or attacks may not be timely detected and their adverse effects appropriately mitigated.

In addition, we noted one agency had an older wireless network that allowed access to internal resources without appropriate identification and authentication. This could allow unauthorized users to access agency systems and data.

User account management issues are pervasive

Agencies generally had processes in place to ensure that management authorized network accounts using role based access methodology. In addition, most agencies had some processes in place to periodically identify and disable network accounts that were not actively being used. However, most agencies did not require system or data owners to periodically review user accounts to ensure that ongoing access remained appropriate.

A number of agencies have implemented a tool capable of monitoring changes to their network groups through reports or real-time alerts. However, most of these agencies have not yet configured the application to provide reports for periodic review of network accounts.

Technical staff at most agencies indicated they usually receive notification from their human resources department when employees leave the agency or transfer to a different position. A few agencies indicated that they receive separation notices from the Department of Administrative Services' payroll unit as well. However, neither of these notifications included external partners or employees from other state agencies who had been granted access to agency systems, making it harder for agencies to ensure that only authorized users retained access to their systems.

Security patches not always applied and anti-virus software missing or outdated

We tested five to ten workstations and servers at each of the agencies to determine if operating system and specific middleware patches were current, and anti-virus software was installed.

All 13 agencies had at least one patching issue and more than half had one or more missing middleware updates on workstations and servers. Three agencies were missing anti-virus software on some workstations and seven were missing anti-virus on some servers.

These issues indicate weaknesses in agencies' strategies for ensuring operating systems and middleware are appropriately updated to reduce the risk that systems could be compromised.

Agencies rely on outdated operating systems

Generally speaking, software vendors do not provide security patches for their products after a set period of time. They routinely announce when they will stop providing these updates for older versions of their software products.

Of the 13 agencies reviewed, 11 indicated they were using servers with unsupported operating systems and nine reported they had workstations with unsupported operating systems. Continuing to use unsupported server and workstation operating systems increases the risk that agency computer programs and data could be compromised.

Employee security awareness training is insufficient

Eight of the reviewed agencies did not provide sufficient security awareness training to staff. Of those, one agency did not have any security awareness training available to staff and the other seven agencies only had training at the time of hire or did not require attendance. The recently signed Governor's executive order addresses this weakness by directing most executive branch agencies to conduct and document OSCIO approved information security training on an annual basis.

Without periodic security awareness training, employees are less likely to recognize potential attacks and may inadvertently share usernames and passwords with unauthorized users or otherwise compromise agency systems.

The Office of the State Chief Information Officer is not fully prepared to centrally administer the state's security function

The OSCIO has not yet provided state agencies with sufficient and appropriate IT security standards and oversight. State law places the state Chief Information Officer in a central position of leadership and accountability for security for most state agencies. Statutorily defined responsibilities include planning for statewide security, setting security standards and policies, and ensuring remedial actions are undertaken to correct known security weaknesses.

In 2009, the Department of Administrative Services released a high-level statewide security plan and standards. However, these standards were insufficient to address the security needs of many state agencies. During 2016, the Chief Information Security Officer and his staff worked with a group of agency staff to update the standards. However, this group did not make significant changes. Hence, the standards continue to remain insufficient for agencies with significant confidential data and those required by federal law to have additional protection measures.

The OSCIO also has not developed oversight processes to ensure that agencies comply with the published statewide standards and regulations imposed by federal requirements.

Executive Order shifts security functions to OSCIO but much work remains

Recognizing these weaknesses, the Governor signed Executive Order No. 16-13 *Unifying Cyber Security in Oregon* on September 12, 2016. The executive order outlines a process to unify IT security functions in order to protect and secure information entrusted to the State of Oregon. This directive includes a process to transfer executive department state agency security functions and staffing into the OSCIO until June 30, 2017. In addition, it directs agencies to work with the OSCIO's newly formed security group to develop and implement security plans, rules, policies, and standards adopted by the OSCIO. The directive also requires agencies to fully cooperate with the OSCIO to implement a statewide, agency-by-agency risk-based security assessment and remediation program.

As of the time of this report, the OSCIO has developed proposed milestones related to security and education awareness, risk assessments, and vulnerability scanning. However, few details are available regarding how the OSCIO and the agencies will achieve the requirements of the executive order. In addition, the executive order may not fully resolve the weaknesses because managing security for computer systems and data within state government is a complicated process with several competing priorities. Ultimately computer systems exist to help agency staff more efficiently and effectively perform needed services. However, use of computers must be done securely to protect state assets and citizens' sensitive information. Both requirements require staffing and other resources.

The executive order transfers security functions from agencies to the OSCIO without adding additional staffing or resources. In addition, the executive order may lead to confusion for agency security staff transferred to the OSCIO but who remain under agency management direction for day-to-day activities. For example, it is not yet clear how agency security staff will split time between the work directed by the OSCIO and agency operational needs.

The executive order also does not resolve the problem of scarce funding and competing priorities. Ultimately, the Governor, the OSCIO, agency directors, and the Legislature must cooperate to create, fund, endorse, and implement a statewide security plan. Without full cooperation of all stakeholders, it is unlikely that the state's security posture will significantly improve.

Recommendations

We recommend that the Office of the State Chief Information Officer:

- Collaborate with state agencies to develop detailed plans in order to fully implement the requirements of Executive Order No. 16-13.
- Develop sufficient statewide standards and processes for oversight to ensure security of agency computer systems.
- Collaborate with state agencies to ensure remediation of the specific weaknesses communicated to state agencies in separate management letters.
- Work with the Governor, Legislature, and agency directors to ensure staffing and resources are available to implement agency security measures.

Objectives, Scope and Methodology

The purpose of this audit was to evaluate state agency efforts to provide security for their computer systems and data. Our audit objectives were to determine whether:

- State agencies have implemented the necessary information technology (IT) security programs and controls to protect their computer systems and data.
- The Office of the State Chief Information Officer provides state agencies sufficient and appropriate IT security standards and oversight to ensure security of agency computer systems.

To achieve the first objective, we conducted reviews of 13 agencies between September 2015 and September 2016. We conducted interviews, reviewed applicable policies and guidelines, and performed limited testing of specific system configurations and user account management practices. We limited our review of user account management to network accounts managed by Microsoft Active Directory and Novell Netware.

We selected agencies of different sizes with different types of information. In addition, some of the agencies utilize the state data center for nearly all of their computing resources while others maintain all or part of their own infrastructure. We also chose to review one agency that is independent of the Governor's authority.

The 13 agencies involved in the review included:

- Department of Consumer and Business Services
- Department of Corrections
- Oregon Education Department
- Oregon Employment Department
- Oregon Department of Forestry
- Oregon Department of Fish and Wildlife
- Oregon Health Authority (also provides IT services to the Department of Human Services)
- Department of Justice (independent of the Governor's authority)
- Oregon Parks and Recreation Department
- Department of Revenue
- Oregon State Police
- Oregon Department of Transportation
- Oregon Youth Authority

Because of the sensitive nature of security, we communicated the extent of the security weaknesses to each agency in separate confidential letters according to ORS 192.501 (23). Copies of the confidential letters were also provided to the OSCIO.

To achieve our second objective, we interviewed staff with the Office of the State Chief Information Officer (OSCIO) and Enterprise Security Office, reviewed state standards against International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 & 27002, reviewed state information security guidance, analyzed archived legislative records, and documented applicable laws, rules, and regulations.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained and reported provides a reasonable basis to achieve our audit objective.

Auditors from our office, who were not involved with the audit, reviewed our report for accuracy, checking facts and conclusions against our supporting evidence.

Appendix A

Office of the Governor
State of Oregon

EXECUTIVE ORDER NO. 16-13

UNIFYING CYBER SECURITY IN OREGON

WHEREAS, information systems, networks, and critical infrastructure around the world are threatened by increasing and evermore sophisticated cyber-attacks; and

WHEREAS, the people of and businesses operating within Oregon have entrusted state government with a large repository of information that they expect will be protected and secured; and

WHEREAS, information is a strategic asset of the state of Oregon that should be managed and secured as a valuable state resource; and

WHEREAS, the continuous and efficient operation of state government information systems is both vital and necessary to the mission of providing government services in Oregon; and

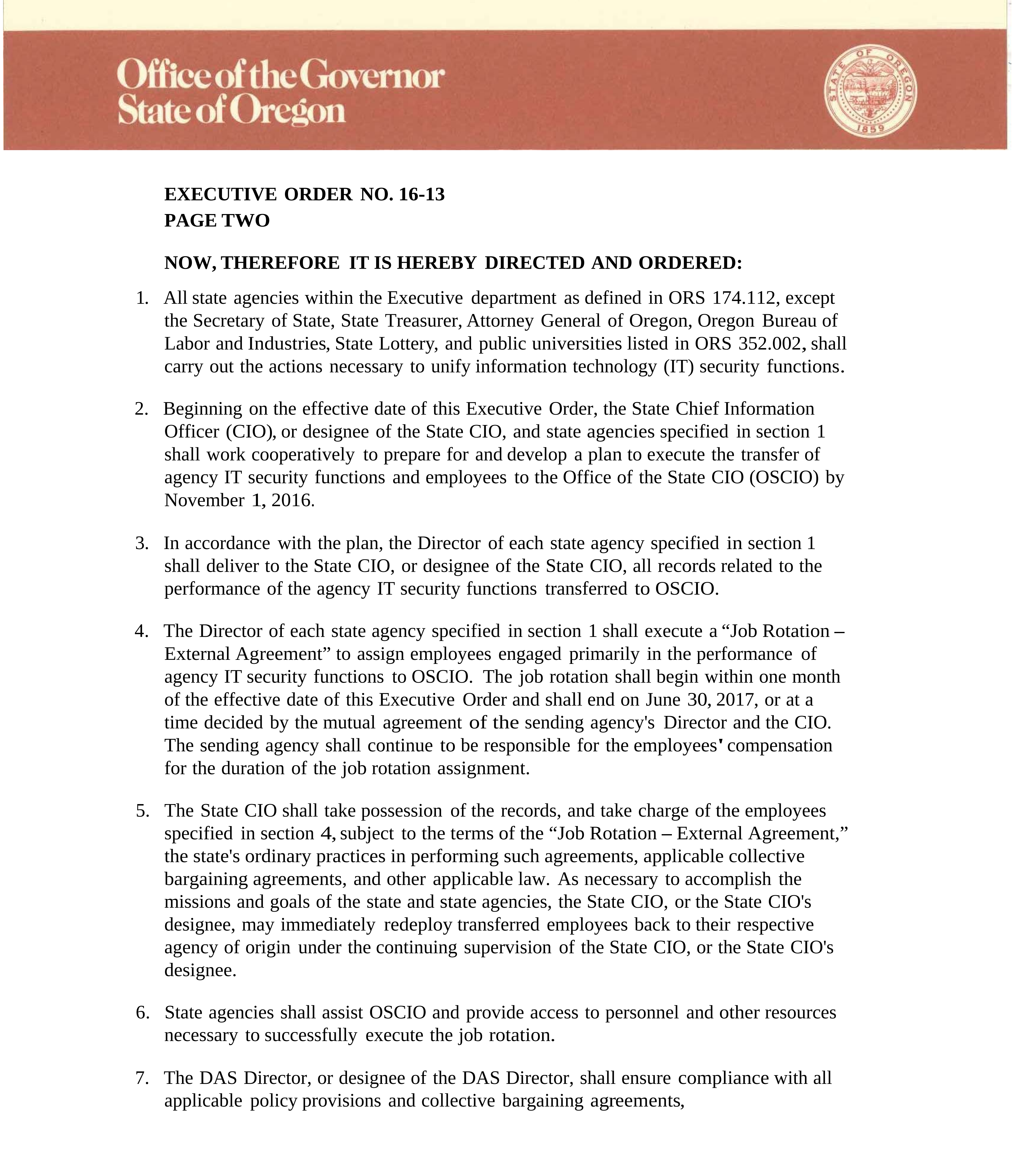
WHEREAS, vulnerabilities of the state's information systems underscore the need to enhance the security of Oregon information systems, networks, and critical infrastructure; and

WHEREAS, aging information technology infrastructure and antiquated legacy information systems in use by state agencies remain vulnerable to cyberattack, placing private information about state employees and their dependents, consumers of state services, taxpayers, and the residents and businesses of Oregon at risk; and

WHEREAS, responsibility and accountability for the security of state information systems is currently dispersed and decentralized with the exception of the enterprise information resources, technology, and telecommunications infrastructure managed and overseen by the State Chief Information Officer.

WHEREAS, ORS 182.122 imposes on state agencies the responsibility to secure their information systems or implement information security plans, policies, standards, and procedures established by the State Chief Information Officer; and

WHEREAS, unification of the state's cyber security functions under the leadership of the State Chief Information Officer is necessary to protect the availability, integrity, and confidentiality of state information systems and the information stored in state information systems pursuant to ORS 182.122;



Office of the Governor
State of Oregon

EXECUTIVE ORDER NO. 16-13
PAGE TWO

NOW, THEREFORE IT IS HEREBY DIRECTED AND ORDERED:

1. All state agencies within the Executive department as defined in ORS 174.112, except the Secretary of State, State Treasurer, Attorney General of Oregon, Oregon Bureau of Labor and Industries, State Lottery, and public universities listed in ORS 352.002, shall carry out the actions necessary to unify information technology (IT) security functions.

2. Beginning on the effective date of this Executive Order, the State Chief Information Officer (CIO), or designee of the State CIO, and state agencies specified in section 1 shall work cooperatively to prepare for and develop a plan to execute the transfer of agency IT security functions and employees to the Office of the State CIO (OSCIO) by November 1, 2016.

3. In accordance with the plan, the Director of each state agency specified in section 1 shall deliver to the State CIO, or designee of the State CIO, all records related to the performance of the agency IT security functions transferred to OSCIO.

4. The Director of each state agency specified in section 1 shall execute a “Job Rotation – External Agreement” to assign employees engaged primarily in the performance of agency IT security functions to OSCIO. The job rotation shall begin within one month of the effective date of this Executive Order and shall end on June 30, 2017, or at a time decided by the mutual agreement of the sending agency's Director and the CIO. The sending agency shall continue to be responsible for the employees' compensation for the duration of the job rotation assignment.

5. The State CIO shall take possession of the records, and take charge of the employees specified in section 4, subject to the terms of the “Job Rotation – External Agreement,” the state's ordinary practices in performing such agreements, applicable collective bargaining agreements, and other applicable law. As necessary to accomplish the missions and goals of the state and state agencies, the State CIO, or the State CIO's designee, may immediately redeploy transferred employees back to their respective agency of origin under the continuing supervision of the State CIO, or the State CIO's designee.

6. State agencies shall assist OSCIO and provide access to personnel and other resources necessary to successfully execute the job rotation.

7. The DAS Director, or designee of the DAS Director, shall ensure compliance with all applicable policy provisions and collective bargaining agreements,

including providing any notices required thereunder within the applicable time periods.

8. All state agencies shall cooperate in the development of and follow the plans, rules, policies, and standards adopted by the State CIO. Further, all state agencies shall provide OSCIO with full cooperation in the implementation of a statewide agency-by-agency risk-based security assessment and remediation program. The State CIO shall determine and charge the costs incurred by the program for third-party security evaluations, vulnerability assessments, other related technical services, and remediation measures to the state agencies that the State CIO serves. The state agency shall pay the cost to the State CIO in the same manner that other claims are paid. Additionally, state agencies will conduct and document the completion of OSCIO approved information security awareness training for all agency employees on an annual basis; report security metrics using methodologies developed by the OSCIO; and participate in activities coordinated by the OSCIO in order to better understand and address security incidents and critical cyber security threats to the state.

9. This Executive Order shall remain in effect until it is otherwise modified, amended or terminated.

Done at Salem, Oregon, this 12th day of September, 2016.

Kate Brown
GOVERNOR

ATTEST:

Jeanne P. Atkins
SECRETARY OF STATE

Oregon
Kate Brown, Governor

Department of Administrative Services
Chief Information Office
155 Cottage St NE, 4th Floor
Salem, OR 97301
PHONE: 503-378-3175
FAX: 503-378-3795

November 29, 2016

Teresa Furnish
Oregon Secretary of State
Audits Division
255 Capitol St. NE, STE 500
Salem, OR 97310

Re: SOS Statewide Security Audit

Dear Miss Furnish:

Summary Response

The Office of the State CIO (OSCIO) generally agrees with the findings and recommendations in this report. Pursuant to the Governor's Executive Order 16-13, *"Unifying Cyber Security in Oregon*" our Office is conducting an enterprise-wide information security risk assessment—working closely with agencies, boards and commissions across state government to identify and prioritize information security weaknesses. The risk assessment is scheduled for completion by mid-2017. The OSCIO will follow-up the risk assessment with a comprehensive enterprise security plan for robust continuous information security management, providing clarity on ownership, accountability, priorities, requirements, policy, oversight and execution of information security functions statewide. The new Enterprise Security Plan is expected to be published and initiated by summer of 2017.

Response to Findings

The Office of the State CIO (OSCIO) generally agrees with the findings and recommendations in this report. Under the Governor's Executive Order 16-13 (EO), the OSCIO is working closely with agencies, boards and commissions across state government to identify and prioritize information security weaknesses based on enterprise-wide information security risk assessment scheduled for completion by mid-2017. The Secretary of State Audit Report will help to inform that activity.

The OSCIO will follow-up the risk assessment with a comprehensive Enterprise Security Plan for robust continuous information security management, including specific clarity on ownership, accountability, priorities, requirements and execution of information security functions statewide. The enterprise plan is expected to be published and initiated by summer 2017.

A specific response to each finding follows:

Security planning and staffing is insufficient

Agree. The security planning efforts already underway as part of the EO 16-13 are focused on risk identification and prioritization—getting available security resources applied to areas of highest risk, while enumerating specific security gaps and determining statewide security needs.

Agency efforts to resolve vulnerabilities are inadequate

Agree. An Enterprise Vulnerability Management Program has been under development for over a year. The EO has accelerated program implementation by realigning existing resources and bringing and enterprise focus to these efforts. Our Office will have regular scanning in place within most agencies, boards and commissions by mid-2017. 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.

Network monitoring efforts are not robust

Agree. While monitoring is in place in several agencies 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 is insufficient and will be addressed in the coming Enterprise Security Plan.

User account management issues are pervasive

Agree. User account management is one of the most difficult areas to address consistently across a highly decentralized operating environment. The coming Enterprise Security Plan will address minimum expectations around user account management, as well as a means for ensuring minimum standards are maintained over time.

Security patches not always applied and antivirus software missing or outdated

Agree. Like user account management, patch management is one of the tougher areas to address consistently within a highly decentralized operating environment. The Enterprise Vulnerability Management Program efforts mentioned previously will help to bring measurement and alerting to this key area, identifying patching issues that create significant vulnerabilities. This program will also address how best to integrate regular scanning and risk assessment into regular IT processes at each agency, with oversight to ensure continued vigilance.

Agencies rely on outdated operating systems

Agree. Enterprise scanning program will help with consistent identification of issues. The continued work to establish an Enterprise Vulnerability Management Program will bring the consistent execution and oversight needed to drive an organized process for granting exceptions that include plans for remediation. OSCIO needs to define security architectural options for systems that must remain on old operating systems under an exception to limit the potential for damage to enterprise.

Employee security awareness training is insufficient

Agree. The OSCIO was already working on acquisition of new training for basic security awareness. With the EO, this effort has 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 as part of the execution of the EO. We also plan to define training guidelines for individuals needing specific training due to their job functions in 2017.

The OSCIO not yet provided sufficient and appropriate IT security standards and oversight

Generally agree. The Enterprise Security Office (ESO) undertook a rewrite of the Information Security Standards in collaboration with eleven (11) agencies including a representative from Secretary of State as well as members of ESO. The effort began in December of 2015 and concluded in June 2016, the primary task was to rewrite the Standards in alignment with ISO 27002-13 from a technical point of view, as well as make specific updates in key areas of risk based on past incidents and current attack landscape.

While this does not provide all standards in one document, this approach was undertaken as the remaining ISO domains (Organization of Information Security, Security Policies, Human Resource Security, Information Security Incident Management, Information Security Aspects of Business Continuity Management and Compliance) are more people and process related and did not fit within the Technical Framework of the Information Security Standards.

Enterprise policy & standards are based on a common baseline, so specific compliance requirements for specific sectors will still need to be a focus locally in agencies where those apply. It would not be a prudent use of resources to apply high water mark across all data and systems.

The revised Information Security Standards have been approved by both the Information Security Council Members and the Chief Information Officers Council, they will be published in 2016. Policy & guidance also being reworked with a focus on a more prescriptive stance to ease agency adoption and tighter oversight to ensure compliance. These updates will be published in 2017 in conjunction with release of the new Enterprise Security Plan.

Executive Order shifts security functions to OSCIO but much work remains

The planning and initial execution of Governor Brown's Executive Order 16-13 (EO) greatly matured since audit was conducted, with very clear actions, timelines, and regular reporting of status and metrics all in place at this time. Given timing of EO 16-13, this was not available to be included in audit findings. The plan for implementation of the EO includes 4 primary deliverables, being worked in collaboration with all agencies, boards, and commissions:

- Complete Enterprise Information Security Risk Assessment
- Publish and implement a new Enterprise Security Plan
- Instantiate a robust Enterprise Vulnerability Management Program
- Implement Enterprise Security Awareness Program

The Enterprise Information Security Risk Assessment is already underway, with enterprise-wide survey completed, expert third-party assessment personnel contracted, assessment approach established and specific list of initial priority areas for assessment identified. Vendors to assist with this work have been contracted and matched to specific agencies and risk areas. Statements of work for specific assessment work are being developed now, with work initiating in

December. The results of this assessment will inform development of a new Enterprise Security Plan.

The Enterprise Security Plan identify clear current and future proposed ownership of all key security areas, be they enterprise or agency provided. The new Enterprise Security Plan will address the following key areas, some of which this audit identified as current weaknesses:

- 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 in risk order using existing resources. Critical resource gaps that remain will be brought forward to the Governor and Legislature for consideration. Our hope is to complete a substantial portion of this work in time to inform 2017 legislative session.

Audit Recommendations

The OSCIO generally agrees with the recommendations of this audit report and is already executing to them as detailed in responses to specific findings above.

Not all gaps identified in this audit report are of equivalent risk level. With limited resources available, a balance must constantly be struck to address the highest risks while mitigating and/or accepting some smaller risks. Gaps identified in this audit report will be mitigated to lowest level practical based on risk assessment and available resources. Ultimately, some level of risk will always need to be accepted.

As the audit report observes, risk management within Oregon state government is generally ad-hoc with inconsistent oversight from the OSCIO. This will be addressed in a new Enterprise Security Plan and applied to the gaps identified in this audit report.

Areas that cannot be brought to an acceptable level of risk due to resource availability will be enumerated, with risk associated, to help shape current and future discussions around additional resources with the Governor and Legislature.

Sincerely,

Alex Z. Pettit, Ph.D.
State Chief Information Officer

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of her office, Auditor of Public Accounts. The Audits Division exists to carry out this duty. The division reports to the elected Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division is authorized to audit all state officers, agencies, boards, and commissions and oversees audits and financial reporting for local governments.

Audit Team

William Garber, CGFM, MPA, Deputy Director

Neal Weatherspoon, CPA, CISA, CISSP, Audit Manager

Teresa Furnish, CISA, Principal Auditor

Ian Green, M.Econ, CGAP, CFE, Senior Auditor

This report, a public record, is intended to promote the best possible management of public resources. Copies may be obtained from:

website: sos.oregon.gov/audits

phone: 503-986-2255

mail: Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem, Oregon 97310

The courtesies and cooperation extended by officials and employees of the Office of the State Chief Information Officer and the reviewed agencies during the course of this audit were commendable and sincerely appreciated.