Secretary of State
Oregon Audits Division

Oregon State Police

Cybersecurity Controls Audit

May 2020
2020-17

Secretary of State Bev Clarno
Audits Division Director Kip Memmott

Secretary of State
Oregon Audits Division

Executive Summary

Oregon State Police

Cybersecurity Controls Audit

Why This Audit is Important

» The Oregon State Police (OSP) is charged with protecting people, wildlife, and natural resources in Oregon. OSP enforces traffic laws, investigates and solves crimes, conducts post-mortem examinations and forensic analysis, and provides background checks and law enforcement data.

» OSP is responsible for meeting federal Criminal Justice Information System (CJIS) security requirements and determining whether state and local agencies with access to CJIS data are also meeting those requirements.

» Cyberattacks are a growing concern for both the private and public sector. Recent breaches at Oregon state agencies have only escalated this concern. To protect against growing threats, information technology (IT) management professionals should apply robust cybersecurity controls at various levels of infrastructure to protect IT resources.

What We Found

Our review identified specific areas where OSP should improve cybersecurity controls. Specifically, OSP does not have a formal security management and compliance program and lacks basic IT controls for all six CIS controls we reviewed as part of this assessment. We identified the following areas where OSP should improve security controls:

1. OSP does not have a formal security management and compliance program that establishes a framework for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of those procedures. (pg. 5)
2. OSP does not actively manage hardware devices on its network to ensure only authorized devices connect to its network. (pg. 6)
3. OSP does not actively manage software to ensure that only authorized software is installed. (pg. 7)
4. Vulnerability assessments and remediation are performed on a limited, ad hoc basis. (pg. 8)
5. OSP does not appropriately manage all users who have significant high-level access to systems and data. (pg. 8)
6. OSP has not created secure configuration baselines for all servers, network devices, and workstations. (pg. 9)
7. OSP does not have the necessary tools to monitor audit logs for all workstations, servers, and network devices. (pg. 10)

Due to the sensitive nature of IT security and in accordance with Oregon state law and government auditing standards, we communicated details of the extent of the security weaknesses we identified to agency management in a confidential appendix.

What We Recommend

We made seven recommendations to OSP that include implementing a security management and compliance program and remedying weakness we identified in basic CIS Controls™. OSP agreed with all of our recommendations. Their response can be found at the end of the report.

The Oregon Secretary of State Audits Division is an independent, nonpartisan organization that conducts audits based on objective, reliable information to help state government operate more efficiently and effectively. The summary above should be considered in connection with a careful review of the full report.

Introduction

Cyberattacks, whether big or small, are a growing concern for both the private and public sector. Recent breaches at Oregon state agencies have only escalated this concern. In order to protect against growing threats, information technology (IT) management professionals should apply robust cybersecurity controls at various levels of infrastructure to protect their networks, servers, and user workstations. State agencies utilize a variety of frameworks and standards with varying levels of detail to guide these efforts.

The Audits Division conducts cybersecurity audits to evaluate IT security risks and provide a high-level view of an agency's current state. We chose to use the Center for Internet Security's CIS Controls™, version 7.1. The CIS Controls™ are a prioritized list of 20 high-priority defensive actions that provide a starting point for enterprises to improve cyber defense. The controls are divided into three categories: basic, foundational, and organizational. This review includes the first six, the basic controls, which the Center for Internet Security, along with other security practitioners, defined as key controls that every organization should implement for essential cyber defense readiness.

In the following pages, we present the results as graphs depicting how many sub-controls in each control are not implemented, partially implemented, or fully implemented. This provides agency management, the Legislature, and others with responsibility for cybersecurity in the state with a snapshot of high-risk areas. It also provides the Audits Division with valuable information that informs our audit planning process and helps us focus limited audit resources where the risks are highest.

This audit does not consider an agency's risk appetite. Therefore, while these controls are considered basic by many security practitioners, agency management may choose not to fully implement a control if they determine within their strategic priorities that the cost of doing so outweighs the risk. In addition, while we generally considered controls that might mitigate some of the risks we identified, we did not perform a detailed review of potential compensating controls for each sub-control.

State agencies and Enterprise Information Services share responsibility for cybersecurity in Oregon government

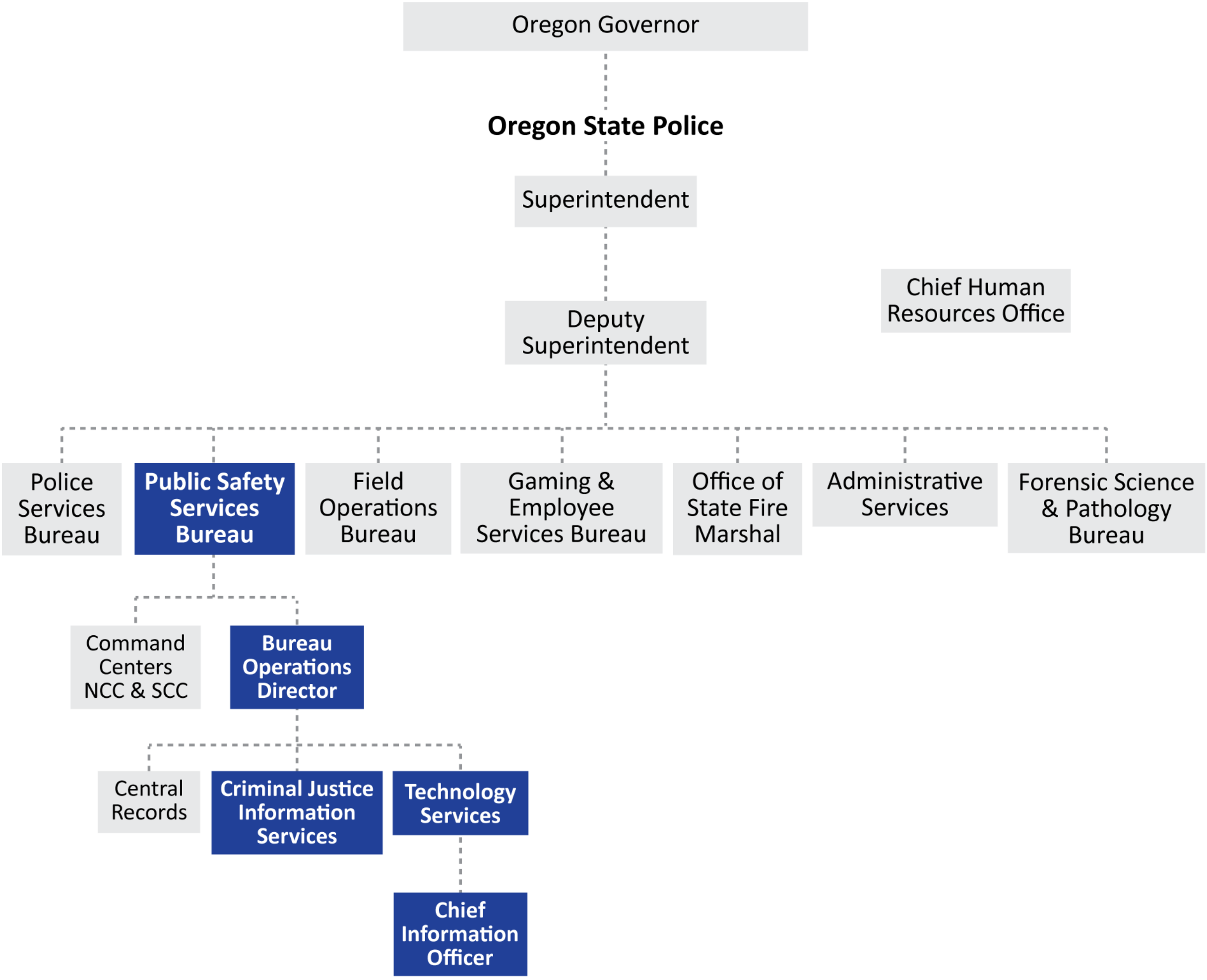
In September 2016, the Governor signed Executive Order 16-13, unifying IT security functions for the majority of state agencies in order to protect and secure information entrusted to the State of Oregon.[1] The order directed executive branch agencies to consolidate security functions and staffing into the Office of the State Chief Information Officer, now known as Enterprise Information Services (EIS). In addition, the order instructed agencies to work with the newly consolidated group to develop and implement security plans, rules, policies, and standards adopted by the State Chief Information Officer.

The passage of Senate Bill 90 in June 2017 made the order permanent, resulting in the transfer of 30 security-related positions from state agencies to EIS.[2] One position was transferred from OSP. After the shift in positions, major executive branch agencies were supposed to be assigned a Business Information Security Officer from EIS to lead the activities normally undertaken by an

[1] Executive Order 16-13, "Unifying Cyber Security in Oregon"
[2] Senate Bill 90, "Transfers information technology security functions of certain state agencies in executive branch to State Chief Information Officer."

agency's Chief Information Security Officer. However, at the time of this audit, OSP reported that EIS had not formally assigned anyone to assist OSP.

EIS maintains policy and statewide IT oversight functions. The Enterprise Security Office, known now as Cyber Security Services (CSS), a division of the EIS, brings together elements of enterprise security — including governance, policy, procedure, and operations — under a single accountable organization. Agencies retain responsibility for many organization-level security controls and work collaboratively with the CSS to ensure the confidentiality, availability, and integrity of their sensitive business information. At the time of this audit, CSS had not fully defined the division of security responsibilities and functions between its office and the agencies.


Oregon Governor
Oregon State Police
Superintendent
Chief Human Resources Office
Deputy Superintendent
Police Services Bureau
Public Safety Services Bureau
Field Operations Bureau
Gaming & Employee Services Bureau
Office of State Fire Marshal
Administrative Services
Forensic Science & Pathology Bureau
Command Centers NCC & SCC
Bureau Operations Director
Central Records
Criminal Justice Information Services
Technology Services
Chief Information Officer

The Oregon State Police organization structure is complex with multiple bureaus and offices

The Oregon State Police (OSP) is charged with protecting people, wildlife, and natural resources in Oregon. OSP is responsible for enforcing the traffic laws on the state's roadways, investigating and solving crimes, conducting post-mortem examinations and forensic analysis, and providing background checks and law enforcement data. OSP also regulates gaming, the handling of hazardous materials and fire codes, educates the public on fire safety, and enforces fish, wildlife, and natural resource laws.

Founded in 1931, the organization's mission is to serve the State of Oregon with a diverse workforce dedicated to the protection of people, property, and natural resources. OSP is the only provider of certain specialized public safety and criminal justice system services in Oregon, including forensic lab services, the State Medical Examiner, criminal justice information systems, and the State Fire Marshal.

OSP has multiple bureaus and offices, including:

- The Superintendent's Office;
- Police Services Bureau;
- Patrol Field Operations Bureau;
- Public Safety Services Bureau;
- Forensic Science & Pathology Bureau;
- Gaming and Employee Services Bureau;
- Office of the State Fire Marshal; and
- Administration Services.

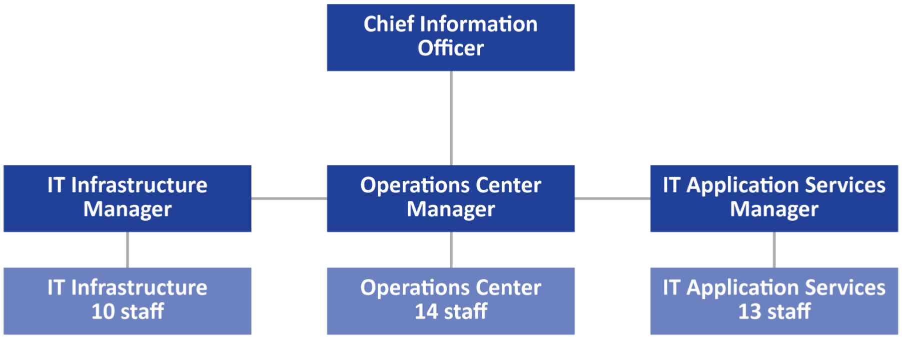
OSP IT Division is located within Public Safety Services

The Technology Division responsible for IT is within the Public Safety Services Bureau and is located within the Bureau Operations. The IT Division has a $10 million operating budget and a staff of 40 who support over 1,300 employees within OSP.

OSP's Chief Information Officer (CIO), who is in charge of the IT Division, reports to the Public Safety Services director, but serves all eight bureaus and offices. Since 2014, OSP has had three CIOs and three interim or temporary CIOs.

The IT Division consists of three teams:

- **The Service Desk** provides primary IT support services for OSP.
- **The Applications Team** provides application support and development.
- **The Infrastructure Team** provides and supports the underlying infrastructure including the network, servers, facilities, and system management.


Chief Information Officer
IT Infrastructure Manager
Operations Center Manager
IT Application Services Manager
IT Infrastructure 10 staff
Operations Center 14 staff
IT Application Services 13 staff

OSP is subject to Criminal Justice Information Services security standards

OSP is responsible for meeting certain federal security requirements to access data held by the Criminal Justice Information Services (CJIS) Division of the FBI. CJIS data contains highly sensitive criminal justice information, including fingerprints and criminal background information. For this reason, CJIS has robust policies and rules that law enforcement agencies and others must follow before they are permitted access to this data.

These policies cover best practices in wireless networking, remote access, data encryption, and multiple authentication. For example, a basic rule covers restricted access based on physical location, job assignment, and time of day.

In addition to being responsible for its own CJIS compliance, OSP is responsible for determining whether state and local agencies with access to CJIS data are also compliant. State systems with CJIS data include:

- Criminal Justice Information System: Oregon's central computerized repository of criminal offender records and related law enforcement information.
- Law Enforcement Data System (LEDS): LEDS connects law enforcement, criminal justice agencies, and other authorized users to centrally maintained files including data relating to wanted and missing persons, sex offenders, drug manufacturers, stolen vehicles, concealed handgun licenses, criminal records, restraining orders, and offenders under parole or probation supervision.
- Identification Services Section (ISS): ISS is comprised of the Criminal History, Regulatory Compliance, Automated Fingerprint Identification System, and Firearms programs.

Access to these state systems is not limited to Oregon. Information gathered by Oregon law enforcement agencies may be shared with and used by jurisdictions nationwide in conducting background checks for a range of activities from checking for active warrants to selling firearms. These systems serve over 700 local, state, and federal criminal justice agencies and over 45,000 law enforcement and criminal justice agents nationwide. Additionally, they serve over 130 non-criminal justice agencies, and 1,200 federally licensed firearm dealers.

Audit Results

Our review identified areas where OSP should improve cybersecurity controls. Specifically, OSP does not have a security management program that establishes a framework for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of those procedures.

Additionally, while some sub-controls are partially implemented, OSP lacks basic foundational IT controls for all six CIS controls we reviewed as part of this assessment. This is largely due to a lack of prioritization for implementing these controls, as well as a perception by management that such controls are unnecessary. This is made more significant because OSP is required to follow CJIS IT security standards, and is responsible for making sure state and local agencies with access to CJIS data are following them as well.

We considered the risks posed by publicly releasing any information related to security findings. We balanced the need for stakeholders, such as the Legislature, to be informed on critical or systemic IT security issues affecting the State against the need to protect the agency from additional threats. Consequently, in accordance to ORS 192.345 (23) and generally accepted government auditing standards, we removed some details of the security weaknesses from the report and provided agency management and EIS a confidential appendix with additional detail and context.

OSP lacks a formal security management and compliance program

Security management programs of all executive branch agencies should be collaborative efforts with Cyber Security Services (CSS), located within Enterprise Information Services (EIS). Under this governance structure, CSS is responsible for enterprise information security strategy and planning, while each individual agency is responsible for the development, documentation, and implementation of a security management and compliance program for its specific environment, including workstations and applications.

Effective security management requires agencies to have policies, plans, and procedures that describe the management program and cover all major systems, facilities, and applications. Detailed roles and responsibilities should be clearly defined. Specifically, agencies should:

- periodically assess and validate risks;
- document and implement security control policies and procedures;
- implement and monitor effective security awareness trainings;
- remediate information security weaknesses; and
- ensure external third party activities are adequately secured.

We determined OSP does not have a formal security management and compliance program and lacks robust policies and procedures for most security-related controls we reviewed. Additionally, we found OSP does not have processes in place to periodically assess and validate risks and lacks controls to ensure access granted to external third party activities are adequately secured. This is partially due to inconsistent leadership in the CIO position. Since 2014, OSP has had three CIOs and three interim or temporary CIOs.

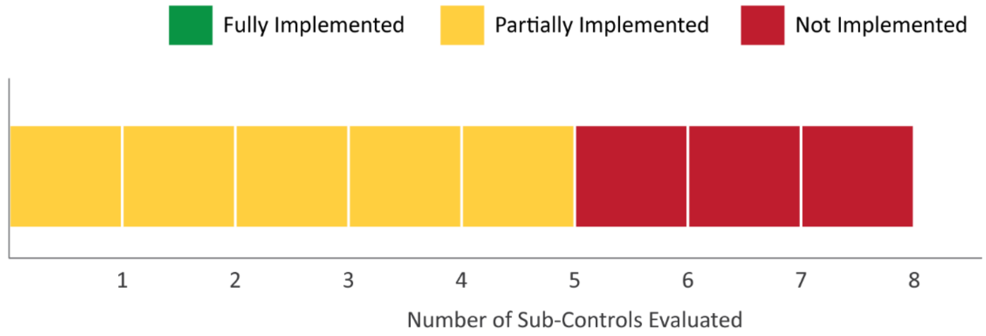
While IT security has been largely consolidated within the CSS, some aspects of IT security — such as application security, network vulnerability scanning and monitoring, and patching of servers not hosted at the State Data Center — remain with the agency. The passage of Senate Bill 90 transferred OSP's only dedicated security person to the CSS. To compensate for the loss of security staffing, the CSS intended to assign executive branch agencies a Business Information Security Officer to provide guidance, planning, and security leadership. However, at the time of this audit, the CSS has not assigned anyone to OSP despite multiple requests for assistance from OSP IT management. Without sufficient staff assigned to security tasks, some critical activities are performed on an ad hoc basis and OSP's ability to identify and respond to security incidents is hindered.

Without a well-designed program with appropriate staffing and resources, security controls are likely inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls are at risk of being inconsistently applied, leaving the agency vulnerable to attacks.

CIS Controls Review

For this audit, we evaluated the implementation level of the agency's cybersecurity control environment against the top six CIS Controls™ and their associated sub-controls. We evaluated each sub-control to provide an assessment of the agency's overall cybersecurity implementation. The charts below illustrate the number of controls evaluated for each control objective, and whether that control is fully implemented, partially implemented, or not implemented.

CIS Control 1™: Inventory of Authorized and Unauthorized Devices



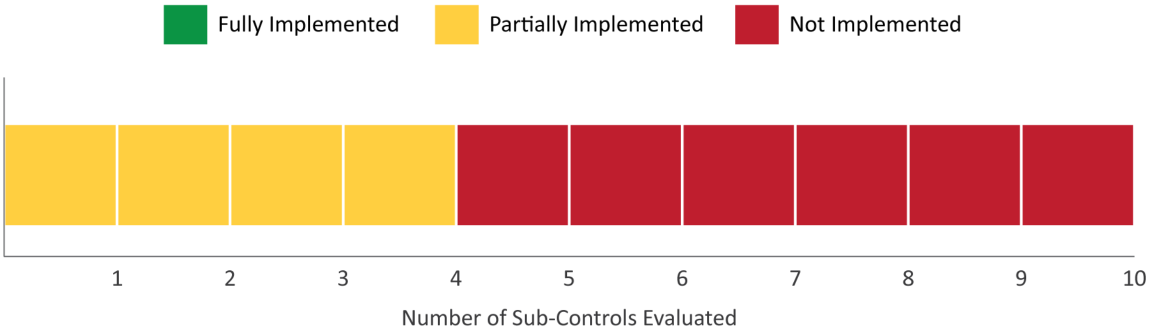
We evaluated OSP's processes to identify network devices, maintain an updated inventory of hardware devices, and ensure only approved devices can connect to the network. We found the agency does not have documented policies and procedures that provide guidance and requirements for safeguarding its network. In addition, OSP cannot accurately identify basic information about its device inventory or rely on the hardware inventory to ensure only authorized devices connect to the network.

OSP relies on an inventory tool that does not integrate with the majority of its IT assets. Because of this, the agency implemented a manual process to track assets that were incompatible with the tool. However, the agency updates the inventory only once a year and does not reconcile the results to devices discovered on its network. The agency is in the process of replacing the tool but the inventory remains incomplete, out-of-date, and inaccurate until the agency fully implements the replacement.

Any new device introduced to an agency's network may introduce vulnerabilities. Ensuring only authorized devices have access to information on the agency's network allows IT professionals to identify and remediate vulnerabilities by implementing proper security controls. However, without a clear understanding of which devices are on the network, the agency cannot ensure proper controls are in place for those devices.

Additionally, without an accurate, up-to-date inventory of authorized hardware, the agency cannot actively manage and monitor all hardware devices on the network so that only authorized devices are given access and unauthorized and unmanaged devices are found and prevented from gaining access.

CIS Control™ 2: Inventory of Authorized and Unauthorized Software

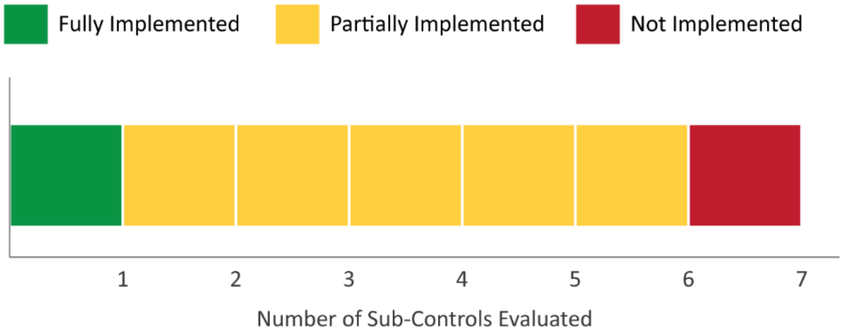


We evaluated OSP's process to document approved software, segregate high-risk software, and identify software installed on its systems. We determined OSP has tools in place to identify and track software installed on devices connected to its network. However, much work remains to ensure only authorized and supported software is installed on agency systems. Among other weaknesses, we noted that OSP lacked policies and procedures, had an incomplete list of approved software, and had not implemented whitelisting to ensure only authorized software can be installed on agency systems.

Controls should be established by implementing software whitelisting, automating software inventory, and monitoring software installations on all systems. Organizations should maintain an inventory of software installed on their computer systems similar to the inventory of its hardware assets. If an agency does not have a complete, accurate, and up-to-date list of the software authorized to be on its systems, it cannot ensure effective controls are in place to update installed software. Attackers continuously scan targeted organizations looking for vulnerable versions of software to exploit. Software that is no longer supported by its vendor is especially vulnerable to this type of attack, as patches are no longer developed to remediate vulnerabilities.

In addition, without an inventory of system software, an agency may be unable to identify unauthorized software on its information systems, such as malicious software or software with known vulnerabilities. Attackers can exploit systems with malicious or vulnerable software to gain unauthorized access to the agency's data or disrupt operations. Workstations are also more likely to be either running software that is unneeded for business purposes, which could introduce potential security flaws, or running malware introduced by an attacker after a system is compromised.

CIS Control™ 3: Continuous Vulnerability Assessment and Remediation



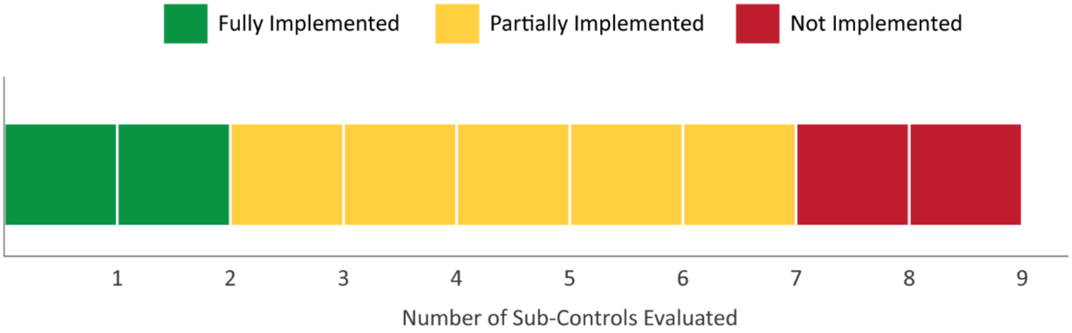
We found that OSP's processes for patching systems to prevent vulnerabilities and for remediating detected vulnerabilities are not adequate to keep systems up-to-date with current software patches and to identify and remediate vulnerabilities.

OSP works with the CSS to perform monthly vulnerability scans. However, OSP lacks defined, repeatable processes and procedures and instead relies on ad hoc processes to remediate the identified vulnerabilities. The vulnerability scans performed by OSP during our audit show an unacceptably high number of critical vulnerabilities across the majority of its network devices. Furthermore, OSP management let licenses lapse, and was using outdated and unsupported tools, to monitor and patch its operating systems and software, which resulted in endpoints not receiving the latest updates for a significant period. In addition, OSP had not maintained critical servers used to support the agency's primary mission.

Organizations should be continuously engaged in identifying, remediating, and minimizing security vulnerabilities to ensure their assets are safeguarded. Attackers commonly exploit IT systems that have not been patched with security updates or have other known vulnerabilities. This could compromise the confidentiality, integrity, or availability of agency data. By scanning the network for known vulnerabilities, an agency can identify and prioritize software patching and other remediation activities to ensure these known risks are controlled.

Agency management should ensure processes are in place to be informed of available patches, test those patches for compatibility on the agency's systems, document the basis for the decision to implement patches or not, and implement appropriate changes in a timely manner.

CIS Control™ 4: Controlled Use of Administrative Privileges



We assessed OSP's processes to grant privileged access accounts, log and monitor login activity, and to establish robust authentication procedures.[3]

We found the agency generally lacked processes and procedures for granting, reviewing, and terminating access for privileged accounts. In addition, the agency lacked access request forms that detail the access provisioned in order to provide an audit trail or support for the business need for the type of access granted and ensure the application and enforcement of the principle of least privilege.[4]

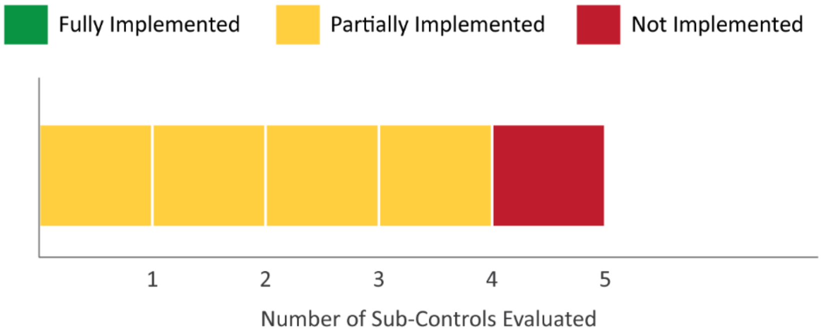
While OSP does not have tools to automatically inventory its administrative accounts, the agency is using centrally automated rules to control users with privileged accounts in multiple environments. However, OSP was unable to provide a complete list of accounts for all the environments and security groups for review. Among other weaknesses, we noted out-of-date

[3] Privileged access refers to the ability of some users to take actions that may affect computing systems, network communications, or the accounts, files, data, or processes of other users. Privileged access implies greater access than the average end user has.
[4] Least privilege is a principal that states that users should have the least amount of privileges (access to services) necessary to perform their duties.

group policy settings, insufficient password setting requirements, and unused accounts that were likely no longer needed.

Management of privileged users should ensure only authorized users are able to perform administrative functions on the agency's information systems. While some users may have authorization to read, edit, or delete data based on their job duties, other users have access to advanced functions such as system control, monitoring, or administrative functions. Actions performed under these administrative accounts may have critical effects on the agency's systems. Therefore, use of accounts with these privileges should be effectively controlled by management, including implementing controls to segregate, manage, and monitor use of these accounts.

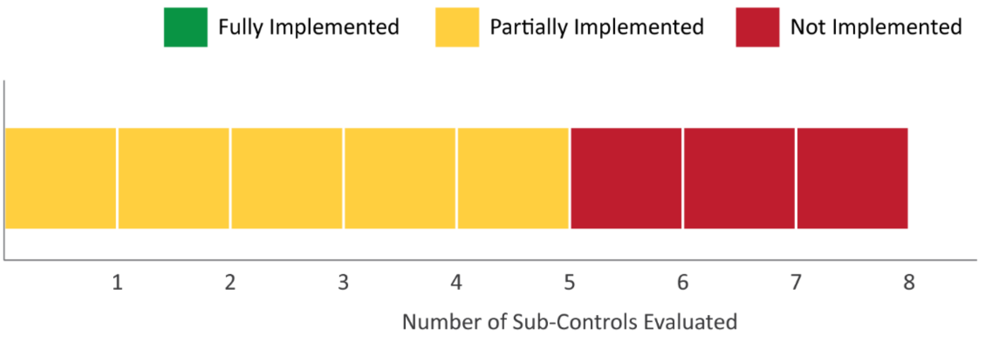
CIS Control™ 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers



We evaluated OSP's processes to document and safeguard baseline configurations, deploy secure configurations, and monitor configurations on its network. We determined OSP has not established secure baselines for most servers, network devices, and workstations. While OSP has documentation showing what some specific workstation and server builds should be, we found OSP relies on staff to establish configuration baselines using individual judgment instead of applying formal guidance or standards. Additionally, although centrally automated rules control most workstation configurations, we found these rules were largely unmanaged, resulting in rules that were sometimes inconsistent, directed at devices that no longer exist, and largely un-auditable.

Organizations should have processes in place to ensure hardware and software are securely configured. This should include verifying that default configurations align with business and security needs so that agency systems are not left vulnerable to attack. The agency should also have configuration management processes in place that address implementing secure system control features at the initiation of the system life cycle. Furthermore, an organization should ensure configurations remain secure as modifications are made to the system. Baselines should be documented so agency personnel can effectively monitor actual configurations to ensure they align with established baselines. Also, policies and procedures should be in place that address how configuration baselines are managed.

CIS Control™ 6: Maintenance, Monitoring, and Analysis of Audit Logs



We reviewed OSP's processes for collecting, managing, and analyzing audit logs of events that could help the agency detect, understand, or recover from an attack. We found synchronized logging enabled for workstations, servers, and most network devices. However, we found most logs are not reviewed on a regular proactive basis.

In addition, we found OSP has not centralized logging or deployed tools that can provide real-time analysis and correlation of event logs for all domains. This is due in part to the lack of clarity at CSS with the roles and responsibility over IT security. CSS has communicated its intent to provide statewide centralized logging and event management at some point in the future; however, at the time of this audit, those plans have not been finalized.

Robust logging and log monitoring processes allow organizations to identify and understand inappropriate activity and recover more quickly from an attack. Deficient logging may allow attackers and malicious activity to go undetected for extended periods. Moreover, attackers know that many organizations rarely review log information, allowing attacks to go unnoticed. Agencies should ensure that information systems record the type, location, time, and source of events that occur. Additionally, processes should be established to ensure these logs are periodically reviewed so the agency can identify inappropriate or unusual activity and remediate security events.

Recommendations

To improve critical cybersecurity controls, we recommend OSP, in cooperation with CSS:

1. Implement a security management and compliance program that includes an established framework and continuous cycle of activity for assessing risk, developing and implementing effective security controls and procedures, and monitoring the effectiveness of those procedures.
2. Remedy weaknesses with CIS Control #1 – Hardware Inventory – by developing written policies and procedures, fully automating asset discovery and inventory, and fully implementing hardware authentication controls.
3. Remedy weaknesses with CIS Control #2 – Software Inventory – by developing written policies and procedures, updating documentation of approved software and software versions, and implementing software whitelisting.
4. Remedy weaknesses with CIS Control #3 – Vulnerability Assessment – by refining and implementing written policies and procedures, and formally tracking the status of identified vulnerabilities to ensure timely remediation.
5. Remedy weaknesses with CIS Control #4 – Privileged Access – by developing written policies and procedures for granting, reviewing, and removing access for privileged accounts, removing end users' administrative access to workstations, maintaining an inventory of administrative accounts, ensuring the use of dedicated administrative accounts, and implementing multifactor authentication for all administrative access.
6. Remedy weaknesses with CIS Control #5 – Secure Configurations – by establishing secure configurations for all workstations, servers, and network devices and by establishing appropriate monitoring and alerts to ensure all changes to configurations are authorized and appropriate.
7. Remedy weaknesses with CIS Control #6 – Audit Logs – by developing a central logging solution, implementing log analytic tools, and automating log review for all domains.

Objective, Scope, and Methodology

Objective

Our audit objective was to determine the extent to which OSP has implemented an appropriate IT security management program, as well as selected controls from the Center for Internet Security's CIS Controls™, version 7.1.[5] These controls are a prioritized set of actions that collectively form a defense-in-depth structure to help protect systems and networks from the most common attacks.[6]

Scope

The scope of this work included a review of security management and the first six of the 20 CIS Controls™ in place at OSP during the third and fourth quarters of 2019. Cybersecurity experts generally agree that these six "basic" controls should be implemented by all organizations for cyber defense readiness.

The following internal control principles were relevant to our audit objective:

- Security Management
  - Establish a security management program;
  - Periodically assess and validate risks;
  - Document and implement security control policies and procedures;
  - Implement effective security awareness and other security-related personnel policies;
  - Monitor the effectiveness of the security program;
  - Effectively remediate information security weaknesses; and
  - Ensure that activities performed by external third parties are adequately secure.
- Inventory and Control of Hardware Assets
  - Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
- Inventory and Control of Software Assets
  - Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.
- Continuous Vulnerability Management
  - Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
- Controlled Use of Administrative Privileges
  - The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
  - Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a

[5] Center for Internet Security CIS Controls

[6] Defense-in-depth refers to the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives.

rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

- Maintenance, Monitoring and Analysis of Audit Logs
    - Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Deficiencies with these internal controls were documented in the audit results section of this report. Other elements of internal control were not deemed necessary to achieve the objective of the audit and were excluded from scope.

Methodology

To assess whether management has established policies and implemented controls to stop cyberattacks that may target the agency, we:

Reviewed:

- IT Policies and procedures;
- External IT risk assessments and audits;
- Hardware asset inventory lists;
- Software asset inventory lists;
- Privileged user access lists;
- Network diagrams.

Observed:

- Configuration settings;
- Vulnerability scan results;
- Software installed on workstations;
- IT processes and ad hoc activities.

Interviewed:

- IT staff;
- IT managers;
- Agency CIO;
- Bureau leadership.

Limitations:

- Controlled Use of Administrative Privileges - Auditors were unable to test privileged accounts for all seven of OSP's domains because the agency was unable to provide a list of privileged accounts for three of the domains.

We considered the risks posed by publicly releasing any information related to security findings. We balanced the need for stakeholders, such as the Legislature, to be informed on critical or systemic IT security issues affecting the State against the need to protect the agency from additional threats. Consequently, in accordance to ORS 192.345 (23) and generally accepted government auditing standards, we removed some details of the security weaknesses from the report and provided agency management and EIS a confidential appendix with additional detail and context.

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 provides a reasonable basis to achieve our audit objective.

We sincerely appreciate the courtesies and cooperation extended by officials and employees of OSP and EIS during the course of this audit.

Oregon

Kate Brown, Governor

Oregon State Police
General Headquarters
3565 Trelstad Ave Se
Salem, OR 97317
503-378-3720
503-378-8282
TTY 503-585-1452

April 15, 2020

Kip Memmott, Director
Secretary of State, Audits Division
255 Capitol St. NE, Suite 500
Salem, OR 97310

Dear Mr. Memmott,

This letter provides a written response to the Audits Division's final draft audit report titled Oregon State Police Cybersecurity Controls Audit.

The Oregon State Police (OSP) Executive Management would like to thank the Secretary of State's Audits Division for all their effort, professionalism, and expertise they provided during this Cybersecurity Audit. OSP is devoted to not only fixing the issues identified but expanding to long term planning and action going forward. This audit will serve as a baseline for future audits to track the future of OSP's security management and compliance program.

To assist with completing these recommendations, OSP will seek in the 21-23 legislative session to establish two permanent Information Technology risk abatement personnel. Completing these recommendations isn't contingent on hiring these personnel but that would assist greatly in long term security and risk abatement for OSP.

Below is OSP's detailed response for each recommendation in the audit.

RECOMMENDATION 1
Implement a security management and compliance program that includes an established framework and continuous cycle of activity for assessing risk, developing and implementing effective security controls and procedures, and monitoring the effectiveness of those procedures.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Aug 2022	Mark S. Hansen, 503-507-7714

Narrative for Recommendation 1

OSP will continue to work with Cyber Security Services (CSS) on a regular basis. OSP continues to seek guidance and clarity on the roles and responsibilities of OSP and CSS and how that relates to protecting OSP technology assets and to establish an Information security program.

OSP is hiring for a Chief Information Officer (CIO), whose first duty will be managing and coordinating OSP's security program, policies and initiatives. The CIO will put OSP on a path to greater security awareness, appropriate the correct positions needed, and direct OSP down a path of a higher security posture. This position has been vacant for a year and six unsuccessful recruitment cycles have occurred.

To assist with completing these recommendations, OSP has taken the initial steps to request the establishment of two permanent IT risk abatement personnel in the 21-23 legislative session. Completing these recommendations isn't contingent on hiring these personnel but it will assist in long term security and risk abatement for OSP. These personnel would be doing the following:

- Establish and maintain a permanent security management and compliance program for OSP.
- Collaborate security and risk assessment efforts with CSS.
- Periodically assess and validate risks.
- Document and implement security control policies and procedures.
- Implement and monitor effective security awareness trainings.
- Remediate information security weaknesses.
- Ensure external third-party activities are adequately secured.

OSP has engaged with CSS to complete a Security Assessment and for a continued Security Evolution.

RECOMMENDATION 2
Remedy weaknesses with CIS Control #1 – Hardware Inventory – by developing written policies and procedures, fully automating asset discovery and inventory, and fully implementing hardware authentication controls.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Aug 2021	Mark S. Hansen, 503-507-7714

Narrative for Recommendation 2
OSP has recently migrated to a new Hardware inventory software that will greatly assist with automating asset discovery and inventory. Policies and procedures are being crafted to provide guidance and for safeguarding OSP's network. Full integration of this software, policies, and verification is expected by early 2021.

OSP will seek in the 21-23 legislative session to establish two permanent risk abatement personnel. These personnel will verify OSP's hardware inventory and continue to monitor for further improvement of OSP's security and risk posture.

A port security program is being planned for implementation in the future. This will prevent unauthorized hardware from introducing vulnerabilities. OSP's risk abatement personnel will continue monitoring and verification of this program.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 3</b>
Remedy weaknesses with CIS Control #2 – Software Inventory – by developing written policies and procedures, updating documentation of approved software and software versions, and implementing software whitelisting.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>Aug 2021</td><td>Mark S. Hansen,
503-507-7714</td></tr>
</table>

Narrative for Recommendation 3
OSP has migrated to a new Software inventory tool that will assist with automating software discovery and inventory. Policies and procedures are being crafted to provide guidance and for safeguarding OSP's network. Full integration of this software, policies, and verification is expected by early 2022.

OSP will seek in the 21-23 legislative session to establish two permanent risk abatement personnel. These personnel will work at establishing controls to implement software whitelisting, automate software inventory, and monitoring software installation on all systems.

All new software is following the guidelines set from DAS (Department of Administrative Services), for software review through EIS (Enterprise Information Services), and through the procurement EULA (End User License Agreement) review guidelines.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 4</b>
Remedy weaknesses with CIS Control #3 – Vulnerability Assessment – by refining and implementing written policies and procedures, and formally tracking the status of identified vulnerabilities to ensure timely remediation.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>Dec 2020</td><td>Mark S. Hansen,
503-507-7714</td></tr>
</table>

Narrative for Recommendation 4
Formal policies and procedures around vulnerability assessment, will be identified, created, and followed to minimize OSP's vulnerabilities. OSP will continue to utilize currently provided CSS tools to proactively scan for vulnerabilities and address them as possible given personnel, funding and time limitations. These tools will be added to the policies and procedures for vulnerability assessment in OSP.

OSP will seek in the 21-23 legislative session to establish two permanent risk abatement personnel. These personnel will work at continuously engaging in identifying, remediation, and minimizing security vulnerabilities at OSP. OSP currently has repurposed other IT staff to fulfill these duties. If the additional staff are not approved, work on this recommendation will continue, although at a slower pace.

RECOMMENDATION 5
Remedy weaknesses with CIS Control #4 – Privileged Access – by developing written policies and procedures for granting, reviewing, and removing access for privileged accounts, removing end users' administrative access to workstations, maintaining an inventory of administrative accounts, ensuring the use of dedicated administrative accounts, and implementing multifactor authentication for all administrative access.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 2022	Mark S. Hansen, 503-507-7714

Narrative for Recommendation 5
OSP will establish formalized policies and procedures for granting, logging, and monitoring privileged access accounts. OSP will establish Privileged Access Management (PAM) to automatically monitor and inventory privileged access accounts. OSP will seek in the 21-23 legislative session to establish two permanent risk abatement personnel. These personnel will work at continuously engaging in identifying, remediation, and minimizing security vulnerabilities at OSP. If the additional staff are not approved, work on this recommendation will continue, although at a slower pace.

RECOMMENDATION 6
Remedy weaknesses with CIS Control #5 – Secure Configurations – by establishing secure configurations for all workstations, servers, and network devices and by establishing appropriate monitoring and alerts to ensure all changes to configurations are authorized and appropriate.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation

Agree	Aug 2021	Mark S. Hansen, 503-507-7714

Narrative for Recommendation 6
OSP will establish policies and procedures for configuring servers and workstations. OSP will seek in the 21-23 legislative session to establish two permanent risk abatement personnel. These personnel will verify that no changes have been made to these configurations. If the additional staff are not approved, work on this recommendation will continue, although at a slower pace.

OSP has repurposed current IT staff to configure and establish secure configurations for all workstations and servers. Other efforts will be established for appropriate monitoring and alerts on configurations.

RECOMMENDATION 7
Remedy weaknesses with CIS Control #6 – Audit Logs – by developing a central logging solution, implementing log analytic tools, and automating log review for all domains.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Oct 2020	Mark S. Hansen, 503-507-7714

Narrative for Recommendation 7
OSP will establish a centralized logging solution that will collect, manage, analyze, and report on events that could help the agency detect, understand, or recover from an attack. OSP is in process to purchase a product that will satisfy these requirements, as well as professional services to expedite the process. OSP will seek in the 21-23 legislative session to establish two permanent risk abatement personnel. These personnel will take over this system to monitor and respond to logs and reports.

Please contact Mark S. Hansen, OSP Infrastructure Services Manager at 503-507-7714 with any questions.

Sincerely,

Travis Hampton
Oregon State Police Superintendent

Audit Team

William Garber, CGFM, MPA, Deputy Director

Teresa Furnish, CISA, Audit Manager

Matthew Owens, MBA, CISA, Principal Auditor

Sherry Kurk, CISA, Staff Auditor

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of the office, Auditor of Public Accounts. The Audits Division performs 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 has constitutional authority to audit all state officers, agencies, boards and commissions as well as administer municipal audit law.

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

Oregon Audits Division
255 Capitol St NE, Suite 500 | Salem | OR | 97310

(503) 986-2255
sos.oregon.gov/audits