



Secretary of State Oregon Audits Division



Department of Administrative Services **Cybersecurity Controls Assessment**

July 2019
2019-28

This page intentionally left blank

Executive Summary

Department of Administrative Services Cybersecurity Controls Assessment

July 2019

Report Summary

DAS is the state's central administrative agency. It supports state agencies by providing management frameworks and infrastructure for information systems and services, procurement, and other functions. Responsibility for cybersecurity is split between DAS, the Office of the State CIO, and the Enterprise Security Office. This audit assessed critical security controls and the information technology (IT) security management practices at the Department of Administrative Services (DAS). We concluded the agency does not have a security management program that identifies necessary actions to ensure systems are appropriately secure, and lacks basic foundational IT controls for all six cybersecurity controls we reviewed. As a result, DAS systems and data may be at risk for unauthorized use, disclosure, or modification.

What We Found

- » DAS lacks a formal security management program. ([pg. 5](#))
- » DAS does not have a consistent IT governance structure, which results in fragmented IT support to business units. ([pg. 5](#))
- » The DAS CIO role lacks appropriate functional authority and staffing to carry out its official responsibilities. ([pg. 6](#))
- » DAS does not actively manage hardware devices on their network to prevent and detect connection of unauthorized devices. ([pg. 8](#))
- » DAS does not actively manage software so that only authorized software is installed. ([pg. 9](#))
- » Vulnerability assessments and remediation are performed on a limited, ad hoc basis. ([pg. 10](#))
- » DAS does not appropriately manage all users who have significant high-level access to systems and data. ([pg. 11](#))
- » DAS has not created secure configurations for all servers, network devices, and workstations. ([pg. 12](#))
- » DAS does not adequately generate and monitor audit logs for all workstations, servers, and network devices. ([pg. 13](#))

Recommendations

We made seven recommendations to DAS that include implementing a security management program and remedying weakness we identified in basic CIS Controls™. DAS agreed with all seven of our recommendations. The agency's 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 assessments 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. 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 assessment covers the first six, the basic controls, which are defined as key controls that should be implemented in every organization for essential cyber defense readiness.

In the following pages, we present the results as graphs depicting whether a particular control is not implemented, partially implemented, or fully implemented. This provides agency management, the Legislature, and those with responsibility for cybersecurity in the state with a snapshot of areas with higher risk that may need additional controls applied. It also provides the Audits Division with valuable information about an entity that informs our audit planning process and helps us focus limited audit resources where the risks are highest.

The assessment does not consider an individual 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 the cost of doing so outweighs the risk. In addition, while we generally considered compensating controls that might mitigate some of the risks we identified, we did not perform a detailed assessment of potential compensating controls for each sub-control.

State agencies and the Office of the State Chief Information Officer 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 (OSCIO), which receives administrative support from the Department of Administrative Services (DAS). 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 (CIO). 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 the OSCIO.² The DAS IT division lost one IT staff as part of this transfer.

The OSCIO maintains policy and statewide IT oversight functions. The Enterprise Security Office (ESO), a division of the OSCIO, 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

¹ [Executive Order 16-13](#), "Unifying Cyber Security in Oregon"

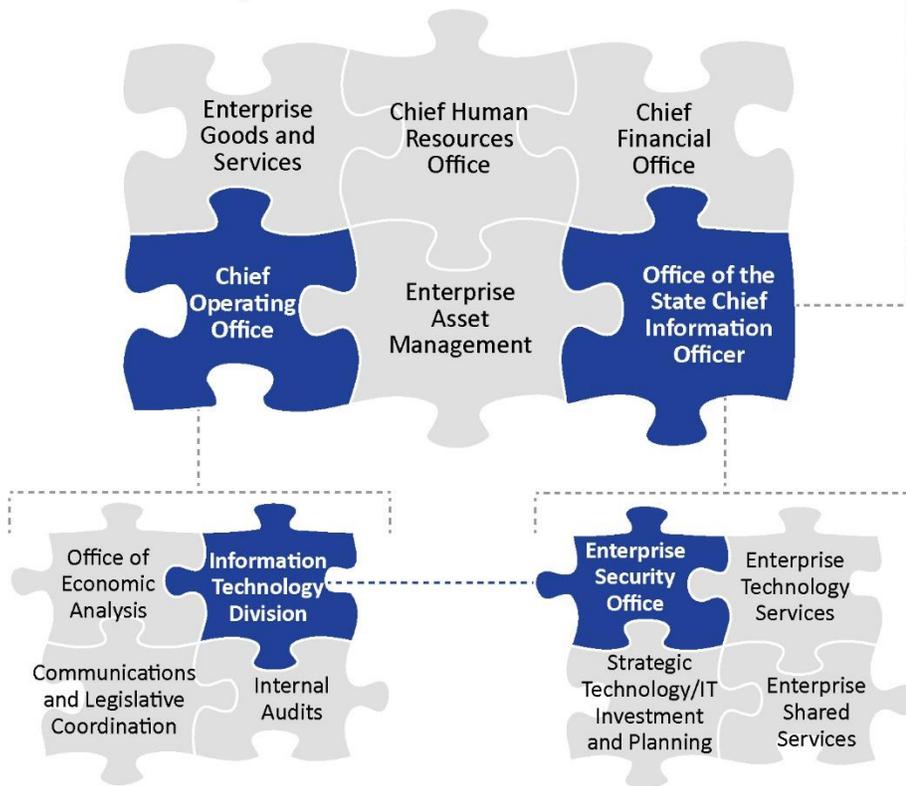
² [Senate Bill 90](#), "Transfers information technology security functions of certain state agencies in executive branch to State Chief Information Officer."

collaboratively with the ESO to ensure the confidentiality, availability, and integrity of their sensitive business information. At the time of this audit, the ESO had not fully defined the division of security responsibilities and functions between their office and the agencies. While DAS provides administrative support to the OSCIO and its divisions, the OSCIO offers the same level of IT governance and security services to DAS as it does to any other executive branch agency.

The Governor's Office

While the office is located within DAS, the State CIO is an independent official who answers directly to the Governor.

Department of Administrative Services



The Department of Administrative Services organization structure is complex with multiple divisions and business units

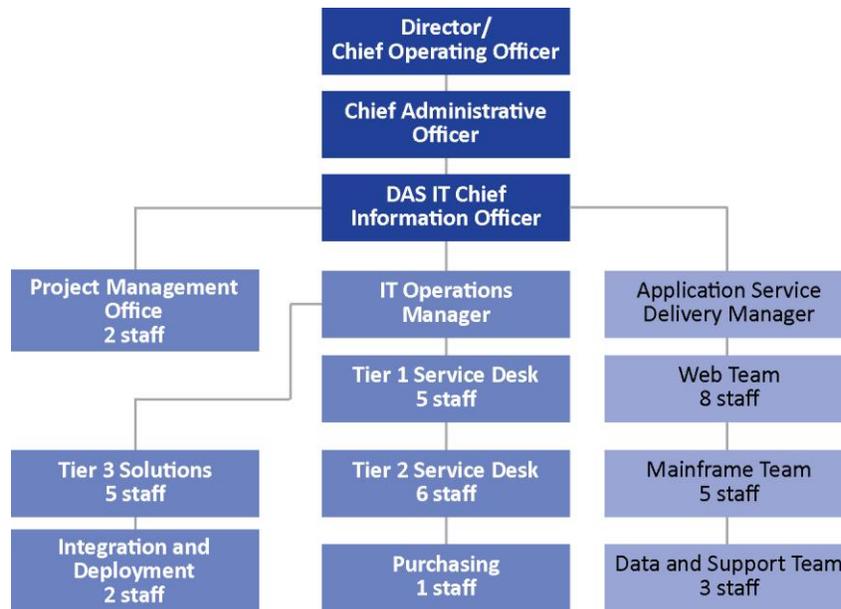
DAS is the state's central administrative agency. DAS supports state agencies in the executive department by providing management frameworks and infrastructure for information systems and services, procurement, and other functions. DAS has multiple subdivisions, including:

- Office of the Chief Operating Officer;
- Chief Financial Office;
- Chief Human Resources Office;
- Office of the State Chief Information Officer;
- Enterprise Asset Management; and
- Enterprise Goods and Services.

In addition to serving as the state’s Chief Operating Officer, the DAS director is responsible for managing and coordinating the policies, programs, and services of DAS divisions. The DAS Information Technology Division, situated within the Chief Operating Office, supports DAS IT systems, including workstations, laptops, state-owned mobile devices, operating systems, internal and enterprise applications, and associated hardware. In addition, DAS IT staff supports the IT needs of a variety of external agencies, boards, and commissions that do not have their own IT staff.

The DAS IT program consists of three units: the Help Desk, the Application Development Team, and the Project Management Office. The DAS CIO, a separate position from the State CIO, leads the DAS IT program. While maintaining an internal focus on DAS and client agency needs, DAS IT works closely with its enterprise partners in the OSCIO.

Figure 1: DAS IT Division



Objective, Scope, and Methodology

Objective

The objective of this work was to determine the extent to which DAS has implemented an appropriate IT security management program, as well as selected controls from the Center for Internet Security's CIS Controls™, version 7.³ 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.⁴

Scope

The scope of this work included a review of security management and the first six of the 20 CIS Controls™ in place at DAS during the first quarter of 2019. Cybersecurity experts generally agree that these six “basic” controls should be implemented by all organizations for cyber defense readiness. Except when necessary to review collaborative security processes with the Enterprise Security Office, we excluded from our scope the divisions of the Office of the State CIO, including Enterprise Technology Services, which manages the State Data Center.

Methodology

To assess whether management has established policies and implemented controls to stop cyberattacks that may target the agency, we interviewed agency staff, reviewed documentation, and performed limited testing of selected security management controls and CIS Controls™ one through six. The period for our testing included controls in place between February 2019 and April 2019.

In addition to the CIS Controls™, we used the Federal Information System Controls Audit Manual as IT security management criteria.

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. Due to the sensitive nature of security and in accordance to ORS 192.345 (23) and Generally Accepted Government Auditing Standards, we communicated the extent of the security weaknesses verbally to agency management to ensure that no critical security information is publicly disclosed.

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

³ [Center for Internet Security CIS Controls](#)

⁴ Defense-in-depth refers to the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives.

Assessment Results

Our review identified specific areas where DAS could improve security controls. In particular, DAS 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, DAS lacks basic foundational IT controls for all six CIS controls we reviewed as part of this assessment. This is largely due to the fragmented organizational structure and the numerous legacy applications within various business units of DAS. This structure makes it difficult to have a consistent IT governance and control framework that would ensure key applications, and the environment in which they are hosted, have the appropriate support and security.

DAS lacks a formal security management program

Security management programs of all executive branch agencies should be collaborative efforts with the Enterprise Security Office, located within the Office of the State Chief Information Officer. Under this governance structure, the ESO is responsible for enterprise information security strategy and planning, while the DAS IT Division is responsible for the development, documentation, and implementation of a security management program for its specific environment, including workstations and applications.

To effectively manage security, agencies should 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 parties are adequately secured.

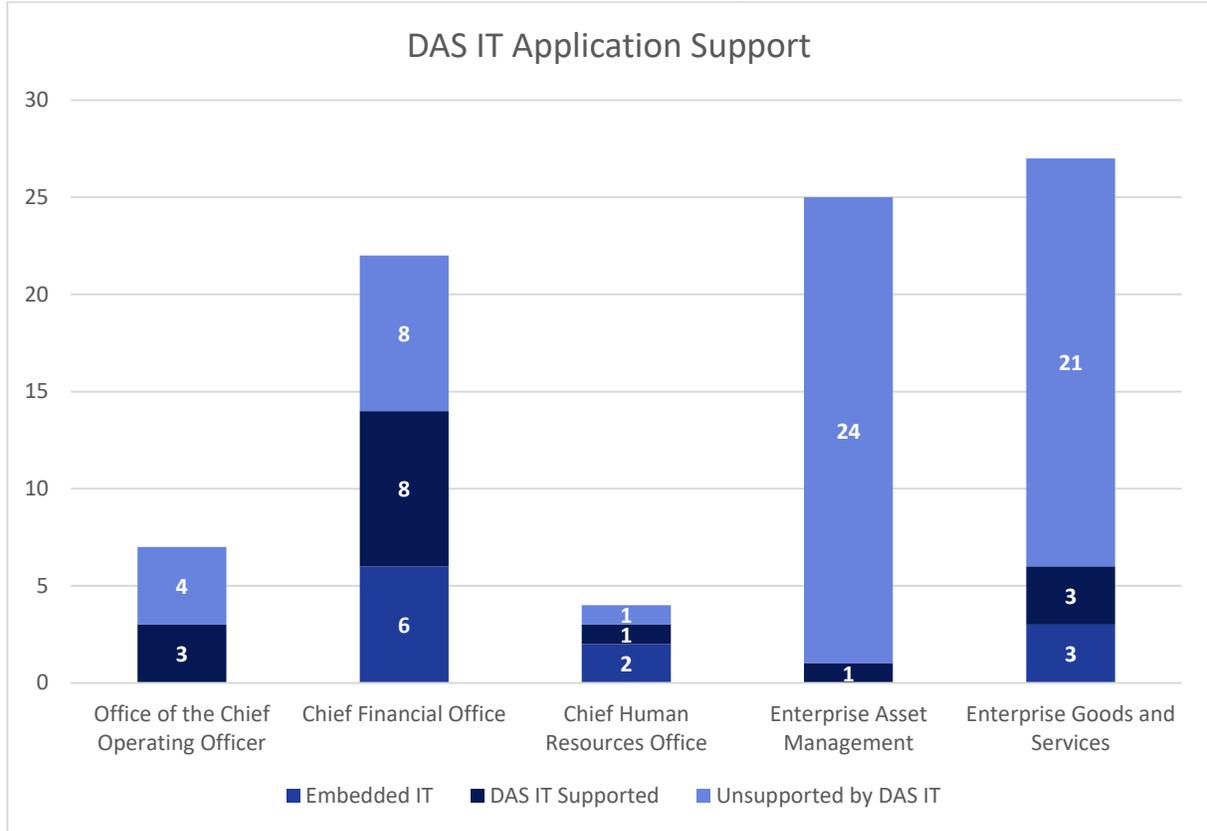
We determined DAS does not have a security management program and lacks formal policies and procedures for all security related controls reviewed. In addition, DAS does not have an established framework for continuously assessing risk, developing and implementing effective procedures, and monitoring the effectiveness of these procedures. In addition, the DAS CIO does not have sufficient knowledge of DAS computer resources or appropriate oversight and staffing to support applications and carry out other responsibilities of the office.

DAS business units have fragmented IT support and lack IT governance

Within the divisions of DAS, there are approximately 30 subdivisions or business units that receive varying levels of support from DAS IT. DAS identified 85 key applications used by these business units, only 16 of which are directly supported by DAS IT.⁵

⁵ This excludes key applications the Office of the State CIO uses, as this division is out of our audit scope.

Figure 2: DAS IT Division staff does not provide support for most agency applications



There are 11 key applications that are supported by IT staff directly embedded within the individual business units, but those staff do not report to DAS IT. Non-IT business unit staff, with no direct involvement or oversight from DAS IT, support the remaining 58 key applications.

This fragmented organizational structure, coupled with numerous unsupported legacy applications within various business units, has created an inconsistent environment where each division or subdivision has their own IT processes and procedures that may or may not align with DAS IT, or accepted best practices. We noted some business units have more robust IT controls in place, while others have limited controls. As such, DAS does not have a consistent IT governance and control framework that would ensure these key applications, and the environments in which they are hosted, have the appropriate support and security.

The DAS CIO role lacks appropriate functional authority and staffing to carry out its official responsibilities

As part of our assessment, we reviewed the DAS CIO official position description duties and compared them to what the CIO has authority over in practice and whether DAS IT has sufficient staff to perform security functions. We found a significant discrepancy between the official position description duties and what the CIO can accomplish. For example, the CIO is tasked with oversight over DAS’s electronic information assets, yet is not always involved with the implementation, monitoring and securing of assets in the business divisions. In addition, 15% of the CIO’s time should be spent ensuring IT security and compliance, which is appropriately considered an “essential” duty, according to the position description. However, the CIO does not have any staff to accomplish the necessary tasks.

While IT security has been largely consolidated within the ESO, 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. However, since DAS IT does not have IT staff dedicated to this work, these critical activities are only performed on an inconsistent, ad hoc basis, which hinders the agency’s ability to address identified weaknesses. For example, while DAS has taken some initial planning steps and requested funding, the agency has not resolved the majority of the numerous critical weaknesses and vulnerabilities identified in four separate third-party assessments performed since 2016.

Without a well-designed program, 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 Assessment

For this assessment, 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 using four levels of implementation to provide an assessment of the agency’s overall cybersecurity implementation. Except when necessary to review collaborative security processes with the Enterprise Security Office, we excluded from our scope the divisions of the Office of the State CIO, including Enterprise Technology Services, which manages the State Data Center. As such, the following graphs include only the controls that are the responsibility of DAS’s IT division.

Figure 3: Control Implementation Level Hierarchy

Performed	Assesses whether the controls are performed at some level. This could include manual and ad hoc actions taken by individuals, even if there are no formal procedures developed around the activity.
Defined	Assesses whether there are defined policies and procedures around the control. This measure does not assess whether or not the controls defined in the policies and procedures are actually performed.
Automated	Assesses whether controls are automated at some level. This could be accomplished through the use of a tool to assist in the performance of the control that still requires manual action (at a lower assessed level), or through automated enforcement of the control (at a higher assessed level).
Continuously Improved	Assesses controls at a higher maturity level. At this level, the controls must at least be fully performed and defined, and the organization uses the operation of these controls to continuously improve the design and execution of the controls.

Some of the sub-controls specifically include automation in the description. For example, sub-controls 2.3 and 3.4 require the use of automated software tools to document software inventory and apply operating system patches, respectively. However, if the agency has manual processes in place that achieve the same objective, we may assess these sub-controls at the performed or partially performed level.

CIS Control 1™: Inventory of Authorized and Unauthorized Devices

Sub-Control	Title	Assessed Control Implementation Rating			
		Performed	Defined	Automated	Continuously Improved
1.1	Utilize an Active Discovery Tool	○	○	○	○
1.2	Use a Passive Asset Discovery Tool	○	○	○	○
1.3	Use DHCP Logging to Update Asset Inventory	○	○	○	○
1.4	Maintain Detailed Asset Inventory	○	○	○	○
1.5	Maintain Asset Inventory Information	○	○	○	○
1.6	Address Unauthorized Assets	○	○	○	○
1.7	Deploy Port Level Access Control	○	○	○	○
1.8	Utilize Client Certificates to Authenticate Hardware Assets	○	○	○	○
○ = Not Implemented ● = Partially Implemented ● = Fully Implemented					

We evaluated DAS's processes to identify network devices, maintain an updated inventory of hardware devices, and control devices that can connect to the network. We found the agency does not maintain inventories of devices and does not utilize available tools to identify devices on its network. While the agency has a spreadsheet that lists some hardware devices, we found this spreadsheet to be incomplete, inaccurate, out-of-date, and generally unreliable.

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 up-to-date inventory of authorized hardware, the agency may not identify unauthorized devices, which limits the agency's ability to prevent or detect unauthorized access to the network.

CIS Control™ 2: Inventory of Authorized and Unauthorized Software

Sub-Control	Title	Assessed Control Implementation Rating			
		Performed	Defined	Automated	Continuously Improved
2.1	Maintain Inventory of Authorized Software	○	○	○	○
2.2	Ensure Software is Supported by Vendor	○	○	○	○
2.3	Utilize Software Inventory Tools	◐	○	○	○
2.4	Track Software Inventory Information	○	○	○	○
2.5	Integrate Software and Hardware Asset Inventories	○	○	○	○
2.6	Address unapproved software	○	○	○	○
2.7	Utilize Application Whitelisting	○	○	○	○
2.8	Implement Application Whitelisting of Libraries	○	○	○	○
2.9	Implement Application Whitelisting of Scripts	○	○	○	○
2.10	Physically or Logically Segregate High Risk Applications	○	○	○	○
○ = Not Implemented ◐ = Partially Implemented ● = Fully Implemented					

We evaluated DAS’s process to document approved software, determine high-risk software, and identify software on its systems. While the agency has a tool that would provide a list of all software utilized on workstations and servers, it does not utilize it. Furthermore, due to the fragmented nature of DAS business units, we found some business units continue to have the ability to install software on their workstations without proper authorization.

Controls should be established by implementing software whitelisting, automating software inventory, and monitoring software installations on all systems.⁶ Organizations should maintain an inventory of software installed on their computer systems similar to the inventory of its hardware assets. Without a complete, accurate, and up-to-date list of the software authorized to be on an agency’s systems, it cannot ensure effective controls are in place to protect software on the agency’s information systems.

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.

⁶ Software whitelisting is the practice of identifying a list of approved software and restricting access to installation to only software on the list. Whitelisting reduces the risk of malicious software such as computer viruses or ransomware infecting systems

CIS Control™ 3: Continuous Vulnerability Assessment and Remediation

Sub-Control	Title	Assessed Control Implementation Rating			
		Performed	Defined	Automated	Continuously Improved
3.1	Run Automated Vulnerability Scanning Tools	●	○	○	○
3.2	Perform Authenticated Vulnerability Scanning	●	○	○	○
3.3	Protect Dedicated Assessment Accounts	●	○	○	○
3.4	Deploy Automated Operating System Patch Management Tools	●	○	●	○
3.5	Deploy Automated Software Patch Management Tools	●	○	●	○
3.6	Compare Back-to-back Vulnerability Scans	○	○	○	○
3.7	Utilize a Risk-rating Process	●	●	○	○
○ = Not Implemented ● = Partially Implemented ● = Fully Implemented					

We evaluated DAS’s processes for patching systems to prevent vulnerabilities and for identifying and remediating detected vulnerabilities. While vulnerability management is intended to be a joint effort between DAS and the ESO, we found that DAS does not have assigned staff to perform these duties. Instead, DAS relies on staff to perform vulnerability assessments and remediation on an ad hoc basis as time allows. Furthermore, DAS IT staff do not have appropriate visibility into DAS’s internal network to adequately identify and remediate vulnerabilities. While the agency patches most of its system automatically, some are patched manually. Without full visibility into its network, there is an increased risk that systems and applications may go unpatched.

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 keep 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

Sub-Control	Title	Assessed Control Implementation Rating			
		Performed	Defined	Automated	Continuously Improved
4.1	Maintain Inventory of Administrative Accounts	●	○	○	○
4.2	Change Default Passwords	○	○	●	○
4.3	Ensure the Use of Dedicated Administrative Accounts	●	○	○	○
4.4	Use Unique Passwords	●	○	○	○
4.5	Use Multifactor Authentication For All Administrative Access	○	○	○	○
4.6	Use of Dedicated Machines For All Administrative Tasks	○	○	○	○
4.7	Limit Access to Script Tools	●	○	○	○
4.8	Log and Alert on Changes to Administrative Group Membership	●	○	○	○
4.9	Log and Alert on Unsuccessful Administrative Account Login	●	○	○	○
○ = Not Implemented ● = Partially Implemented ● = Fully Implemented					

We evaluated DAS’s processes to grant and monitor privileged access, to log and monitor login activity, and to establish robust authentication procedures.⁷ We found inconsistent practices across the various business units, with little monitoring of privileged accounts. Furthermore, we found some business units were not applying the “least privilege” principle of providing only the necessary access to perform respective job duties.⁸ Controls could be improved by developing more detailed policies and procedures for privilege accounts, improving alerting of changes to administrative account assignments, expanding multifactor authentication for administrative tasks, and ensuring privileged users use dedicated machines and accounts for all administrative tasks.

Management 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.

⁷ 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.

⁸ Least privilege is the principle that a security system should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

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

Sub-Control	Title	Assessed Control Implementation Rating			
		Performed	Defined	Automated	Continuously Improved
5.1	Establish Secure Configurations	●	○	○	○
5.2	Maintain Secure Images	●	○	○	○
5.3	Securely Store Master Images	●	○	○	○
5.4	Deploy System Configuration Management Tools	●	○	○	○
5.5	Implement Automated Configuration Monitoring Systems	●	○	○	○
○ = Not Implemented ● = Partially Implemented ● = Fully Implemented					

We evaluated DAS’s processes to document and safeguard baseline configurations, deploy secure configurations, and monitor configurations on its network. We determined DAS has not taken important steps to establish secure baselines for most servers, network devices, and workstations. While most workstation configurations are controlled through centrally automated rules, there is no formal review to ensure those rules are not modified inappropriately. Furthermore, DAS does not have processes in place to monitor configurations on devices to ensure no unauthorized changes are made.

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

Sub-Control	Title	Assessed Control Implementation Rating			
		Performed	Defined	Automated	Continuously Improved
6.1	Utilize Three Synchronized Time Sources	●	○	●	○
6.2	Activate audit logging	●	○	●	○
6.3	Enable Detailed Logging	●	○	●	○
6.4	Ensure adequate storage for logs	●	○	●	○
6.5	Central Log Management	●	○	○	○
6.6	Deploy SIEM or Log Analytic tool	○	○	○	○
6.7	Regularly Review Logs	○	○	○	○
6.8	Regularly Tune SIEM	○	○	○	○
○ = Not Implemented ● = Partially Implemented ● = Fully Implemented					

We evaluated DAS’s processes to collect, manage, and analyze audit logs of events that could help the agency detect, understand, or recover from an attack. We found that DAS does not adequately generate audit logs for all workstations, servers, and network devices. Furthermore, DAS does not monitor or review logs that are generated automatically by network devices. Additionally, DAS has not developed formal processes or procedures regarding the maintenance, monitoring, and analysis of audit logs.

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 of time. 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 DAS, in cooperation with the ESO, where appropriate:

1. Implement a security management 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, automating asset discovery and inventory, and implementing hardware authentication controls.
3. Remedy weaknesses with CIS Control #2 – Software Inventory – by developing written policies and procedures, implementing tracking and documentation of approved software and software versions, and implementing software whitelisting.
4. Remedy weaknesses with CIS Control #3 – Vulnerability Assessment – by developing written policies and procedures, working with the ESO to ensure DAS IT has full visibility into its network, and formally tracking the status of identified vulnerabilities to ensure timely remediation.
5. Remedy weaknesses with CIS Control #4 – Privileged Access – by restricting privileged access to only those who need it to perform their job duties, maintaining and inventory of administrative accounts, ensuring default passwords are changed, ensuring the use of dedicated administrative accounts, implementing multifactor authentication for all administrative access, and implementing alerts associated with administrative account activities.
6. Remedy weaknesses with CIS Control #5 – Secure Configurations – by establishing secure configurations for all workstations, servers, and network devices under DAS IT's control. Additionally, 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.



Oregon

Kate Brown, Governor

Department of Administrative Services
Office of the Chief Operating Officer
155 Cottage Street NE
Salem, OR 97301
PHONE: 503-378-3104
FAX: 503-373-7643

June 25, 2019

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 **Department of Administrative Services Cybersecurity Controls Assessment**.

Thank you for providing the Department of Administrative Services (DAS) the audit report. We appreciate the work and collaborative approach of the Audits Division staff and are pleased to have the recommendations in the report. The report highlights the importance of security controls as it relates to our IT systems. We are committed to improve our efforts in this area going forward.

DAS is currently in a transition phase as it relates to IT Security. In 2016 Governor Brown issued Executive Order 16-13 that directed agencies to unify cyber security in Oregon under the Office of the State Chief Information Officer (OSCIO). This was codified in the 2017 Legislative session with Senate Bill 90. The OSCIO is in the process of identifying what the ongoing security role will be between the OSCIO and state agencies, including DAS.

DAS has already made some progress in improving how DAS IT functions. There is a project to develop a formal IT Governance structure. DAS included in its budget request, which was finalized in March of 2018, additional IT resources, including one position to oversee the DAS IT Asset Management program for both hardware and software. DAS also requested resources to engage an independent external consultant(s) to assess and advise on DAS modernization, IT structure, capabilities and governance. The budget requests related to DAS IT functions have now been approved by the 2019 legislature and DAS will be able to begin its critical work related to improving DAS IT security.

DAS, working in concert with the OSCIO, will be using this information, new resources, and audit recommendations to move forward in addressing critical security responsibilities.

Below you will find DAS' response to the specific audit recommendations.

RECOMMENDATION 1		
Implement a security management 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	July 2023	Greg Sanker

Narrative for Recommendation 1

With the consolidation of information security resources and responsibility into the Enterprise Security Office (ESO), DAS will continue working closely with the ESO to establish an agency framework for information security program within DAS.

DAS has received funding in the 2019-21 budget for an external independent assessment that includes assessing DAS IT capability, including information security. The recommendations, in conjunction with the ESO will inform a request for resources for the 2021-23 biennium to operationalize the DAS information security program.

RECOMMENDATION 2		
Remedy weaknesses with CIS Control #1 – Hardware Inventory – by developing written policies and procedures, automating asset discovery and inventory, and 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	July 2021	Greg Sanker

Narrative for Recommendation 2

The DAS 2019-21 budget includes funding to establish an asset management (hardware and software) position starting October 2019.

The independent external assessment (see recommendation 1) will evaluate and provide specific recommendations for creating an overall asset management program and inform DAS IT management on a roadmap to implement an effective program for managing hardware and software assets.

DAS IT will work with the OSCIO as state policies are updated, and incorporate into the DAS asset management program.

While DAS anticipates having a functional program in place by June 2021, updated information security policies and additional recommendations from the external assessment may expand the scope of the program and necessitate additional resource requests for the 2021-23 biennium.

RECOMMENDATION 3		
Remedy weaknesses with CIS Control #2 – Software Inventory – by developing written policies and procedures, implementing a tracking and documentation of approved software and software versions, and implementing software whitelisting.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	July 2021	Greg Sanker

Narrative for Recommendation 3

The asset management position referenced in the narrative for Recommendation 2 is expected to be in place by October 2019 and will also focus on software asset management.

DAS IT is developing an application whitelisting practice in the upcoming Windows 10 update, scheduled for completion by June 2020. This foundation will enable additional maturity in software inventory controls.

As state information security policies are updated and recommendations from the assessment are considered, additional resources may be requested for the 2021-23 biennium.

RECOMMENDATION 4		
Remedy weaknesses with CIS Control #3 – Vulnerability Assessment – by developing written policies and procedures, working with the ESO to ensure DAS IT has full visibility into its network, and formally tracking the status of identified vulnerabilities to ensure timely remediation.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	July 2023	Greg Sanker

Narrative for Recommendation 4

DAS will work collaboratively with the ESO to establish vulnerability management program scope, policies, procedures, and roles and responsibilities for DAS.

The DAS external independent assessment of DAS IT capability will include information security. Recommendations from the vulnerability assessment, in conjunction with the ESO will inform a request for resources for the 2021-23 biennium to operationalize the DAS vulnerability assessment program.

RECOMMENDATION 5		
Remedy weaknesses with CIS Control #4 – Privileged Access – by restricting privileged access to only those who need it to perform their job duties, maintaining and inventory of administrative accounts, ensuring default passwords are changed, ensuring the use of dedicated administrative accounts, implementing multifactor authentication for all administrative access, and implementing alerts associated with administrative account activities.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	July 2023	Greg Sanker

Narrative for Recommendation 5

DAS management will work collaboratively with the ESO to establish policies and procedures for privileged access management and establish privilege access practice.

The independent external assessment will include analysis and recommendations for privilege access management practices. DAS anticipates some recommendations may require budget items that will be included in the 2021-23 budget request.

RECOMMENDATION 6		
Remedy weaknesses with CIS Control #5 – Secure Configurations – by establishing secure configurations for all workstations, servers, and network devices under DAS IT’s control. Additionally, 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	July 2023	Greg Sanker

Narrative for Recommendation 6

For servers and network devices, DAS uses enterprise services provided by Enterprise Technology Services (ETS). DAS management will work with ETS and the ESO to ensure these services comply with the Statewide Information Security Plan maintained by the ESO.

For workstations, DAS management will establish and maintain standard configurations for PC hardware and software, and develop policies and procedures to monitor and maintain secure configuration.

RECOMMENDATION 7		
Remedy weaknesses with CIS Control #6 – Audit Logs – by developing a central logging solution, implementing log analytic tools, and automating log review.		
Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	July 2023	Greg Sanker

Narrative for Recommendation 7

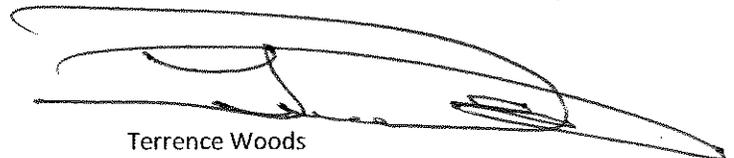
DAS will work closely with the ESO as state policies are updated and enterprise information security capabilities are developed and available for agency use.

DAS will collaborate with the ESO to establish operational policies, procedures, and roles and responsibilities. This, along with the external independent assessment will inform budget requests for 2021-23 biennium.

Please contact Lisa Upshaw, DAS Chief Audit Executive at Lisa.UPSHAW@oregon.gov or 503-378-3076 with any questions.

Sincerely,


Katy Coba
COO | DAS Director


Terrence Woods
State Chief Information Officer



Assessment 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