Department of Consumer and Business Services

Cybersecurity Controls Audit

November 2021
Report 2021-31

OREGON SOS
Secretary of State
Shemia Fagan

OREGON AUDITS DIVISION
Audits Director
Kip Memmott

Audit Highlights

Department of Consumer and Business Services
Cybersecurity Controls Audit

Why this audit is important

- The Department of Consumer and Business Services (DCBS) provides a broad range of consumer protection, health insurance access, and commercial regulations for the state. It is Oregon's largest consumer protection and business regulatory agency.
- DCBS has a budget of approximately $660 million and over 900 employees.
- 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.
- This audit assessed critical security controls and the IT security management practices at DCBS.

What we found

Our review identified specific areas where DCBS should improve cybersecurity controls. DCBS has an incomplete security management and compliance program and does not meet all the basic IT controls for the six CIS controls we reviewed. We identified the following areas for improvement:

1. DCBS has established a security management and compliance program, but more work remains to ensure that agency systems and data are protected against unauthorized use, disclosure, or modification. (pg. 4)
2. DCBS does not actively manage hardware devices on its network to ensure only authorized devices connect, nor does it actively manage its software to ensure only authorized software is installed. (pg. 5)
3. Vulnerability and patch management are performed on a limited, ad-hoc basis. (pg. 7)
4. DCBS does not appropriately manage all users who have high-level access to its systems and data. (pg. 8)
5. More work is needed to ensure that all devices are appropriately configured and monitored to ensure settings remain appropriate. (pg. 8)
6. The agency needs processes, central logging, and the necessary tools to monitor and review the audit logs for all workstations, servers, and network devices for inappropriate behavior. (pg. 9)

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 DCBS that include improving IT security plans and remedying weaknesses we identified in basic CIS Controls™. DCBS agreed with all of our recommendations. The response can be found at the end of the report.

OREGON SOS
OREGON AUDITS DIVISION

Introduction

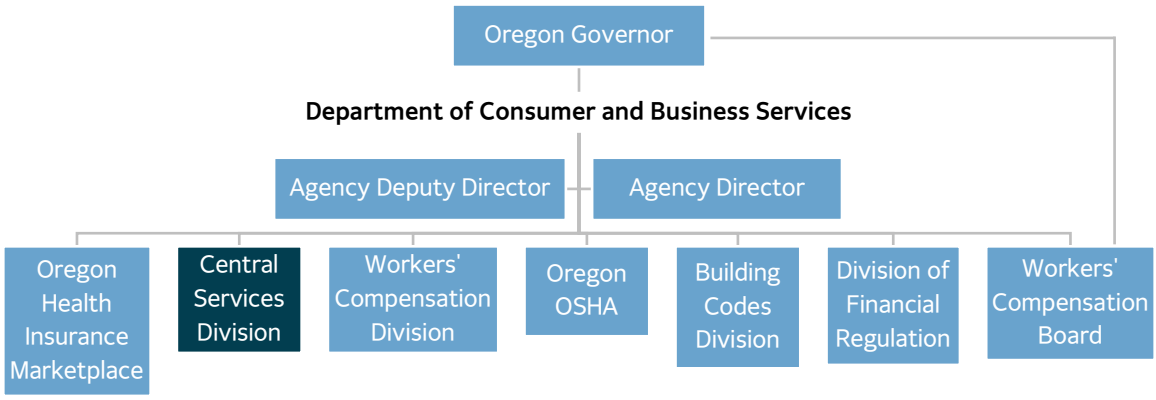
Cyberattacks are a growing concern for both the private and public sector. Past breaches at Oregon state agencies have only escalated this concern. To protect against growing threats, state agency leadership should ensure that information technology (IT) management professionals apply robust cybersecurity controls at various levels of infrastructure to protect their networks, servers, and user workstations for the agencies they oversee. 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, define as key controls that every organization should implement for essential cyber defense readiness. Additionally, used the Government Accountability Offices Federal Information System Controls Audit Manual's Security Management criteria to evaluate security management practices at the agency.

In the following pages, we present the results as charts depicting the implementation status of sub-controls in each control as fully implemented, partially implemented, or not implemented. This provides agency management, the Legislature, and others with responsibility for cybersecurity in the state with a snapshot of high-risk areas.

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.

DCBS serves as an umbrella agency over most state functions affecting businesses



The Department of Consumer and Business Services (DCBS) is Oregon's largest consumer protection and business regulatory agency. As such, DCBS increasingly focuses on IT to support agency initiatives including, but not limited to, electronic application and renewal processes for professional licensees; online systems for businesses to submit assessments, reports, and data to the department; filing complaints; accepting citation appeals; and Workers' Compensation Board transactions. The department was formed in 1993 to serve as an integrated umbrella agency over most state functions affecting businesses to improve efficiency and effectiveness. For the 2021-23 biennium, the agency's budget was over $662 million funding 929 full-time equivalent (FTE) positions.

The mission of DCBS is to protect and serve Oregon's consumers and workers while supporting a positive business climate. The agency serves as a resource to consumers and businesses in areas involving building safety, workplace health and safety, financial services, and health care enrollment.

DCBS has multiple divisions or units, including:

- Building Codes Division;
- Central Services Division;
- Division of Financial Regulation;
- Director's Office;
- Oregon Occupational Safety and Health Division;
- Workers' Compensation Division; and
- Workers' Compensation Board.[1]

The Information Technology and Research Section is located within the Central Services Division

The Information Technology and Research Section (IT&R) designs, develops, and maintains IT applications and infrastructure for all divisions of DCBS. In addition, the section collects, researches, analyzes, and reports data for internal and external use. IT&R consists of four main groups:

- Systems Infrastructure (13 FTE)
- Customer Support & System Maintenance (25 FTE)
- Solution Development & Delivery (20 FTE)
- Research (15 FTE)

In the 2021-23 Governor's Budget, the IT&R section had over $21.6 million allocated for 79 FTE to support agency staff.

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.[2] The order directed executive branch agencies to consolidate security functions and staffing

[1] DCBS provides administrative support to the Worker's Compensation Board. The board chair is appointed by the Governor and confirmed by the Legislature.
[2] Executive Order 16-13, "Unifying Cyber Security in Oregon"

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. 1.5 FTE were transferred from DCBS. To compensate for the loss of security staffing, Cyber Security Services (CSS), the EIS branch responsible for cyber security, intended to assign executive branch agencies a Business Information Security Officer to provide guidance, planning, and security leadership. In the interim period, CSS has provided services to DCBS, including a 2018 assessment of the agency's security controls. EIS, through CSS, conducts vulnerability assessments of state agency information systems to evaluate and respond to the information systems threats.

EIS maintains policy and statewide IT oversight functions. CSS 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 CSS to ensure the confidentiality, availability, and integrity of their sensitive business information. CSS continues to define the division of security responsibilities and functions between its office and agencies.

Audit Results

Our review identified areas where DCBS should improve cybersecurity controls. Specifically, DCBS needs to mature its security management program by establishing a framework for assessing risk, developing and implementing effective security processes and procedures, and monitoring the effectiveness of those processes and procedures.

Additionally, while some sub-controls are partially implemented to various degrees, DCBS lacks fully implemented cybersecurity controls for all six basic foundational CIS controls reviewed. We determined this is largely due to a lack of prioritization for implementing these controls, as most of the weaknesses identified had been previously communicated to DCBS in 2016 and 2018, with limited progress.

We considered the risks posed by publicly releasing any information related to security findings. As part of our consideration, 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 cybersecurity threats. Consequently, in accordance with ORS 192.345(23) and generally accepted government auditing standards, we excluded some details of the security weaknesses from this public report and provided them to agency management and EIS in a confidential appendix.

DCBS has not fully implemented a security management and compliance program

Security management programs of all executive branch agencies should be collaborative efforts with EIS and CSS. 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 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 training;
- Remediate information security weaknesses; and
- Ensure external third-party activities are adequately secured.

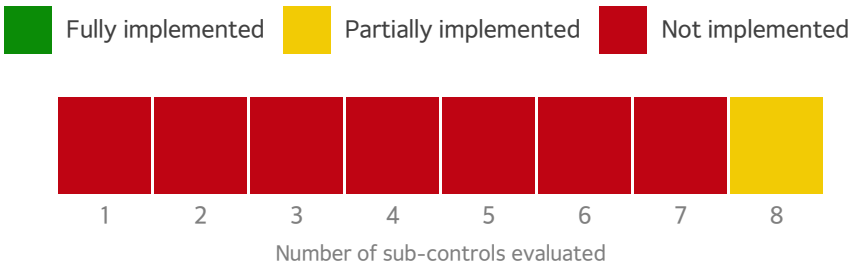
We determined that DCBS has established a security management and compliance program, but extensive work remains to ensure that agency systems and data are protected against unauthorized use, disclosure, or modification. Specifically, DCBS needs to mature processes for assessing, validating, and mitigating risks, ensuring third-party activities are secure, and finish documenting security control policies and procedures. This finding is particularly significant because these weaknesses and more have been identified and communicated in two separate confidential assessments in 2016 and 2018 first by the Oregon Audits Division and then by CSS.

While some aspects of IT security have been consolidated within CSS, other aspects of IT security — application security, network vulnerability scanning and monitoring, and patching of servers not hosted by EIS' Data Center Services — remain with the agency. Yet without sufficient staff assigned specifically to security tasks, most critical activities are performed on an ad-hoc basis, potentially hindering DCBS' ability to thoroughly identify and respond to security incidents.

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

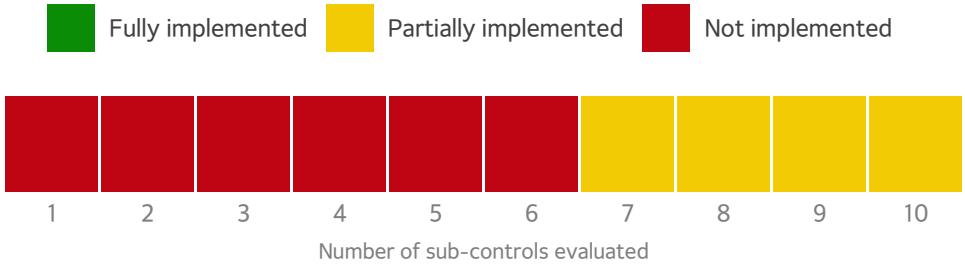


We evaluated DCBS' processes to identify network devices, maintain an updated inventory of hardware devices, and ensure only approved devices can connect to the network. We determined DCBS has not fully implemented any IT controls that would help identify, respond to, or protect its hardware assets so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Specifically, DCBS does not use automated tools to track and monitor hardware assets. Instead, the agency uses a manual process at the division level to track assets in separate inventories. These inventories are updated with new asset purchases and during annual physical inventories. However, no single, complete inventory of all agency assets is maintained by DCBS, and the processes used may not fully capture all its hardware assets.

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

CIS Control™ 2: Inventory of Authorized and Unauthorized Software

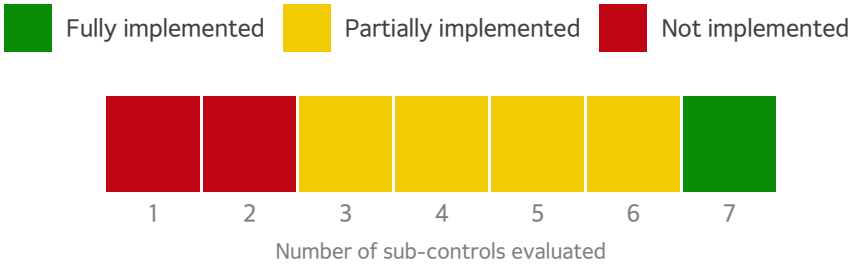


We evaluated DCBS' process to document approved software, segregate high-risk software, and identify software installed on its systems. We determined the agency has some tools in place to identify and track software installed on devices connected to its network, although these tools were primarily directed toward procurement instead of creation of a complete, accurate, agencywide inventory. However, DCBS does use an application portal that limits what software users have access to within its environment. Other weaknesses identified include not having a list of approved software, not integrating hardware and software inventories, and not fully implementing whitelisting to ensure only authorized software could be installed on agency systems. In practice, DCBS does isolate systems that were determined to be riskier.

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 hardware assets. Attackers continuously scan targeted organizations looking for vulnerable versions of software to exploit. 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. 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 unnecessary 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



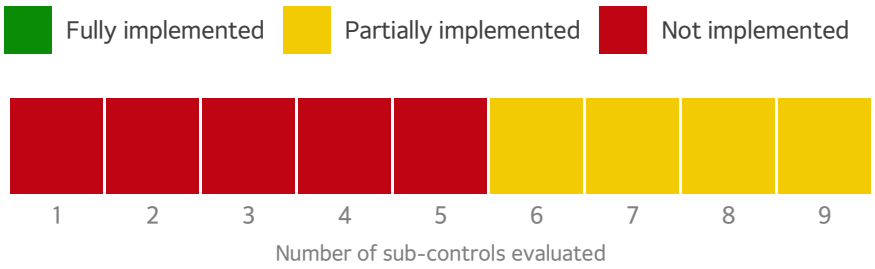
We evaluated DCBS' processes related to continuous vulnerability management, including the use of authenticated vulnerability scans, protection of dedicated assessment accounts, deploying automated operating system and application patch management tools, and comparing back-to-back vulnerability scans.

We found DCBS performs monthly network vulnerability scans, which identifies critical vulnerabilities that may impact its network environment. However, processes to assign, review, and remediate critical vulnerabilities were informal and largely ad-hoc. While EIS' Data Center Services manages most of DCBS' server patch management, we noted the agency does not have reliable processes in place to monitor and ensure that these critical activities take place. While we noted most systems were fully patched, gaps in patch management processes resulted in some systems not receiving critical software updates. Additionally, we noted some systems did not have required anti-virus protection. These were corrected at the time of the audit.

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 whether or not to implement patches, and implement appropriate changes in a timely manner.

CIS Control™ 4: Controlled Use of Administrative Privileges

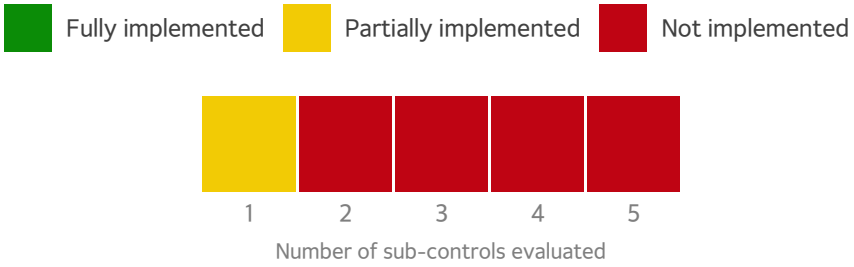


We assessed DCBS' processes and tools used to control access to privileged accounts, log and monitor login activity, and to establish robust authentication procedures.[3]

We found the agency generally lacked processes and procedures for granting, reviewing, monitoring, and terminating access for privileged accounts. Additionally, we found that DCBS lacks a full listing of users with significant access, has insufficient password setting requirements for some servers, has unused accounts that were no longer needed, and lacks multifactor authentication for all administrative accounts.

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 their use.

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



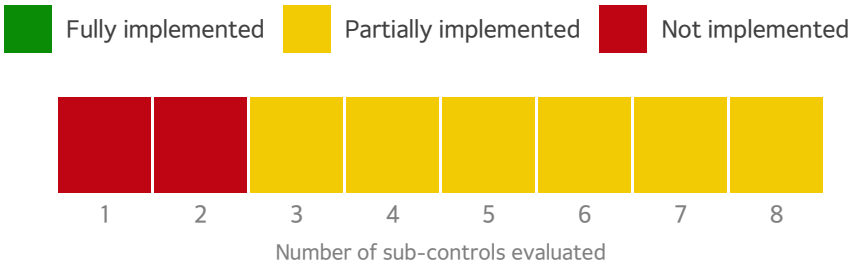
We evaluated DCBS' processes to document and safeguard baseline configurations, deploy secure configurations, and monitor configurations on its network. We noted DCBS has established secure configurations for most end user hardware, including desktops and mobile devices. However, more work is needed to ensure that all servers are appropriately configured. Additionally, we found DCBS

[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.

lacks appropriate tools to monitor and automatically redeploy system configurations if settings are inadvertently or maliciously changed.

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 to ensure 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. 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. 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 DCBS' processes for collecting, managing, and analyzing audit logs of events that could help detect, understand, or recover from an attack. We found logging enabled for most workstations, servers, and network devices. However, we determined that these logs were reviewed on an ad-hoc basis and that not all logs contained the necessary information to fully analyze potential threats.

Additionally, DCBS was found to have centralized logging for some, but not all, devices, and the retention period for all logs was insufficient to meet the statewide standard of three years. Furthermore, the agency relies on two time sources provided by EIS' Data Center Services to ensure audit log time stamps are accurate and has not established a third independent time source as required by the CIS Controls.

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 complete information for each event. Additionally, processes should be established to ensure these logs are reviewed in a timely fashion to identify inappropriate or unusual activity and remediate security events.

Recommendations

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

1. Fully implement an agency security management program to include an established framework and continuous cycle of activity for assessing and mitigating risk, developing and implementing effective security controls and procedures, monitoring the effectiveness of those procedures, and ensuring agency security plans address current IT risks. Track deficiencies and have a plan of action to remediate prior noted risks by external assessments or audits.

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, automating the documentation of DCBS' inventory, ensuring software is supported by its vendor, integrating hardware and software inventories, and implementing software whitelisting.

4. Remedy weaknesses with CIS Control #3 — Vulnerability Assessment — by developing formal policies and procedures, and formally monitoring and tracking the status of identified vulnerabilities to ensure timely remediation.

5. Remedy weaknesses with CIS Control #4 — Privileged Access — by creating processes and procedures for granting privileged access, reviewing privileged access regularly to verify it remains appropriate, maintaining an inventory of administrative accounts, implementing multifactor authentications for all administrative access, and ensuring alerts associated with administrative account activities are timely sent to appropriate staff.

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

7. Remedy weaknesses with CIS Control #6 — Audit Logs — by establishing an adequate number of independent time sources, increasing available log storage size to meet statewide standards, ensuring detailed logging includes all required fields, developing a central logging solution for all agency devices, utilizing available log analytic tools, and automating and formalizing processes for log review for all domains.

Objective, Scope, and Methodology

Objective

Our audit objective was to determine the extent to which DCBS 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.[4] These controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices to help protect systems and networks from the most common attacks.[5]

Scope

The scope of this work included a review of security management based on FISCAM Security Management criteria, and the first six of the 20 CIS Controls™ in place at DCBS during the second and third quarters of 2021. Cybersecurity experts generally agree that these six "basic" controls should be implemented by all organizations for cyber defense readiness.

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; and
- Network diagrams.

Observed:

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

Interviewed:

- IT staff;
- IT managers;
- DCBS' Chief Information Officer; and
- Executive leadership.

[4] Center for Internet Security CIS Controls.
[5] Defense-in-depth refers to the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives.

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 with 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.

Internal control review

We determined that the following internal controls were relevant to our audit objective.[6]

- 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

[6] Auditors relied on standards for internal controls from the U.S. Government Accountability Office, report GAO-14-704G.

using a 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 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.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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

Audit team
Teresa Furnish, CISA, Audit Manager
Matthew Owens, MBA, CISA, Principal Auditor
Karin Bryant, Staff Auditor
Sheila Faulkner, 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.

Oregon
Kate Brown, Governor

Department of Consumer and Business Services
Director's Office
350 Winter Street NE, Room 200
PO Box 14480
Salem, OR 97309-0405
Voice: 503-947-7872
Fax: 503-947-0088
www.dcbs.oregon.gov

October 28, 2021

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

Director Memmott:

This letter provides a written response to the Audits Division's final draft audit report titled "Department of Consumer and Business Services Cybersecurity Controls Audit."

The Department of Consumer and Business Services (DCBS) appreciates the collaboration demonstrated by the Secretary of State (SOS) during the performance of this audit. We appreciate your partnership and thank you for recognizing where good work is already being done. We welcome the findings in the report as areas for further improvement and are committed to working with our central state partners to fully implement a mature cybersecurity framework.

DCBS complies with Oregon's cybersecurity standards, either through full compliance, mitigating controls, or risk acceptance (particularly in areas outside of DCBS control). As with any government entity, DCBS experiences many attempts to probe our external systems, but successfully identifies and stops these attempts. DCBS has also uncovered and remediated hundreds of software code vulnerabilities to lower the risks of attackers exploiting our applications. DCBS has not had any cybersecurity incidents that have resulted in data breaches or significant system outages in the past five years.

As is typical within any risk management framework and across the state enterprise, some minor risks are accepted in which data and privacy protection are not at stake. These occasional risks are accepted to maintain business operations and address business-side resource or partner constraints. Past audits and assessments accounted for organizational maturity and risk acceptance to temper resultant grading.

The inherent challenges faced by DCBS are similar to other Oregon state organizations. Maturing the DCBS cybersecurity program requires that the organization increase the available resources (staffing and tools), particularly around threat and risk assessment, documentation, inventory detection and management, and monitoring. During this audit, DCBS took active steps to update its existing risk tracking, perform remediation task prioritization, and complete or begin work on several additional (to work already in flight) cybersecurity process and procedure improvements.

DCBS is fully committed to continuing to improve its security stance, protect state systems and data, and reduce risk. As outlined below, we have already responded to several audit findings. We are also establishing an executive oversight committee, led by the agency director and deputy director, to meet regularly with program staff and track compliance with a project plan that will respond to all audit findings. DCBS takes its responsibility as a steward of state systems and data very seriously and appreciates the areas for improvement identified through this audit.

Below is our detailed response to each recommendation in the audit.

RECOMMENDATION 1

Fully implement an agency security management program to include an established framework and continuous cycle of activity for assessing and mitigating risk, developing and implementing effective security controls and procedures, monitoring the effectiveness of those procedures, and ensuring agency security plans address current IT risks. Track deficiencies and have a plan of action to remediate prior noted risks by external assessments or audits.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Deficiency tracking: **complete** Controls/procedures: **mid-2022** Full program: **end-2023**	Dane Wilson 971-718-2374

Narrative for Recommendation 1

DCBS has an active security management program performed by a risk and compliance analyst and fractions of additional operational staff. Included in this program are an active and creative security awareness program, threat exercise program, incident response plan and playbook, and IT security governance. DCBS also engages in active solution vetting and risk assessments (cloud workbooks, for instance) not measured by the SOS audit, but required by the Cybersecurity Services office (CSS) and the Department of Administrative Services (DAS) Procurement office.

DCBS assesses risk areas operationally and then applies work efforts and operational processes to address risks. This leads to well-protected and monitored environments, while working within the resources available to DCBS.

To make incremental, but continuous, improvement within its resources, DCBS uses severity prioritization to address identified risks and mitigations. DCBS also continuously engages with CSS and leverages CSS programs, utilities, materials, and assessments. Work to improve the DCBS cybersecurity stance has been continuous since June 2016.

DCBS agrees its cybersecurity program can be improved. Based upon this audit, an updated remediation matrix has been created and serves as a tool to log assessment and prioritization of tasks and tracking towards completion. The matrix also facilitates conversations about the progress needed.

DCBS will continue its partnership with EIS and CSS, and speak to the Legislature about the needed resources to accomplish the maturing of its security management program. If no additional resources are forthcoming, DCBS will consult with CSS for guidance on how to best proceed.

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	Procedures, improved asset discovery/inventory: **end-2022** Fully complete: **mid-2023**	Dane Wilson 971-718-2374

Narrative for Recommendation 2

DCBS is actively working on documenting existing processes and procedures.

DCBS will require new tools and staffing to identify, implement, and operate automated asset discovery, inventory, and hardware authentication. DCBS may have to make organizational process and procedure changes to facilitate a more centralized approach. This is also an enterprise problem and may require partnership with EIS, CSS, and Data Center Services (DCS) to complete.

DCBS agrees this area can be improved. DCBS will develop and implement improved hardware inventory strategies that include an appropriate mix of tools, policies/procedures, and controls by December 2022. This process will mature over time and be carried out in consultation with CSS and input from other Oregon organizations as partners and resources for solutions.

RECOMMENDATION 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, automating the documentation of DCBS' inventory, ensuring software is supported by its vendor, integrating hardware and software inventories, 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	Procedures, approved software, tracking support: **end-2022** Fully complete: **end-2023**	Dane Wilson 971-718-2374

Narrative for Recommendation 3
DCBS is a large agency with multiple lines of business, each with its own program controls, goals, and requirements. This increases the DCBS software portfolio. For instance, DCBS must acquire and support tools used to review building plans, conduct bank examinations, or create work safety training videos.

DCBS already has a software purchasing/vetting process and is restricting allowed mobile device software leveraging our mobile device management (MDM) tool.

Much like recommendation No. 2, continued process improvement will require new or expanded use of existing tools and staffing to identify, implement, and operate automated software discovery, inventory, and track vendor support of products. DCBS may have to make organizational process and procedure changes to facilitate a more centralized approach. This is also an enterprise problem and may require partnership with EIS, CSS, and DCS to complete.

DCBS agrees this area can be improved. DCBS will develop and implement software inventory strategies that include an appropriate mix of automated tools, policies/procedures, and controls by December 2022. This process will also mature over time and in consultations with CSS and input from other Oregon organizations.

RECOMMENDATION 4

Remedy weaknesses with CIS Control #3 — Vulnerability Assessment — by developing formal policies and procedures, and formally monitoring and 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	VM plan: **mid-2022** Fully complete: **end-2022**	Dane Wilson 971-718-2374

Narrative for Recommendation 4
DCBS relies on the CSS vulnerability scanning service. DCBS does not control when CSS reports on vulnerabilities, particularly in relation to system patching for systems hosted at the DCS facilities. This means that monthly reported vulnerabilities are often remediated within the next patching cycle. Enterprise maturity or reporting adjustments may be needed for DCBS to demonstrate improved compliance.

DCBS does initiate separate internal scanning using the same CSS scanning tool. DCBS staff members regularly monitor its systems and platforms, along with consulting industry resources to identify vulnerabilities. Ongoing work occurs to regularly address known vulnerabilities.

User authentication is necessary to access nearly all DCBS data and services. DCBS leverages its virtual computing environment access control and user authentication to provide remote access, multi-factor authentication (MFA), and segmented privileges. DCBS can detect attackers' scans and maintains a high level of vigilance on all systems that are Internet accessible. Most DCBS non-Internet accessible and data resources are protected by layers and are not typically susceptible to external scans; however, support staff monitor them, as well.

DCBS agrees this area can be improved. In partnership with CSS and DCS, DCBS will develop a vulnerability management program plan by April 2022 and implement vulnerability assessment strategies that include an appropriate mix of tools, policies/procedures, and controls that align with the agency's computing and staff resources. DCBS will also improve its monitoring of vendors to ensure remediations and maintenance are applied and operational. This is another area that will mature over time as resources are brought to bear and additional enterprise progress is made.

RECOMMENDATION 5

Remedy weaknesses with CIS Control #4 — Privileged Access — by creating processes and procedures for granting privileged access, reviewing privileged access regularly to verify it remains appropriate, maintaining an inventory of administrative accounts, implementing multifactor authentications for all administrative access, and ensuring alerts associated with administrative account activities are timely sent to appropriate staff.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Processes, review, and inventory: **mid-2022** Fully complete: **mid-2023**	Dane Wilson 971-718-2374

Narrative for Recommendation 5

User authentication is necessary to access nearly all DCBS data and services. DCBS leverages its virtual computing environment access control and user authentication to provide remote access, MFA, and segmented privileges.

DCBS has prioritized expanding our implementation of MFA. Implementing MFA on DCBS computing resources that are not accessible outside of the DCBS network or to general staff is in progress. This was started before the SOS audit. During the audit period and since, DCBS has continued to advance the number of internal systems that require MFA.

DCBS has also completed an access control project to define role-based access groups across the department. Software requirements were created and proof-of-concept efforts to test software tools were accomplished. Acquisition and implementation of a new access control tool is on hold due to resource constraints.

DCBS agrees this area can be improved. DCBS will assess the resources needed to make improvements. Meanwhile, DCBS will consult with CSS and improve its hybrid manual/automated processes.

RECOMMENDATION 6

Remedy weaknesses with CIS Control #5 — Secure Configurations — by establishing secure configurations for all workstations, servers, and network devices. Establish 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	Configuration strategy: **end-2022** Fully complete: **mid-2023**	Dane Wilson 971-718-2374

Narrative for Recommendation 6

DCBS centrally creates, tests, and deploys workstation images. Server images are provided by DCS or derived from the DCS base image for servers managed by DCBS. DCBS leverages the state's network services, so it does not manage network device images.

Improvement in this area will require staff time to enhance the agency's use of existing tools, identify additional tool capabilities, and implement and operate automated configuration management. DCBS may have to make organizational process and procedure changes to facilitate a more centralized approach. This is also an enterprise problem and may require partnership with EIS, CSS, and DCS to complete.

DCBS agrees this area can be improved. DCBS will develop and implement configuration management strategies that include an assessment of automated tools, completion of written policies/procedures, and consultation with CSS about next steps.

RECOMMENDATION 7

Remedy weaknesses with CIS Control #6 — Audit Logs — by establishing an adequate number of independent time sources, increasing available log storage size to meet statewide standards, ensuring detailed logging includes all required fields, developing a central logging solution for all agency devices, utilizing available log analytic tools, and automating and formalizing processes for 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	Time sources, log storage, fields: **end-2022** Fully complete: **mid-2023**	Dane Wilson 971-718-2374

Narrative for Recommendation 7

DCBS partners with CSS to coordinate security event monitoring services using the CSS security analytics tool.

DCBS staff regularly analyze the logs of critical systems to be on the lookout for errors and non-standard activity. DCBS employs a log analysis tool to enhance this work and is setting up dashboards in the tool to enhance log analysis and alerting even more.

DCBS agrees this area can be improved. DCBS will re-examine the state standards on log retention and content, and correct any deviations in our current practices. DCBS does not possess a central logging solution for all devices. This is most likely also an enterprise problem and may require partnership with EIS, CSS, and DCS to complete.

If you have any questions, please contact DCBS Chief Information Officer Dane Wilson at 971-718-2374.

Kind regards,

Andrew R. Stolfi
Director
Department of Consumer and Business Services

OREGON SOS
Secretary of State
Shemia Fagan

OREGON AUDITS DIVISION
Audits Director
Kip Memmott

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
audits.sos@oregon.gov
sos.oregon.gov/audits