Department of Corrections

Cybersecurity Controls Audit

July 2022
Report 2022-20

OREGON SOS
Secretary of State
Shemia Fagan

OREGON AUDITS DIVISION
Audits Director
Kip Memmott

Audit Highlights

Department of Corrections
Cybersecurity Controls Audit

Why this audit is important

- The Oregon Department of Corrections (DOC) operates prisons for adult offenders sentenced to prison for longer than 12 months. To support this work, the agency stores and transmits sensitive data, including criminal justice and health records for adults in custody.
- In 2021, the Legislature appropriated just over $2 billion to DOC. The agency's information technology (IT) department supports more than 6,000 users of IT resources.
- 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, IT management professionals should apply robust cybersecurity controls at various levels of infrastructure to protect IT resources.

What we evaluated

The Audits Division conducts cybersecurity audits to evaluate IT security risks and provide a high-level view of an agency's current state. We used the Center for Internet Security's CIS Controls™, version 8. The CIS Controls™ are a prioritized list of 18 high-priority defensive actions providing a framework for enterprises to improve cyber defense.

What we found

We found DOC has partially implemented 16 of the 17 CIS Controls™ we evaluated. Due to gaps in inventory management processes, we could not identify all assets and provide complete assurance that some controls were in place. These controls included those associated with safeguards in data management, configuration management, vulnerability management, and malware defense. Additionally, gaps in training — specifically role-based training — may be cause for some of the deficiencies identified during the audit.

What we reported

Based on the sensitive nature of our findings, details have been excluded from this public report; full details were issued in a separate, confidential appendix to DOC and Enterprise Information Services (EIS).

What we recommend

We made 17 recommendations to DOC to remedy weaknesses we identified in the CIS Controls™. DOC agreed with all of our recommendations. The response can be found at the end of the report. For security purposes, those recommendations have been communicated in a separate, confidential appendix in accordance with ORS 192.345(23).

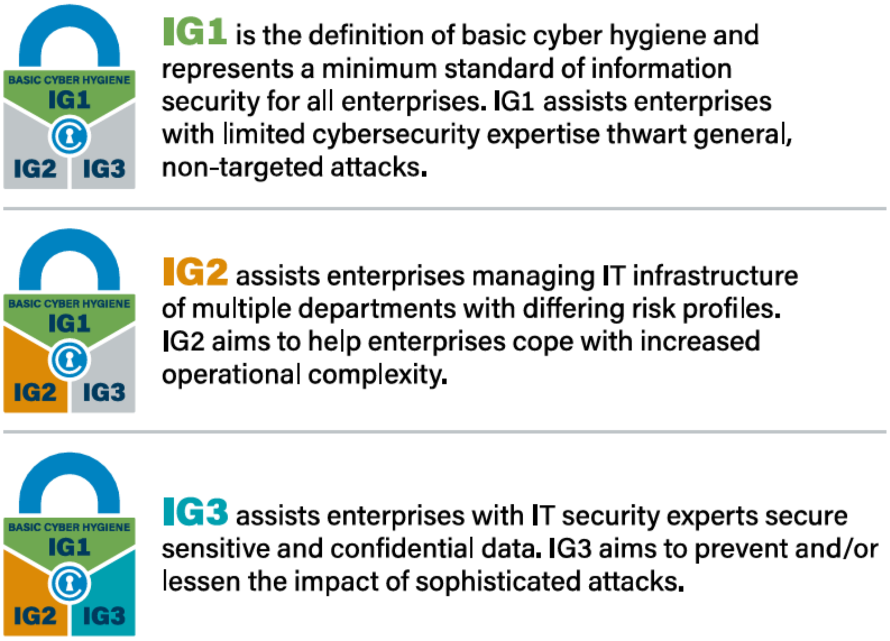
Introduction

Cyberattacks are an ongoing concern for both the private and public sectors. Past breaches at Oregon state agencies have only escalated this concern. To protect against these threats, state agency leadership should ensure 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 CIS Controls™ provide a framework for enterprises to improve cyber defense. The controls are divided into three Control Implementation Groups (IGs) based on the risk profile and resources of the organization:

- The Center for Internet Security™ defines IG1 enterprises as small to medium-sized with limited IT and cybersecurity expertise. These organizations are primarily concerned with keeping their business operational and the sensitivity of their data is low.
- IG2 enterprises are those with individuals responsible for managing and protecting IT infrastructure. They support multiple departments with differing risk profiles and often store and process sensitive information.
- An IG3 enterprise employs security experts who specialize in different facets of cybersecurity. They must maintain service availability and the confidentiality and integrity of sensitive data. Successful attacks against IG3 organizations can cause significant harm to public welfare.

This audit includes cybersecurity controls applicable to IG2 organizations.



IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

CIS Controls™ are divided into three categories based on risk profile and available resources. | Source: CIS Controls™ Implementation Groups Handout

Each of the 18 controls has a number of "safeguards," or specific individual defensive actions against potential cyberattacks. Safeguards are grouped as controls that focus efforts on a certain defensive goal; each safeguard must be in place before a control is considered fully implemented. In the following pages, we present our findings as charts depicting the implementation status of safeguards in each control. Our goal is to provide agency management, the Legislature, and others with responsibility for cybersecurity in the state with a snapshot of high-risk areas.

Figure 1: Implementation status categories

Not
The safeguard is not in place or could not be audited due to lack of evidence.

Somewhat
Largely incomplete, but some things are in place (e.g., processes are ad hoc, only occurs in one environment, etc.).

Mostly
Largely complete, but some things are missing (e.g., process in place but not formally defined, missing in one environment, etc.).

Fully
The safeguard is in place.

This audit does not consider an agency's risk appetite.[1] Therefore, while these controls are considered best practice 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 safeguard.

This public report omits certain details in the interest of security. Full details, including recommendations on how to address identified gaps, have been communicated to the agency in a confidential appendix.

The Oregon Department of Corrections oversees the state's prison system

The mission of the Oregon Department of Corrections (DOC) is to promote public safety by holding criminal offenders accountable for their actions and reducing the risk of future criminal behavior. To this end, the agency operates prisons for adult offenders sentenced to prison for longer than 12 months. DOC houses approximately 14,900 adults in 14 prisons throughout the state.

The 2021-2023 legislatively approved budget for DOC totals $2.2 billion. The budget includes 4,791 positions. Of this total, the approved budget for DOC's Administrative Service Division — which includes Information Technology Services, among other functions — was just under $132 million, with 270 positions.

Information Technology Services at DOC provides central support, management, and maintenance of IT services for more than 6,000 users. Users consist of both agency staff and community corrections staff in counties across the state. This section also develops and maintains software and databases to support adult in custody management and programs, and agency operational functions. The agency is

[1] An agency's risk appetite is the amount of risk the agency is willing to accept in pursuit of its mission and vision.

responsible for the secure storage and transmittal of sensitive data related to adults in custody, including criminal justice data and health records.

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 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.[3] Two positions were transferred from DOC. To compensate for the loss of security staffing, Cyber Security Services (CSS), the EIS branch responsible for cyber security, provides various security services, including:

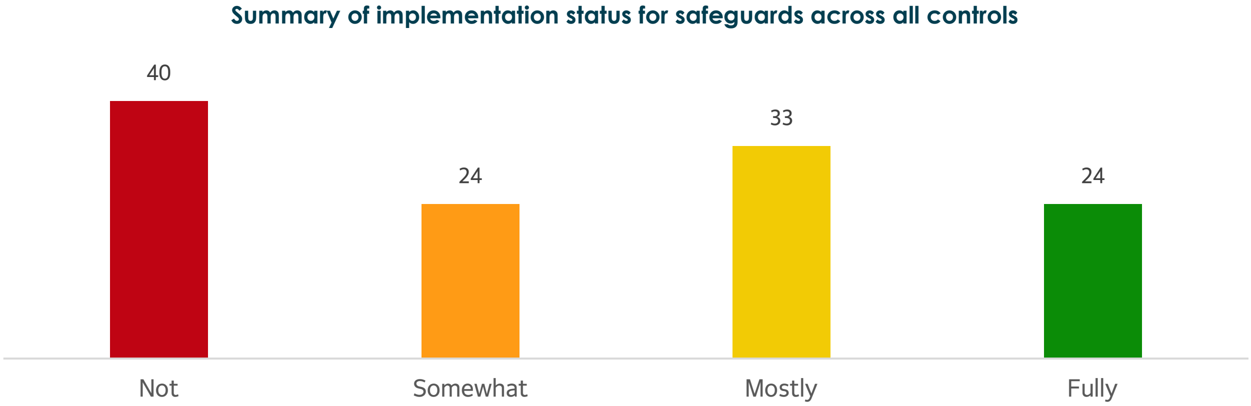
- General security awareness training;
- Infrastructure and data protection guidance and consultation;
- Identity lifecycle management and advisory services;
- Security operations services;
- Security administration advisory services;
- Systems integration guidance;
- Vendor management services; and
- Security consulting services.

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.

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

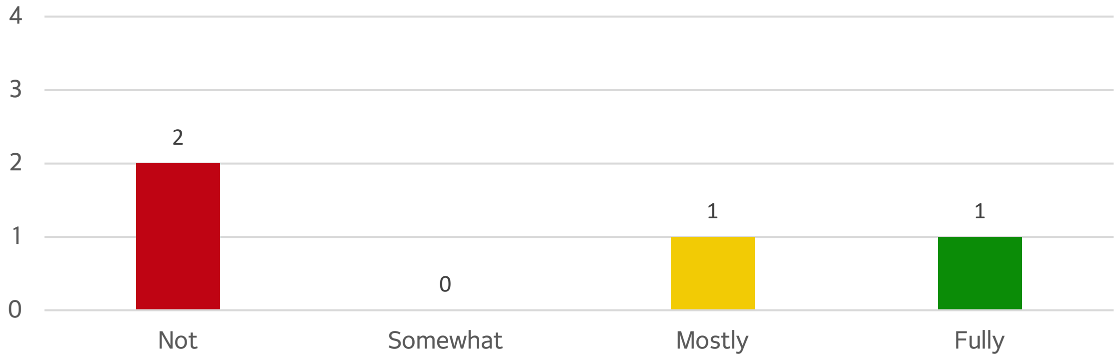
Audit Results

For this audit, we evaluated the implementation level of DOC's cybersecurity control environment against the CIS Controls™ and the associated safeguards enumerated under IG2, which are described below.



We evaluated each safeguard to provide an assessment of the agency's overall cybersecurity implementation. The charts below illustrate the number of safeguards evaluated for each control objective and how many of those safeguards fall into each of the implementation status categories. Additionally, we have described why each control group is important based on narrative in the CIS Controls™ documentation. See pg. 2 of this report for an overview of how auditors determined the category of each safeguard.

CIS Control™ 1: Inventory and Control of Enterprise Assets



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

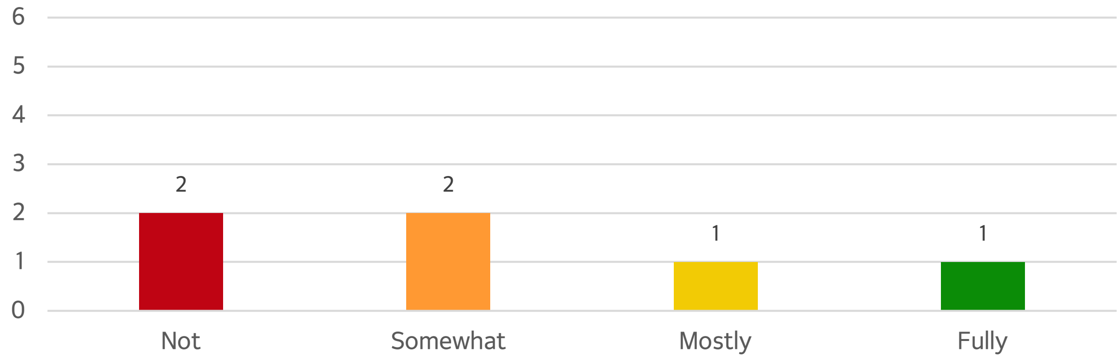
1. Establish and Maintain Detailed Enterprise Asset Inventory
2. Address Unauthorized Assets
3. Utilize an Active Discovery Tool to Identify Assets
4. Use Dynamic Host Configuration Protocol Logging to Update Enterprise Asset Inventory

WHY THIS MATTERS:

Agencies cannot defend assets they do not know they have. New or unidentified devices on an agency's network may introduce vulnerabilities. Without adequate controls in place, attackers can take advantage of new or unidentified assets that are not securely configured. Therefore, managed control of all assets is critical to effective security monitoring, system backup, and recovery. Moreover, complete asset management can support incident response, including identification of the origination of unauthorized network traffic and potentially affected assets.

Organizations should maintain a complete and up-to-date inventory with sufficient detail to effectively track and manage all enterprise assets.

CIS Control™ 2: Inventory and Control of Software Assets



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

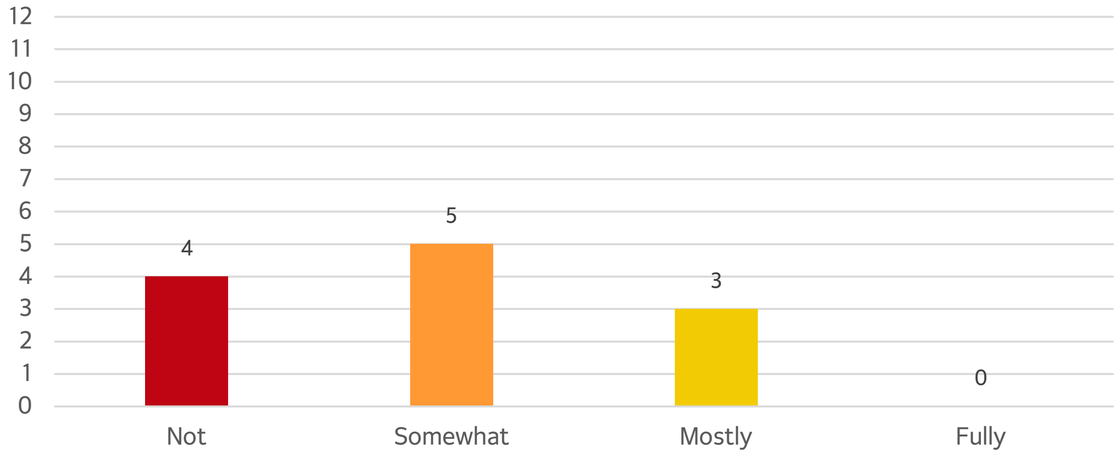
1. Establish and Maintain a Software Inventory
2. Ensure Authorized Software is Currently Supported
3. Address Unauthorized Software
4. Utilize Automated Software Inventory Tools
5. Allowlist Authorized Software
6. Allowlist Authorized Libraries

WHY THIS MATTERS:

Attackers continuously scan targeted organizations looking for vulnerable versions of software to exploit. Agencies can prevent these attacks by ensuring only authorized and up-to-date software is installed on agency assets. However, without a complete, accurate, and up-to-date list of the software authorized to be on its systems, an agency cannot determine whether vulnerable software exists in its environment.

Organizations should maintain an inventory of software installed on their computer systems, similar to the inventory of hardware assets, so they are aware of what they possess and the risks those assets pose. Additionally, organizations should implement software and library allowlisting, automate software inventory, and monitor software installations on all systems to ensure only appropriate software is installed on agency assets.

CIS Control™ 3: Data Protection



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

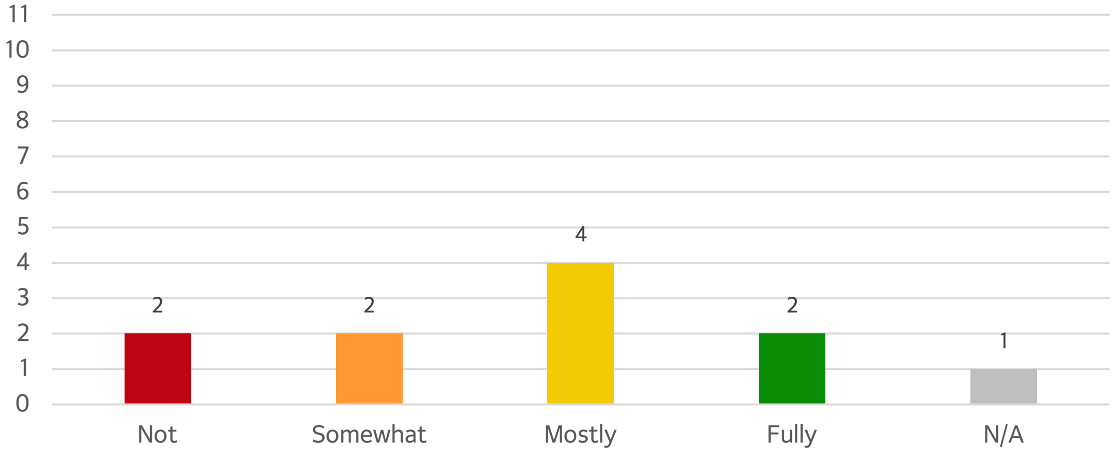
1. Establish and Maintain a Data Management Process
2. Establish and Maintain a Data Inventory
3. Configure Data Access Control Lists
4. Enforce Data Retention
5. Securely Dispose of Data
6. Encrypt Data on End-User Devices
7. Establish and Maintain a Data Classification Scheme
8. Document Data Flows
9. Encrypt Data on Removable Media
10. Encrypt Sensitive Data in Transit
11. Encrypt Sensitive Data at Rest
12. Segment Data Processing and Storage Based on Sensitivity

WHY THIS MATTERS:

Agency data is stored in a variety of locations and shared with a variety of partners and online services. Once breached, attackers can find and exfiltrate data. Data may also be lost or otherwise compromised as a result of poor data management or user error. To protect sensitive data, ensure alignment with regulations, and protect data privacy, agencies should use and manage data through its entire life cycle.

An effective data management process should include a framework, classification guidelines, and requirements for protection, handling, retention, and disposal of data. Once the sensitivity of data has been defined, agencies should develop a data inventory or mapping identifying software accessing data at various sensitivity levels and the enterprise assets housing those applications. One key tool for mitigating data compromise is the use of data encryption both in transit and at rest. Ideally, the network would be separated so enterprise assets of the same sensitivity level are on the same network and separated from enterprise assets with different sensitivity levels.

CIS Control™ 4: Secure Configuration of Enterprise Assets and Software



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

1. Establish and Maintain a Secure Configuration Process
2. Establish and Maintain a Secure Configuration Process for Network Infrastructure[4]
3. Configure Automatic Session Locking on Enterprise Assets
4. Implement and Manage a Firewall on Servers
5. Implement and Manage a Firewall on End-User Devices
6. Securely Manage Enterprise Assets and Software
7. Manage Default Accounts on Enterprise Assets and Software
8. Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
9. Configure Trusted DNS Servers on Enterprise Assets
10. Enforce Automatic Device Lockout on Portable End-User Devices
11. Enforce Remote Wipe Capability on Portable End-User Devices

WHY THIS MATTERS:

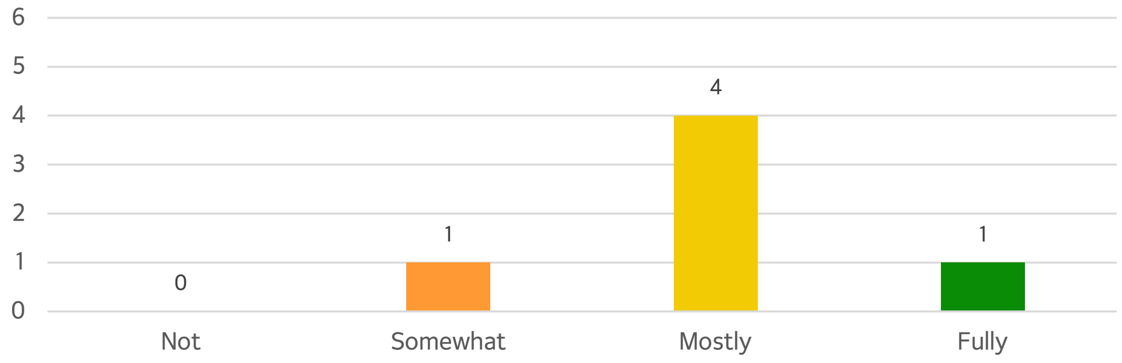
Default configurations for IT assets and software are normally geared toward ease of deployment and ease of use rather than security. Default accounts or passwords, excessive access, or unnecessary services could be exploited by attackers.

To address these risks, organizations should have processes in place to ensure hardware and software are securely configured. This should include verifying configurations align with business and security needs to ensure agency systems are not left vulnerable to attack. Agencies should have configuration management processes in place to implement secure system control features at the initiation of the system life cycle. Entities should also ensure software is patched and configurations remain secure as modifications are made to the system.

To achieve this, baselines satisfying security requirements and standards should be developed. Deviations from baselines should be monitored and documented. Additionally, policies and procedures should be in place to address how configuration baselines are managed.

[4] We did not evaluate this safeguard because the control is primarily managed by Enterprise Information Services.

CIS Control™ 5: Account Management



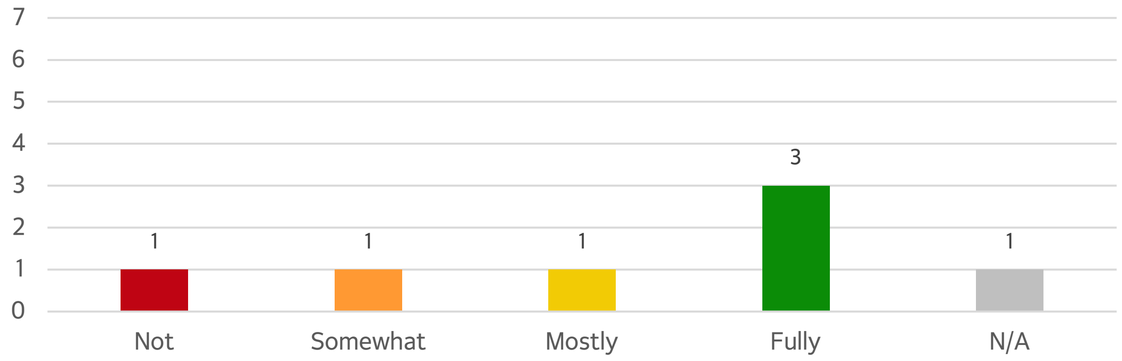
CIS Controls™ indicates organizations in IG2 should have the following safeguards in place:

1. Establish and Maintain an Inventory of Accounts
2. Use Unique Passwords
3. Disable Dormant Accounts
4. Restrict Administrator Privileges to Dedicated Administrator Accounts
5. Establish and Maintain an Inventory of Service Accounts
6. Centralize Account Management

WHY THIS MATTERS:

It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets by using valid user credentials than through “hacking.” To mitigate these risks, management should ensure only authorized users can access agency accounts. Effective management should include maintenance of an inventory of all agency accounts (user, administrative, and service), unique password requirements, and centralization of management through a directory or identity service.

CIS Control™ 6: Access Control Management



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

1. Establish an Access Granting Process
2. Establish an Access Revoking Process

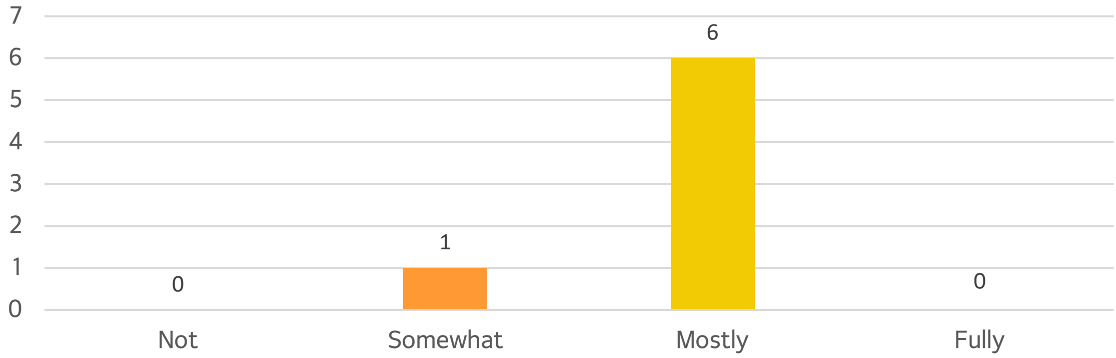
3. Require MFA for Externally-Exposed Applications[5]
4. Require MFA for Remote Network Access
5. Require MFA for Administrative Access
6. Establish and Maintain an Inventory of Authentication and Authorization Systems[6]
7. Centralize Access Control

WHY THIS MATTERS:

The more access a user has to agency systems, the more vectors for attack are available if their account is compromised. Therefore, users should only have access to the data or assets necessary for their role. Moreover, some user activities pose greater risk because they are initiated from untrusted networks or are performed from accounts with elevated privileges allowing them to modify other accounts or agency systems.

Where CIS Control™ 5 focused on management of accounts, CIS Control™ 6 focuses on management of access to agency accounts, ensuring appropriate role-based access, and ensuring strong, appropriate authentication is in place. Key practices for access management include development of consistent processes for assigning access rights and roles and granting of and removal of access. Use of MFA and Privileged Access Management tools are important for reducing the risk of accounts inappropriately accessing agency resources.

CIS Control™ 7: Continuous Vulnerability Management



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

1. Establish and Maintain a Vulnerability Management Process
2. Establish and Maintain a Remediation Process
3. Perform Automated Operating System Patch Management
4. Perform Automated Application Patch Management
5. Perform Automated Vulnerability Scans of Internal Enterprise Assets
6. Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets
7. Remediate Detected Vulnerabilities

[5] MFA, or multifactor authentication, is the use of two or more different factors when verifying a user's identity. Authentication factors may include something you know (such as a password), something you are (such as a fingerprint), or something you have (such as a cryptographic key).

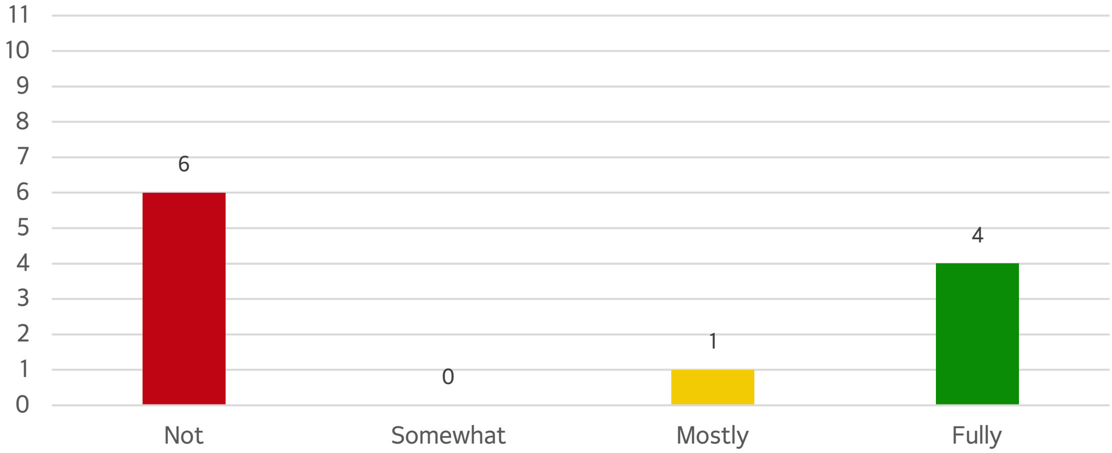
[6] We did not evaluate this safeguard because the control is currently not applicable at DOC.

WHY THIS MATTERS:

Attackers are constantly looking for vulnerabilities to exploit and gain access to organizations' technology resources. Threat actors commonly exploit IT systems missing security patches or with other known vulnerabilities. If an adversary were to gain an initial foothold on the internal network, they could leverage these vulnerabilities to execute arbitrary code on affected systems. This could also allow the adversary to move laterally within the compromised environment.

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 to implement patches, and implement appropriate changes in a timely manner. Organizations should also be continuously engaged in identifying, remediating, and minimizing security vulnerabilities to ensure their assets are safeguarded. 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.

CIS Control™ 8: Audit Log Management



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

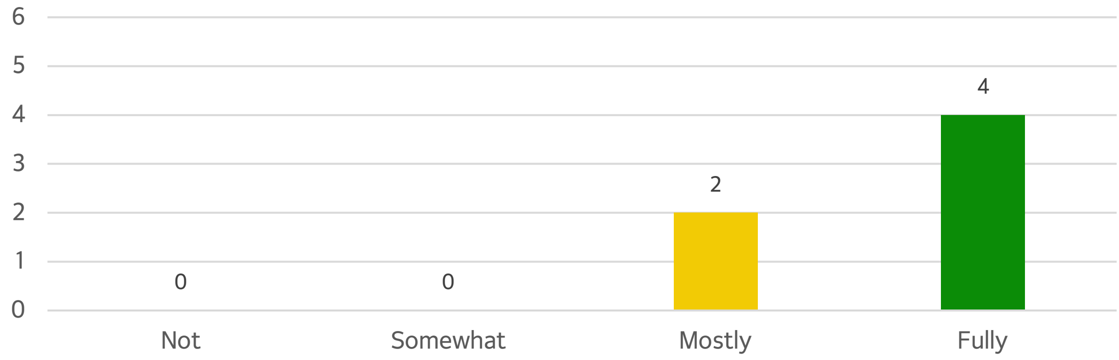
1. Establish and Maintain an Audit Log Management Process
2. Collect Audit Logs
3. Ensure Adequate Audit Log Storage
4. Standardize Time Synchronization
5. Collect Detailed Audit Logs
6. Collect DNS Query Audit Logs
7. Collect URL Request Audit Logs
8. Collect Command-Line Audit Logs
9. Centralize Audit Logs
10. Retain Audit Logs
11. Conduct Audit Log Reviews

WHY THIS MATTERS:

Without adequate audit logs, an attack may go unnoticed indefinitely and the damage done may be irreversible. Deficiencies in security logging and analysis allow attackers to hide malicious software or their own presence. Without protected and complete logging records the agency is blind to the details of the attack and subsequent actions taken by attackers. Deficient logging may allow attackers and malicious activity to go undetected for extended periods.

Robust logging and log monitoring processes allow organizations to identify and understand inappropriate activity and recover more quickly from an attack. Agencies should ensure 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. Log review can be a cumbersome task; therefore, it is best to centralize logging functions to allow defenders to focus on higher-risk events.

CIS Control™ 9: Email and Web Browser Protections



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

1. Ensure Use of Only Fully Supported Browsers and Email Clients
2. Use DNS Filtering Services
3. Maintain and Enforce Network-Based URL Filters
4. Restrict Unnecessary or Unauthorized Browser and Email Client Extensions
5. Implement DMARC[7]
6. Block Unnecessary File Types

WHY THIS MATTERS:

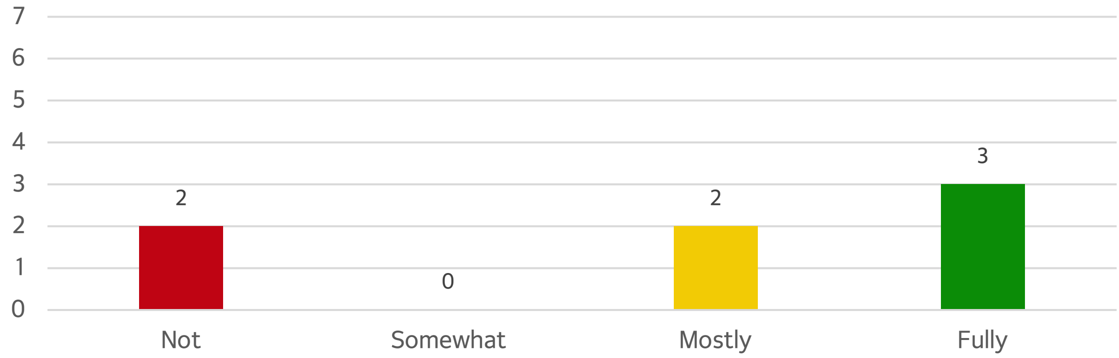
Web browsers and email clients are common attack vectors because they are public facing. Cybercriminals can use web browsers to craft malicious websites to exploit vulnerabilities on devices used by unsuspecting users, or leverage third-party plugins to gain access to users' browser or operating system. Email is involved in more than 90% of all network attacks. Email can be used by attackers to perform phishing or to impersonate a legitimate business in order to trick individuals into providing financial or other sensitive information.[8]

Ensuring browsers and email client versions are current and restricting unnecessary extensions and file types helps protect agency resources from known attacks. Filtering helps reduce unwanted or

[7] DMARC, or Domain-based Message Authentication, Reporting & Conformance, is an email authentication, policy, and reporting protocol designed to improve and monitor protection from fraudulent email.
[8] Phishing is a technique for attempting to acquire sensitive information through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

nefarious emails. Finally, DMARC helps email senders and receivers coordinate to better secure email traffic.

CIS Control™ 10: Malware Defenses



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

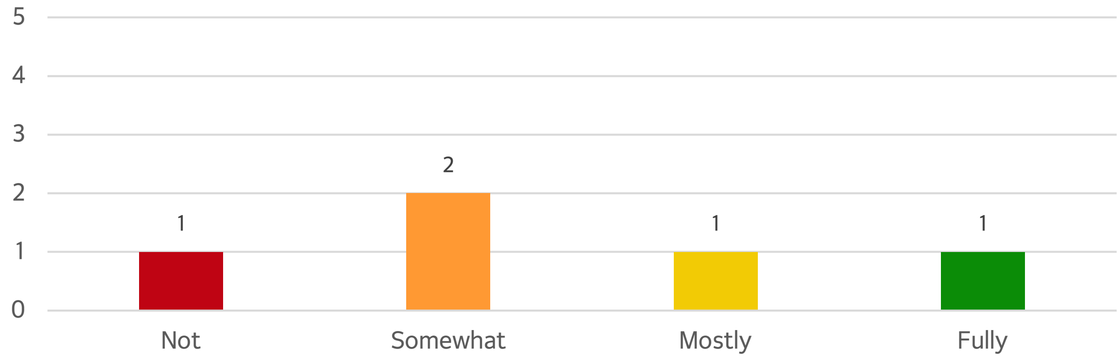
1. Deploy and Maintain Anti-Malware Software
2. Configure Automatic Anti-Malware Signature Updates
3. Disable Autorun and Autoplay for Removable Media
4. Configure Automatic Anti-Malware Scanning of Removable Media
5. Enable Anti-Exploitation Features
6. Centrally Manage Anti-Malware Software
7. Use Behavior-Based Anti-Malware Software

WHY THIS MATTERS:

Malware is used as a means for threat actors to capture credentials, steal data, identify other potential attack targets, and encrypt or destroy data. This can disrupt an agency's ability to serve its mission or put sensitive data at risk. Malware enters enterprises through vulnerabilities and often relies on users performing insecure actions such as clicking on a bad link, opening unknown attachments, installing malicious software, or inserting a compromised flash drive.

Agencies should leverage tools to prevent and detect malicious software. Best practices include managing detection and prevention centrally, with automated processes to ensure malware indicators are up to date.

CIS Control™ 11: Data Recovery



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

1. Establish and Maintain a Data Recovery Process
2. Perform Automated Backups
3. Protect Recovery Data
4. Establish and Maintain an Isolated Instance of Recovery Data
5. Test Data Recovery

WHY THIS MATTERS:

Nefarious actions or human error can result in agency systems being compromised due to configuration changes, malicious or unnecessary accounts, or unapproved software. Configuration changes may result in turning on insecure ports, destroying system logs, or other changes that can make systems insecure. Backups provide management with a means to fall back to a known secure state when systems are compromised.

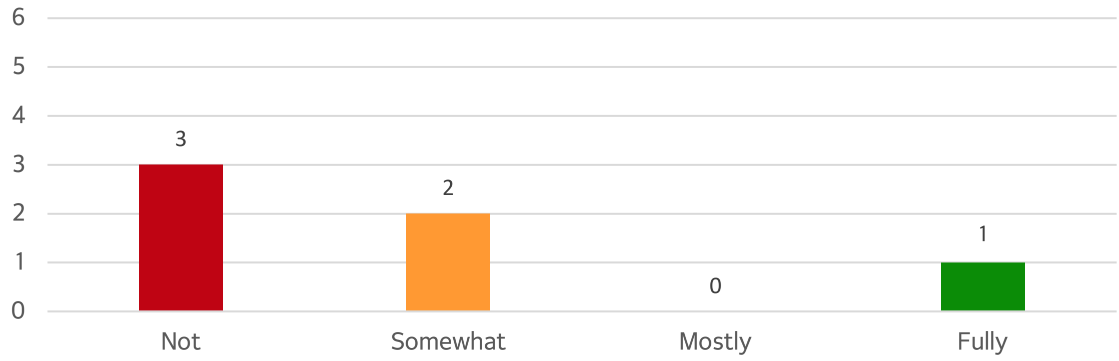
Moreover, ransomware attacks have become more prevalent over recent years. Attackers often encrypt their target's data and demand a ransom for its restoration. Recent reliable backups reduce the organization's risk of losing data or having to pay to have it restored.

Organizations should have processes in place to backup data based on data value and sensitivity, or compliance requirements. Periodic testing should be performed to ensure backups can be restored to an intact and functional state.

CIS Control™ 12: Network Infrastructure Management

We did not evaluate this control because the control is primarily managed by Enterprise Information Services, not DOC.

CIS Control™ 13: Network Monitoring and Defense



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

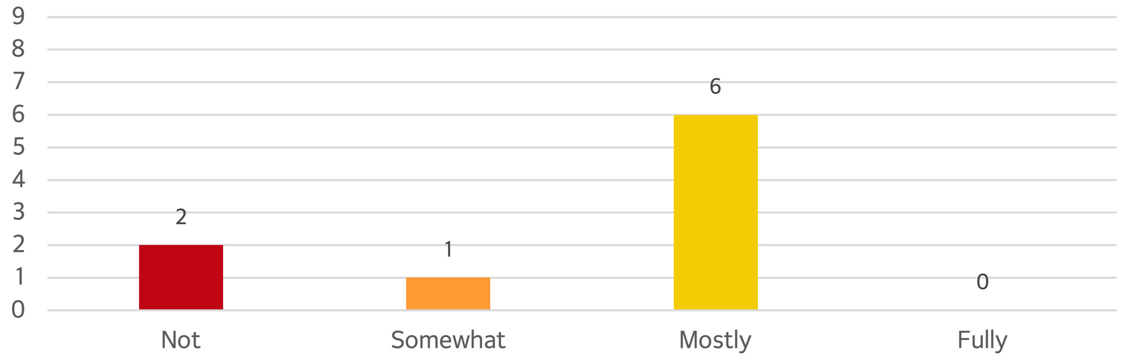
1. Centralize Security Event Alerting
2. Deploy a Host-Based Intrusion Detection Solution
3. Deploy a Network Intrusion Detection Solution
4. Perform Traffic Filtering Between Network Segments
5. Manage Access Control for Remote Assets
6. Collect Network Traffic Flow Logs

WHY THIS MATTERS:

Network defenses will never be perfect. Adversaries continue to evolve and develop new means to bypass security controls. Even controls working as intended need to be continually monitored, tuned, and logged to ensure they remain secure and efficient. Without proper monitoring in place, organizations may not successfully prevent, or timely detect and respond, to security compromises.

Agencies should have processes in place to continuously monitor network security so that defenders can detect, analyze, and respond to threats in a timely manner. Moreover, recovery from security incidents can be achieved faster and more effectively if the agency has access to complete information about how, when, and where the incident occurred.

CIS Control™ 14: Security Awareness and Skills Training



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

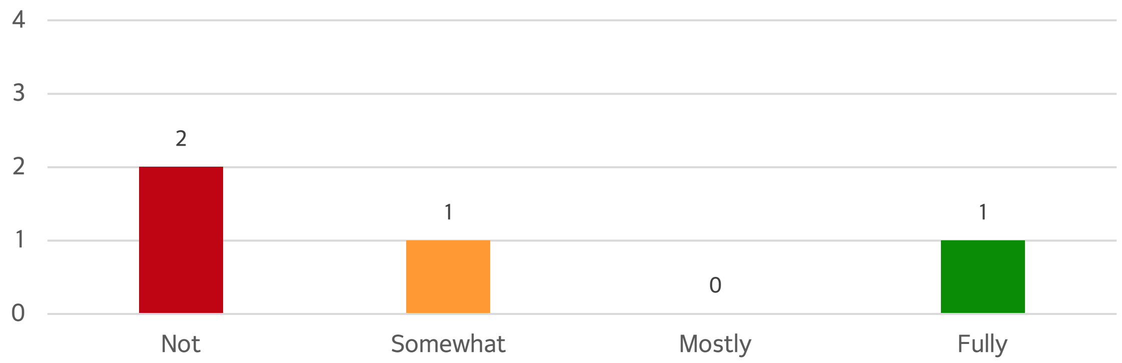
1. Establish and Maintain a Security Awareness Program
2. Train Workforce Members to Recognize Social Engineering Attacks
3. Train Workforce Members on Authentication Best Practices
4. Train Workforce on Data Handling Best Practices
5. Train Workforce Members on Causes of Unintentional Data Exposure
6. Train Workforce Members on Recognizing and Reporting Security Incidents
7. Train Workforce Members on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
8. Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
9. Conduct Role-Specific Security Awareness and Skills Training

WHY THIS MATTERS:

Most security professionals agree any organization’s weakest link is its people. It is easier for an attacker to gain access to an enterprise’s network by enticing a user to click a link than it is to exploit a vulnerability in the network and gain access directly. Moreover, users can easily cause incidents, intentionally or accidentally, by mishandling sensitive data, using weak passwords, or clicking a malicious link.

Agency personnel should receive ongoing security awareness training to understand their role in recognizing and reducing the likelihood and impact of security threats. Training should be ongoing to increase awareness about potential social engineering, authentication, data handling, and other threat topics. Additionally, training should be tailored to the agency's environment as well as users' various roles.

CIS Control™ 15: Service Provider Management



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

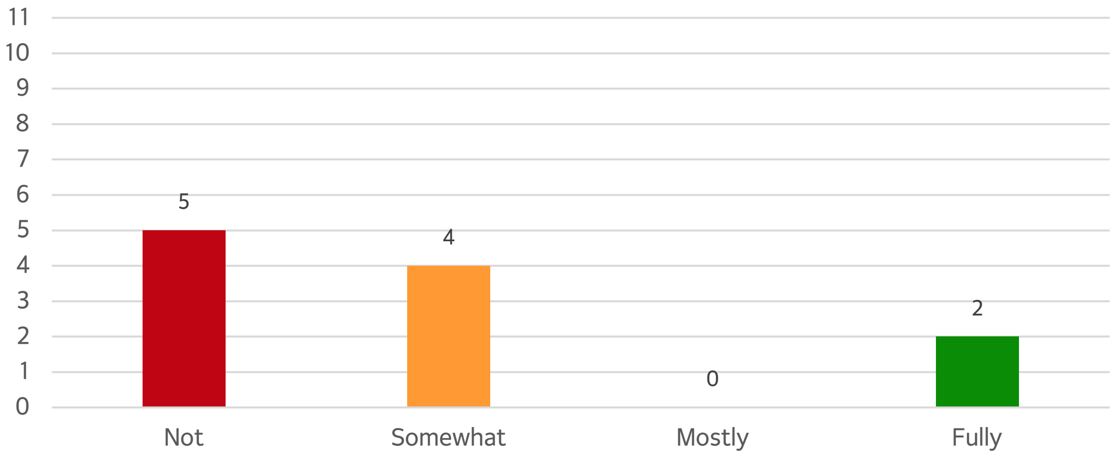
1. Establish and Maintain an Inventory of Service Providers
2. Establish and Maintain a Service Provider Management Policy
3. Classify Service Providers
4. Ensure Service Provider Contracts Include Security Requirements

WHY THIS MATTERS:

Most organizations rely on vendors or partners to provide services to help with data management, infrastructure, or other functions. Service providers present another avenue through which enterprise systems or data may be compromised. These impacts may be indirect, such as when an attack disables a partner from being able to provide services, or direct, such as when a compromised vendor has access to enterprise systems or data putting it at risk of loss or theft.

Similar to assets, agencies should maintain an inventory of service providers, and assess the risk associated with each provider, so the agency can make informed decisions about how to address those risks. Contract language should be in place to ensure responsibilities are clearly defined, so providers can be held accountable if an incident impacts the agency or its data.

CIS Control™ 16: Application Software Security



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

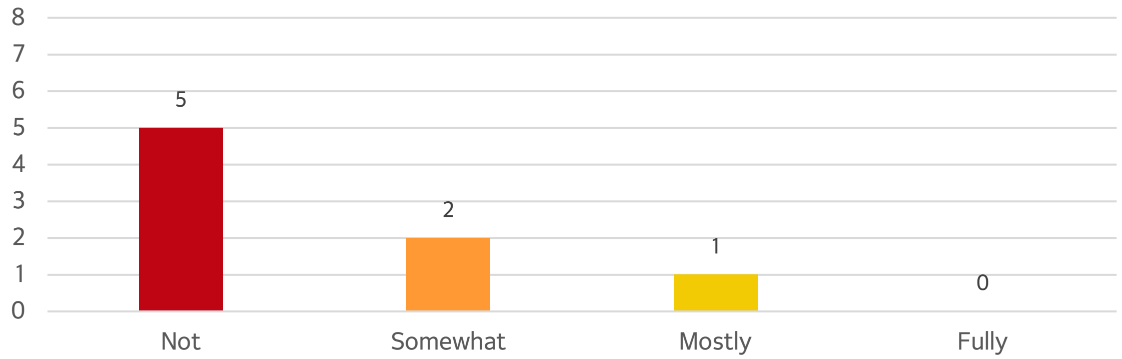
1. Establish and Maintain a Secure Application Development Process
2. Establish and Maintain a Process to Accept and Address Software Vulnerabilities
3. Perform Root Cause Analysis on Security Vulnerabilities
4. Establish and Manage an Inventory of Third-Party Software Components
5. Use Up-to-Date and Trusted Third-Party Software Components
6. Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities
7. Use Standard Hardening Configuration Templates for Application Infrastructure
8. Separate Production and Non-Production Systems
9. Train Developers in Application Security Concepts and Secure Coding
10. Apply Secure Design Principles in Application Architecture
11. Leverage Vetted Modules or Services for Application Security Components

WHY THIS MATTERS:

Application flaws provide attackers with a direct route to access sensitive data. These weaknesses can be present due to insecure application design, insecure infrastructure, coding mistakes, weak authentication, and failure to test for unexpected inputs. Vulnerabilities can provide a pathway for attackers to obtain data or credentials to gain access to an organization’s environment. Modern practices such as increasingly complex platforms, shorter development cycles, and assembly from various development frameworks and libraries make application security more challenging.

Agencies should have an application security program in place which includes vulnerability management processes, developer training in security concepts and secure coding, and minimizing the attack surface. These processes help ensure vulnerabilities are less prevalent and more likely to be addressed in a timely manner when they do occur.

CIS Control™ 17: Incident Response Management



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

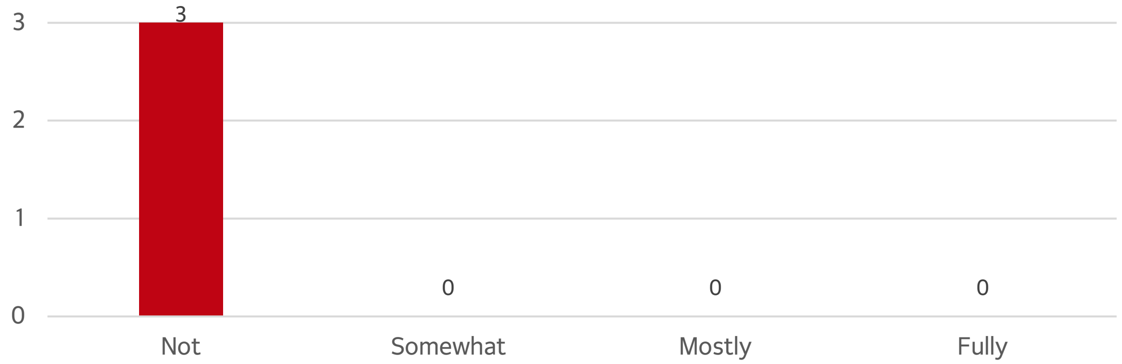
1. Designate Personnel to Manage Incident Handling
2. Establish and Maintain Contact Information for Reporting Security Incidents
3. Establish and Maintain an Enterprise Process for Reporting Incidents
4. Establish and Maintain an Incident Response Process
5. Assign Key Roles and Responsibilities
6. Define Mechanisms for Communicating During Incident Response
7. Conduct Routine Incident Response Exercises
8. Conduct Post-Incident Reviews

WHY THIS MATTERS:

Even appropriate protections will not be effective every time. When an attack occurs, a quick and successful response is essential. The longer it takes to detect and respond to an attack, the longer the attacker has to do more harm and develop ways to maintain persistent access. Without a well-documented response plan, responders may not know appropriate and effective procedures necessary to respond and recover from an incident.

All agencies should have a plan in place which outlines responsibilities, procedures, data collection, legal protocols, reporting, and communication strategies in the event of an incident. Once procedures are in place, the agency should periodically test the plan to ensure individuals understand their role and how to respond. There should also be processes to ensure post-incident reviews are conducted so agencies can benefit from lessons learned.

CIS Control™ 18: Penetration Testing



CIS Controls™ indicate organizations in IG2 should have the following safeguards in place:

1. Establish and Maintain a Penetration Testing Program
2. Perform Periodic External Penetration Tests
3. Remediate Penetration Test Findings

WHY THIS MATTERS:

An organization’s defense posture is rarely perfect. Attackers are constantly testing enterprise environments to identify and take advantage of security weaknesses.

Penetration testing allows an agency to understand what weaknesses exist, and how they might be exploited, so they can be remedied before an attack occurs. Penetration testing includes reconnaissance of an organization and its environment, identification of vulnerabilities, exploitation of those vulnerabilities to demonstrate how controls can be circumvented, and reporting on findings. Because of the risk involved with intentionally exploiting controls, penetration tests should be conducted by experienced people from reputable organizations.

Recommendations

To improve critical cybersecurity controls, we recommend DOC:

1. Remedy weaknesses with CIS Control #1 – Inventory and Control of Enterprise Assets – by implementing recommendations associated with separately communicated confidential findings.
2. Remedy weaknesses with CIS Control #2 – Inventory and Control of Software Assets – by implementing recommendations associated with separately communicated confidential findings.
3. Remedy weaknesses with CIS Control #3 – Data Protection – by implementing recommendations associated with separately communicated confidential findings.
4. Remedy weaknesses with CIS Control #4 – Secure Configuration of Enterprise Assets and Software – by implementing recommendations associated with separately communicated confidential findings.
5. Remedy weaknesses with CIS Control #5 – Account Management – by implementing recommendations associated with separately communicated confidential findings.
6. Remedy weaknesses with CIS Control #6 – Access Control Management – by implementing recommendations associated with separately communicated confidential findings.
7. Remedy weaknesses with CIS Control #7 – Continuous Vulnerability Management – by implementing recommendations associated with separately communicated confidential findings.
8. Remedy weaknesses with CIS Control #8 – Audit Log Management – by implementing recommendations associated with separately communicated confidential findings.
9. Remedy weaknesses with CIS Control #9 – Email and Web Browser Protections – by implementing recommendations associated with separately communicated confidential findings.
10. Remedy weaknesses with CIS Control #10 – Malware Defenses – by implementing recommendations associated with separately communicated confidential findings.
11. Remedy weaknesses with CIS Control #11 – Data Recovery – by implementing recommendations associated with separately communicated confidential findings.
12. Remedy weaknesses with CIS Control #13 – Network Monitoring and Defense – by implementing recommendations associated with separately communicated confidential findings.
13. Remedy weaknesses with CIS Control #14 – Security Awareness and Skills Training – by implementing recommendations associated with separately communicated confidential findings.
14. Remedy weaknesses with CIS Control #15 – Service Provider Management – by implementing recommendations associated with separately communicated confidential findings.
15. Remedy weaknesses with CIS Control #16 – Application Software Security – by implementing recommendations associated with separately communicated confidential findings.

16. Remedy weaknesses with CIS Control #17 – Incident Response Management – by implementing recommendations associated with separately communicated confidential findings.

17. Remedy weaknesses with CIS Control #18 – Penetration Testing – by implementing recommendations associated with separately communicated confidential findings.

Objective, Scope, and Methodology

Objective

Our audit objective was to determine the extent to which DOC has implemented controls from the Center for Internet Security's CIS Controls™, version 8.[9] 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.[10]

Scope

The scope of this work included a review of 18 CIS Controls™ applicable to IG2 that are in place at DOC from December 2021 through April 2022. Cybersecurity experts generally agree these controls should be implemented for cyber defense readiness by organizations with the risk profile and size as DOC.

We excluded safeguards 4.2 and 6.6, and control 12 from our audit scope.

Methodology

To assess whether management has established policies and implemented controls to stop potential cyberattacks we:

Reviewed:

- IT policies and procedures;
- External IT risk assessments;
- Hardware and software inventory lists;
- User account lists and forms;
- Vulnerability scan reports;
- Data backup records;
- Training records; and
- Third-party contracts.

Observed:

- Security configuration settings on workstations, servers, and mobile phones;
- Patch status on workstations, servers, and phones;
- Authentication settings;
- Vulnerability scan configurations;
- Logging configurations;
- Web filtering settings and email configuration;
- Application development tools and settings; and
- Security software installation on workstations and servers;

[9] Center for Internet Security Controls.

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

Interviewed:

- DOC Information Security Officer;
- DOC IT staff;
- DOC training staff;
- EIS security management; and
- EIS policy staff.

Where sampling was performed, tested items were chosen using a combination of random and judgmental selection. This method provided auditors with sufficient evidence to conclude as to whether information systems security controls are in place on all assets, including those managed differently from standard processes. Due to the use of judgmental selection, results cannot be extrapolated to the entire population.

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 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.[11]

- Control activities
    - We considered whether management has designed control activities to achieve objectives and respond to risk.
    - We considered whether management has designed the entity's information system and related control activities to achieve objectives and respond to risks.
    - We considered whether management has implemented control activities through policies.

Deficiencies with these internal controls were documented in the confidential appendix separately communicated to DOC and EIS.

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 DOC during the course of this audit.

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

Audit team
Teresa Furnish, CISA, Audit Manager
Jessica Ritter, CPA, CISA, Senior Auditor
Karin Bryant, CPA, Staff Auditor
Julie Moffenbier, MAcc, 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

Oregon Department of Corrections
Administrative Services Division
3601 State Street
Salem, OR 97301

June 23, 2022

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

Re: Department of Corrections Cybersecurity Controls Audit response

Dear Mr. Memmott,

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

The Department of Corrections (DOC) would like to thank the Secretary of State's Audits Division for the work performed over the past six months. Your team has been very professional and considerate of my staff time during this process. I am thankful for the hard work of your team in helping us to find areas of improvement in Cybersecurity.

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

RECOMMENDATION 1
Remedy weaknesses with CIS Control #1 – Inventory and Control of Enterprise Assets – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 30th, 2023	Larry Mack 503.334.6043

Narrative for Recommendation 1
The DOC will develop and implement a process for reviewing and reconciling inventory sources to ensure inventory records are complete. This process will also address concerns regarding detecting, alerting, and managing unauthorized devices.

RECOMMENDATION 2
Remedy weaknesses with CIS Control #2 – Inventory and Control of Software Assets – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 30th, 2023	Larry Mack 503.334.6043

Narrative for Recommendation 2
The DOC will develop and implement a process to ensure that the software inventory includes software installed on all agency assets. Periodic review will be implemented to maintain accurate "allowlisting" of software and libraries as well as detect unauthorized software.

RECOMMENDATION 3
Remedy weaknesses with CIS Control #3 – Data Protection – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Post 2023-25 legislative budget approval	Travis Graham 503.428.1940

Narrative for Recommendation 3
The DOC will develop and implement a Data Protection program that addresses the concerns listed in the confidential findings. This program will address concerns related to sensitivity, ownership, retention, and disposal of data.

RECOMMENDATION 4
Remedy weaknesses with CIS Control #4 – Secure Configuration of Enterprise Assets and Software – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Partially completed during audit. June 30th, 2023 for remaining activities	Rob Marquardt 971.600.7167

Narrative for Recommendation 4
Firewall concerns were addressed and resolved during the audit. The DOC will develop and implement further processes regarding secure configuration of enterprise assets and software.

RECOMMENDATION 5
Remedy weaknesses with CIS Control #5 – Account Management – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 30th, 2023	Laura Carney 541.697.0060

Narrative for Recommendation 5
The DOC will develop and implement a documented account management process that addresses account validation at least quarterly and enforces the centralization and control of accounts and privileges.

RECOMMENDATION 6
Remedy weaknesses with CIS Control #6 – Access Control Management – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 30th, 2023	Travis Graham 503.428.1940

Narrative for Recommendation 6
The DOC will continue its current efforts regarding implementing MFA throughout the agency and centrally managing access control.

RECOMMENDATION 7
Remedy weaknesses with CIS Control #7 – Continuous Vulnerability Management – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 30th, 2023	Rob Marquardt 971.600.7167

Narrative for Recommendation 7
The DOC will further develop its Vulnerability Management program to remediate the concerns noted by Secretary of State, including automated patch management applications.

RECOMMENDATION 8
Remedy weaknesses with CIS Control #8 – Audit Log Management – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Post 2023-25 legislative budget approval	Rob Marquardt 971.600.7167

Narrative for Recommendation 8
The DOC is currently testing audit log collection and in the process of procuring an Audit Log Management product. Development and implementation of such Audit Log Management product will require funding from the 23-25 legislative budget.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 9</b>
Remedy weaknesses with CIS Control #9 – Email and Web Browser Protections – by implementing recommendations associated with separately communicated confidential findings.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>June 30th, 2023</td><td>Travis Graham
503.428.1940</td></tr>
</table>

Narrative for Recommendation 9
The DOC will develop and implement a documented process to implement DMARC across all DOC-managed domains and enforce access to only supported browsers and clients.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 10</b>
Remedy weaknesses with CIS Control #10 – Malware Defenses – by implementing recommendations associated with separately communicated confidential findings.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>June 30th, 2023</td><td>Larry Mack
503.334.6043</td></tr>
</table>

Narrative for Recommendation 10
The DOC will continue its efforts in defending against malware by developing and implementing a process for the use of behavior-based anti-malware software, enabling anti-exploitation features, and enforcing more stringent security regarding removable media.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 11</b>
Remedy weaknesses with CIS Control #11 – Data Recovery – by implementing recommendations associated with separately communicated confidential findings.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>June 30th, 2023</td><td>Travis Graham
503.428.1940</td></tr>
</table>

Narrative for Recommendation 11
The DOC will enhance and document its data recovery process to encompasses all DOC assets, define requirements, and routinely test backups.

RECOMMENDATION 12
Remedy weaknesses with CIS Control #13 – Network Monitoring and Defense – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Post 2023-25 legislative budget approval	Rob Marquardt 971.600.7167

Narrative for Recommendation 12
The DOC is actively pursuing remediation efforts related to logging and event collection. An IDS system is planned, but as with Recommendation 8, any procurement progress will be dependent on the 23-25 legislative budget.

RECOMMENDATION 13
Remedy weaknesses with CIS Control #14 – Security Awareness and Skills Training – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 30th, 2023	Rob Marquardt 971.600.7167

Narrative for Recommendation 13
In addition to the Security Awareness training currently provided by Enterprise Information Services (EIS), the DOC will develop and implement its own Security Awareness and Skill Training program to address more advanced topics such as role-specific awareness, incident handling, etc.

RECOMMENDATION 14
Remedy weaknesses with CIS Control #15 – Service Provider Management – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 30th, 2023	Parm Kaur 503.798.5328

Narrative for Recommendation 14
The DOC will develop and implement a service provider management process that address classification, inventory, assessment, monitoring, and decommissioning of service providers.

RECOMMENDATION 15
Remedy weaknesses with CIS Control #16 – Application Software Security – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Post 2023-25 legislative budget approval	Jason Miranda 503.910.9478

Narrative for Recommendation 15
The DOC will develop and implement a documented secure application development process that addresses software vulnerabilities, root cause analysis, third-party component management and developer training among other topics. Training of developers in Application Security concepts and secure coding is the core of this effort, however progress in this endeavor will be entirely dependent on the 21-23 legislative budget.

RECOMMENDATION 16
Remedy weaknesses with CIS Control #17 – Incident Response Management – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 30th, 2023	Rob Marquardt 971.600.7167

Narrative for Recommendation 16
The DOC will continue to improve upon its Incident Response Management by developing and implementing a documented process that creates a well-defined structure for responding to incidents including contacts, reporting processes, roles and responsibilities, incident communications and post-incident review.

RECOMMENDATION 17
Remedy weaknesses with CIS Control #18 – Penetration Testing – by implementing recommendations associated with separately communicated confidential findings.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Contingent on Cyber Security Services (CSS) offerings	Rob Marquardt 971.600.7167

Narrative for Recommendation 17
The DOC will work in conjunction with CSS to determine what, if any, offerings are available State-wide in this area.

Please contact Donald Pack, Chief Information Officer at 503.302.3317 with any questions.

Sincerely,

Donald A. Pack

Donald A. Pack
Chief Information Officer

cc: Jim Paul, ODOC Assistant Director, Administrative Services Division
Eli Ritchie, ODOC Internal Audits Administrator

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 180
Salem OR 97310

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