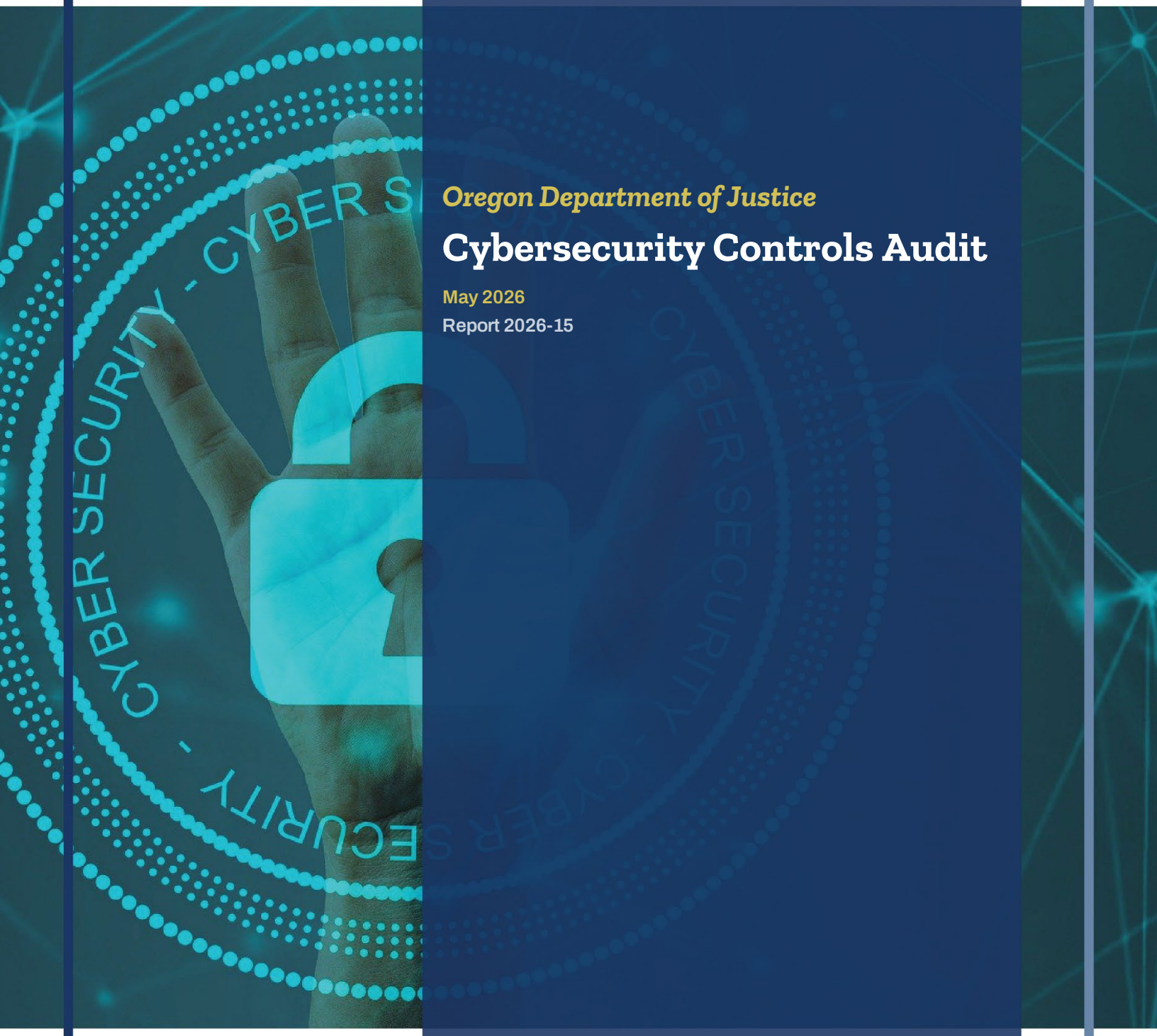


Oregon Department of Justice

Cybersecurity Controls Audit

May 2026

Report 2026-15

Oregon
Secretary *of* **State**

Oregon Secretary of State

Secretary of State **Tobias Read**
Audits Director **Steve Bergmann**

Audit Summary

Oregon Department of Justice

Cybersecurity Controls Audit

OBJECTIVE

Our audit objective was to determine the extent to which the Oregon Department of Justice (DOJ) has implemented controls from the Center for Internet Security's CIS Controls®, version 8.1. 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.

SCOPE

The scope of this work included a review of all 18 CIS Controls® in Implementation Groups 1, 2, and 3. Within each of the 18 CIS Controls® are associated "safeguards," or specific individual defensive actions against potential cyberattacks. For security purposes, the results for the specific safeguards have been communicated directly to the agency in a confidential appendix.

Why this audit is important

Effective cybersecurity, including strong data security and system resilience, is essential for the Oregon Department of Justice to protect sensitive legal, investigative, and personally identifiable information entrusted to it by Oregonians and partner agencies.

As the state's chief legal office, DOJ must maintain cyber defense readiness consistent with organizations of similar size, complexity, and risk profile to ensure continuity of critical legal services.

Without robust cybersecurity controls, DOJ risks operational disruption, compromised prosecutions and civil actions, financial loss, and erosion of public trust in its ability to uphold the rule of law.

What we found

Cybersecurity controls were largely implemented, with some areas that could be improved (pg. 5)

We found all 18 of the CIS Controls® were partially implemented. The controls are further split into 153 safeguards for Implementation Groups 1, 2, and 3. Of these safeguards, we found 64 were fully implemented, 61 were mostly implemented, 19 were somewhat implemented, and 9 were not implemented according to criteria.

Security policies and procedures specific to CIS Controls® should be updated annually (pg. 6)

A common theme we identified during the audit was that while DOJ had policies, procedures, standards, and formal documentation for information security processes, the documents were largely one year or more out of date. Several CIS safeguards recommend annual review of documentation. In practice, if no changes are deemed necessary after review, agencies can update the revised date to the date of review and include appropriate signatures signaling periodic and formal review.

What we recommend

To improve critical cybersecurity controls, we recommend DOJ management:

1. Implement recommendations associated with separately communicated confidential findings in Appendix B.

To improve overall documentation, we recommend DOJ management:

2. Schedule annual reviews of documentation relevant to the CIS safeguards and update the effective date and signatures as necessary.

In accordance with ORS 297.070(10), the Audits Division will follow up on DOJ's progress toward implementing our recommendations. This follow-up will address both the public and confidential findings and recommendations and will assess whether the agency has taken appropriate action to resolve them.

Agency response

We made two recommendations to DOJ in this public report and 76 recommendations in confidential Appendix B. DOJ agreed with all of our recommendations. The agency's public response can be found at the end of the report.

Read the full audit report

Scan the QR code to read the full audit report, including the agency response, on our website.

Oregon Secretary of State

Introduction

Cyberattacks are an ongoing concern for Oregon state government. Past breaches at state agencies underscore the importance of having robust cybersecurity controls to protect Oregonians' data and ensure agencies can continue to operate in service to Oregonians.

The Center for Internet Security® (CIS) has identified 18 controls as a simplified set of best practices to help organizations strengthen their cybersecurity posture.[1] Within each of the 18 CIS Controls® are associated "safeguards," or specific individual defensive actions against potential cyberattacks. The safeguards are divided into three Implementation Groups (IGs) based on the size and risk profile of the organization:

- IG1 enterprises are small to medium-sized with limited IT and cybersecurity expertise. These organizations are primarily concerned with keeping their business operational; the sensitivity of their data is low.
- IG2 enterprises have 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 has 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 cause significant harm to public welfare.

This audit includes cybersecurity controls applicable to IG3 organizations.

Each safeguard must be in place before a control is considered fully implemented. This means an agency can have all but one safeguard fully implemented, but the control would only be considered partially implemented.

This audit does not consider an agency's risk appetite. While these controls are considered best practice by many security experts, control implementation can vary for many reasons, including agency resource allocation strategy, budgetary spending limitations, and prioritization of information security within the agency, and ultimately, within the State of Oregon. While we generally considered mitigating controls, we did not perform a detailed review of potential compensating controls for each safeguard.

This public report omits most details in the interest of security. A breakdown of each control's safeguards and the importance of each control to an organization's cybersecurity posture, which we used as criteria, is included in Appendix A. Full details, including recommendations on how to address identified gaps, have been communicated to the agency in confidential Appendix B.

The Oregon Department of Justice has a centralized structure for its IT services which support all offices in the State of Oregon

DOJ is responsible for all court actions and legal proceedings in which the state of Oregon is a party or has an interest, including all civil and criminal cases before state and federal courts. DOJ exercises virtually complete authority over all legal business for approximately 100 state agencies, boards, and commissions.

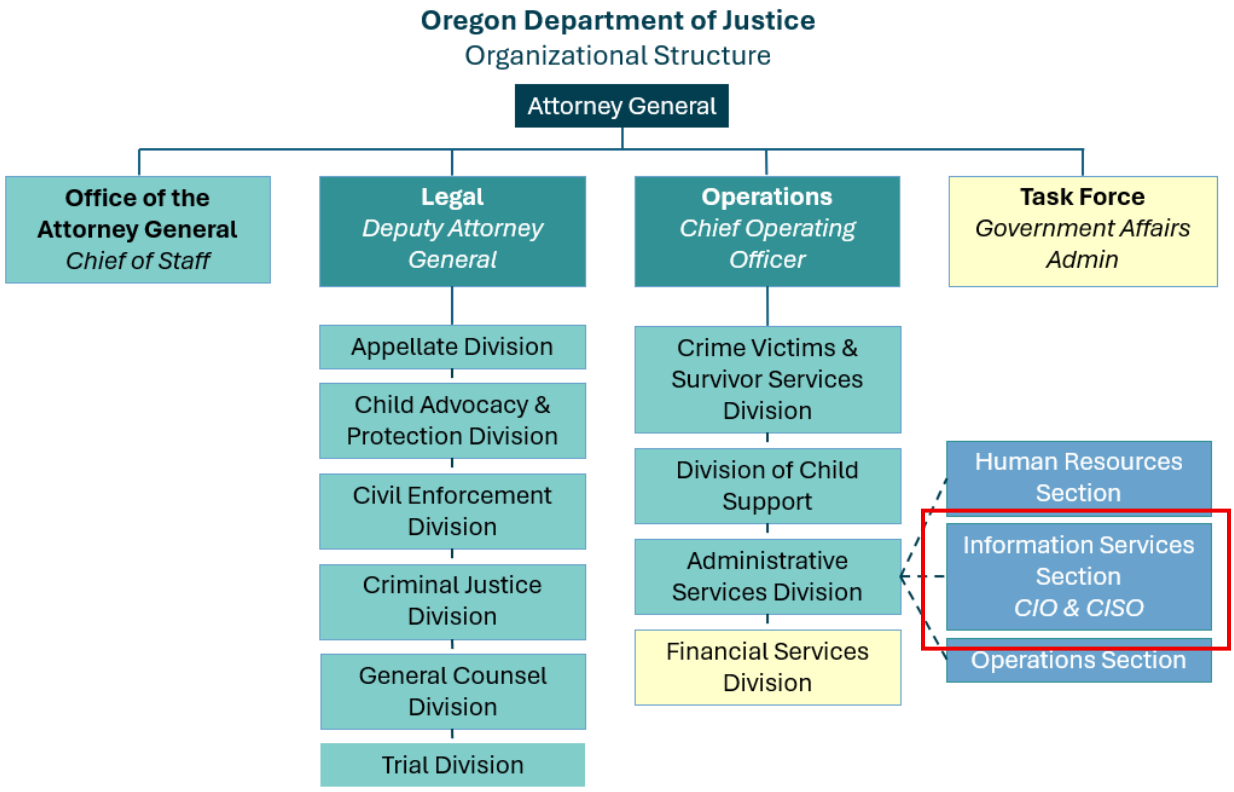
[1] CIS Critical Security Controls

The mission of the DOJ is to serve state government and to support safe and healthy communities throughout Oregon by providing essential justice services, including serving the most vulnerable. DOJ is overseen by the Attorney General, a statewide elected official whose authority is established in statute rather than the constitution. The Attorney General is the chief legal officer of the state, with a term of office of four years.

For the 2025-27 biennium, the legislatively adopted budget for DOJ consisted of $966.8 million and 1,604 (1,588.84 Full-Time Equivalent) positions.

DOJ is organized into the following divisions or program areas: Office of the Attorney General, Administrative Services, Appellate, Civil Enforcement, Criminal Justice, Crime Victims and Survivor Services, General Counsel, Trial, Child Advocacy and Protection, and Child Support.

Figure 1: Organizational structure of the Oregon Department of Justice



The Administrative Services Division includes the Information Services Section that oversees the agency's IT security functions

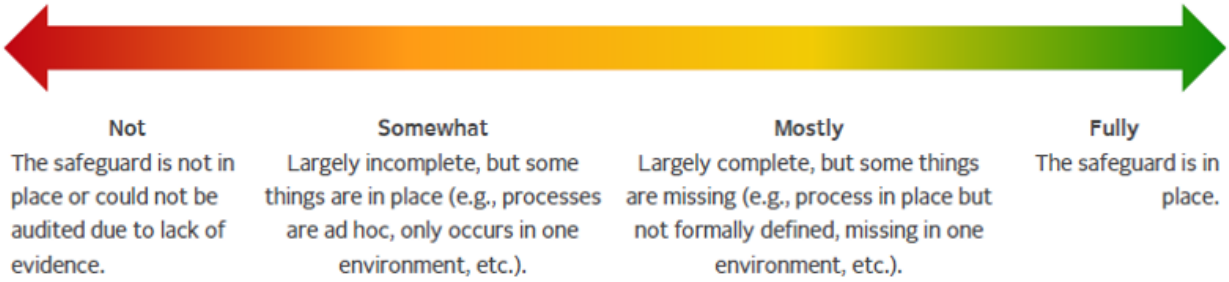
Although DOJ operates within the executive branch, it functions independently from the Governor. Senate Bill 90 from the 2017 regular legislative session unified IT security functions for most state agencies by consolidating security functions and staffing into Enterprise Information Services (EIS) under the Department of Administrative Services. However, DOJ is not subject to the requirements of Senate Bill 90. Instead, the department's Information Services department headquartered in Salem, Oregon performs IT and security services for 10 legal and 13 child support offices throughout the state.

The mission of Information Services is to deliver secure, integrated information technology solutions and services that advance the mission and goals of the Oregon Department of Justice. Information Services uses a defense in depth approach to their security architecture. They accomplish this by implementing network security, application security, security assessments, maintaining system and data security, endpoint security, identity and access management, and privacy controls. This audit evaluated the security functions performed by DOJ's Information Services.

CIS Controls Review

For this audit, we evaluated the implementation level of the agency's cybersecurity control environment against the CIS Controls® and the associated safeguards enumerated under IG3. The implementation status levels include: not implemented (red), somewhat implemented (orange), mostly implemented (yellow), or fully implemented (green).

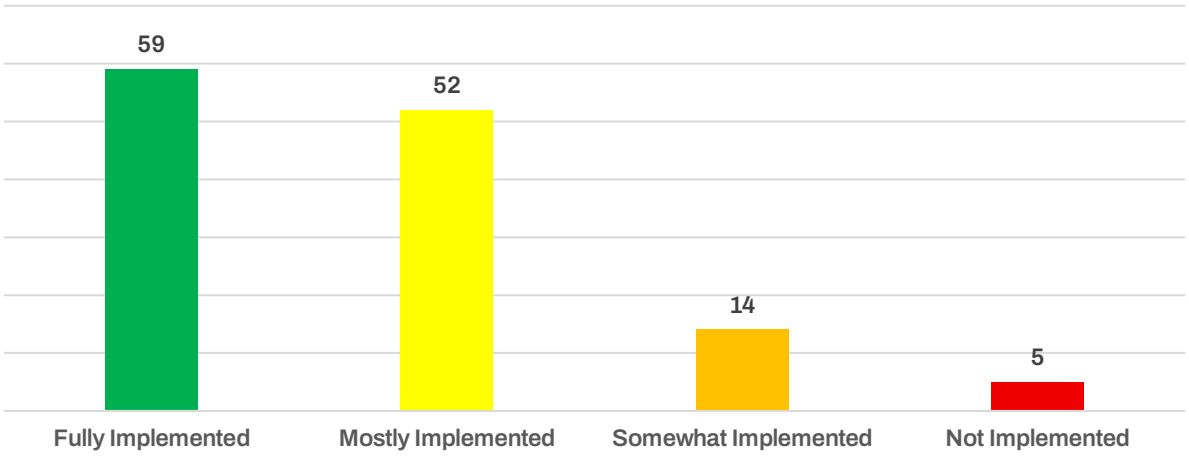
Figure 2: Implementation status categories



We evaluated each safeguard to provide an assessment of the agency's overall cybersecurity implementation. A control is only considered fully implemented if all associated safeguards are also fully implemented. That is to say, an agency can fully implement all but one safeguard under a CIS control, but the control itself would only be considered partially implemented.

For reference, we have defined each safeguard and described why each control group is important based on narrative in the CIS Controls® documentation in Appendix A. See the Objectives, Scope, and Methodology section of this report for an overview of how auditors determined the implementation status category of each safeguard.

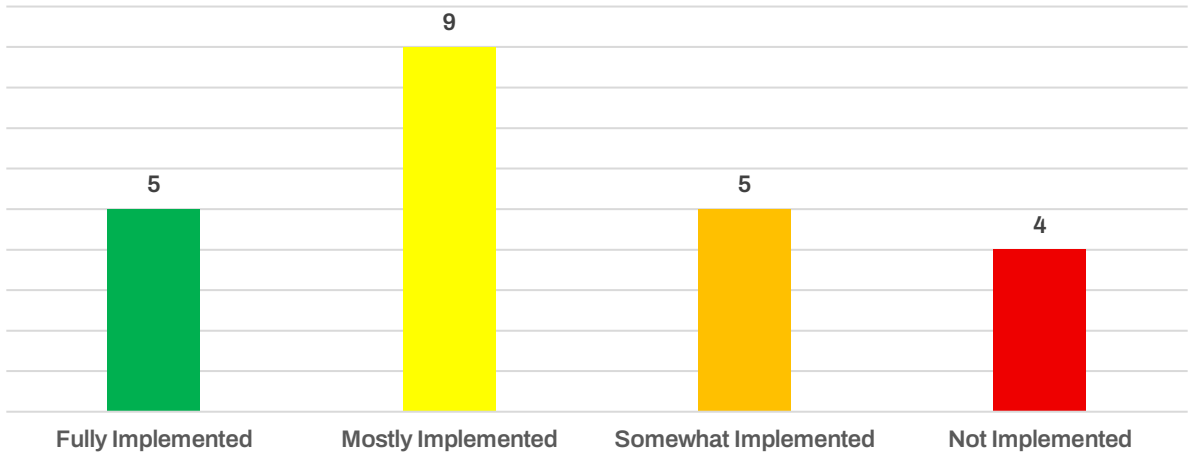
Figure 3: Summary of implementation levels for IG1 and IG2 safeguards



Of the 130 IG1 and IG2 safeguards assessed, 59 were fully implemented, 52 were mostly implemented, 14 were somewhat implemented, and five were not implemented. Of the 18 controls assessed at IG1 and IG2,

two were found to be fully implemented. We separated the IG1 and IG2 summary from the IG3 summary to allow for comparisons to other cybersecurity audits where we only assessed IG1 and IG2.

Figure 4: Summary of implementation levels for IG3 only safeguards



Of the 23 IG3 safeguards assessed, five were fully implemented, nine were mostly implemented, five were somewhat implemented, and four were not implemented.

Of the 18 controls assessed at IG1, IG2, and IG3, zero were found to be fully implemented and 18 were found to be partially implemented. Partial implementation could occur whether one or all safeguards were assessed at any level other than fully implemented.

Formal documentation, while thorough, was largely out of date

CIS Controls® require organizations to formally document their plans, policies, processes, procedures, and other written materials that support the implementation of safeguards. These documents should be reviewed at least annually, or when significant changes occur that could affect a given safeguard.

A common theme we identified during the audit was that while DOJ had comprehensive policies, procedures, standards, and formal documentation for information security processes, the documents were largely one year or more out of date.

Without an updated and formally approved set of documented plans, policies, processes, and other written materials governing information security, agencies can face confusion and challenges when changes and security incidents occur.

Recommendations

To improve critical cybersecurity controls, we recommend DOJ management:

1. **Implement recommendations associated with separately communicated confidential findings in Appendix B.**

To improve overall documentation, we recommend DOJ management:

2. **Schedule annual reviews of documentation relevant to the CIS safeguards and update the effective date and signatures as necessary.**

In accordance with ORS 297.070(10), the Audits Division will follow up on DOJ's progress toward implementing our recommendations. This follow-up will address both the public and confidential findings and recommendations and will assess whether the agency has taken appropriate action to resolve them.

Objective, Scope, and Methodology

OBJECTIVE

Our audit objective was to determine the extent to which DOJ has implemented controls from the Center for Internet Security's CIS Controls®, version 8.1. 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.

SCOPE

The scope of this work included a review of all 18 CIS Controls® applicable to Implementation Groups 1, 2, and 3 that were in place at DOJ from October 2024 to February 2026. Cybersecurity experts generally agree these controls should be implemented for cyber defense readiness by organizations with the risk profile and size as DOJ.

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;
- Penetration testing 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;

Interviewed:

- DOJ CIO and CISO; and
- DOJ IT managers and staff.

For all DOJ data provided, we assessed the reliability of data by performing electronic testing, reviewing existing information about the data and the system that produced them, and interviewing agency officials knowledgeable about the data. We determined that the data was sufficiently reliable for the purposes of this report. Where sampling was performed, tested items were judgmentally selected. This method provided auditors with sufficient evidence to reasonably conclude as to whether the information systems security controls were 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 of 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 with a confidential appendix with additional detail and context.

INTERNAL CONTROL REVIEW

We determined that the following internal controls were relevant to our audit objective.[2]

- 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 DOJ and in the summarized results in this report.

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 DOJ during the course of this audit.

Audit team

Erika Ungern, CISSP, CISA, Audit Manager
Courtney Hilton, Principal Auditor
Jeff Watson, CISA, Senior Auditor

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

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 Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The Secretary of State has constitutional authority to audit all state officers, agencies, boards, and commissions.

Appendix A: CIS Controls®

CIS Control® 1: Inventory and Control of Enterprise Assets

CIS Controls® indicate organizations in IG 1, 2 & 3 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
4. Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory
5. Use a Passive Asset Discovery Tool

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 IG 1, 2 & 3 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
7. Allowlist Authorized Scripts

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 IG 1, 2 & 3 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
13. Deploy a Data Loss Prevention Solution
14. Log Sensitive Data Access

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 IG 1, 2 & 3 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
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
12. Separate Enterprise Workspaces on Mobile End-User Devices

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.

CIS Control® 5: Account Management

CIS Controls® indicate organizations in IG 1, 2 & 3 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

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 IG 1, 2 & 3 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
4. Require MFA for Remote Network Access
5. Require MFA for Administrative Access
6. Establish and Maintain an Inventory of Authentication and Authorization Systems
7. Centralize Access Control
8. Define and Maintain Role-Based Access Control

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 Multifactor Authentication (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 IG 1, 2 & 3 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

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 with 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 IG 1, 2 & 3 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
12. Collect Service Provider Logs

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. 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.

CIS Control® 9: Email and Web Browser Protections

CIS Controls® indicate organizations in IG 1, 2 & 3 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
6. Block Unnecessary File Types
7. Deploy and Maintain Email Server Anti-Malware Protections

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 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.

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 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 IG 1, 2 & 3 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

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 IG 1, 2 & 3 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

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

CIS Controls® indicate organizations in IG 1, 2 & 3 should have the following safeguards in place:

1. Ensure Network Infrastructure is Up-to-Date
2. Establish and Maintain a Secure Network Architecture
3. Securely Manage Network Infrastructure
4. Establish and Maintain Architecture Diagram(s)
5. Centralize Network Authentication, Authorization, and Auditing (AAA)
6. Use of Secure Network Management and Communication Protocols
7. Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure
8. Establish and Maintain Dedicated Computing Resources for All Administrative Work

A secure network infrastructure is vital for protecting against cyberattacks. This involves implementing a strong security architecture, addressing vulnerabilities, and continuously monitoring and reassessing configurations. Network infrastructure includes critical devices like gateways, firewalls, wireless access points, routers, and switches, both physical and virtual. These devices, when left with default configurations, may contain open ports, default passwords, or outdated protocols, all of which attackers exploit to breach systems, reroute traffic, or intercept data.

As network environments evolve constantly, regular reviews of network architecture, access controls, and traffic flows are essential. Over time, device configurations can become less secure due to user demands for exceptions. If these exceptions aren't removed or re-evaluated once they're no longer necessary, they can introduce unassessed security risks. Attackers often take advantage of these overlooked changes to infiltrate networks.

CIS Control® 13: Network Monitoring and Defense

CIS Controls® indicate organizations in IG 1, 2 & 3 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
7. Deploy a Host-Based Intrusion Prevention Solution
8. Deploy a Network Intrusion Prevention Solution
9. Deploy Port-Level Access Control
10. Perform Application Layer Filtering
11. Tune Security Event Alerting Thresholds

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 IG 1, 2 & 3 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

Most security professionals agree, any organization's weakest link are its end-users. 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 IG 1, 2 & 3 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
5. Assess Service Providers
6. Monitor Service Providers
7. Securely Decommission Service Providers

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 IG 1, 2 & 3 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
12. Implement Code-Level Security Checks
13. Conduct Application Penetration Testing
14. Conduct Threat Modeling

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, training software developers 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 IG 1, 2 & 3 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
9. Establish and Maintain Security Incident Thresholds

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 IG 1, 2 & 3 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
4. Validate Security Measure
5. Perform Periodic Internal Penetration Tests

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.

Appendix B: Confidential CIS Control® Status

This appendix is confidential and was separately shared with DOJ.

DAN RAYFIELD
Attorney General

BENJAMIN GUTMAN
Deputy Attorney General

DEPARTMENT OF JUSTICE

May 1, 2026

Steve Bergmann, Director
Secretary of State, Audits Division
255 Capitol St. NE, Suite 180
Salem, OR 97310

Dear Mr. Bergmann,

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

The Oregon Department of Justice (DOJ) appreciates the Secretary of State's Audits Division for their thorough and detailed efforts throughout this audit. The audit team was knowledgeable, professional, and responsive to our questions throughout the entire process and we understand how much time and effort went into performing this audit.

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

RECOMMENDATION 1 To improve critical cybersecurity controls, we recommend DOJ management implement recommendations associated with separately communicated confidential findings in Appendix B.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	36 months	Richard Rylander, 971-209-8632

Narrative for Recommendation 1

DOJ responded to all confidential recommendations and identified actions steps and timelines if applicable.

RECOMMENDATION 2 To improve overall documentation, we recommend DOJ management schedule annual reviews of documentation relevant to the CIS safeguards and update the effective date and signatures as necessary.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	18 months	Richard Rylander, 971-209-8632

Narrative for Recommendation 2
Policies are in the process of being updated. A process to review policies annually will be completed within 18 months.

Please contact Richard Rylander at 971-209-8632 with any questions.

Sincerely,

Benjamin Gutman
Deputy Attorney General

Oregon
Secretary *of* **State**

Secretary of State **Tobias Read**
Audits Director **Steve Bergmann**

Oregon Audits Division
255 Capitol St NE, Suite 180
Salem OR 97310
(503) 986-2255

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