Fundamental Deficiencies in OS' Cybersecurity Incident Response Program Increase the Risk of Cyberattacks

FINAL REPORT NO. OIG-23-017-I

MARCH 22, 2023

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

March 22, 2023

MEMORANDUM FOR: Don Graves
Deputy Secretary of Commerce

FROM: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *Fundamental Deficiencies in OS' Cybersecurity Incident Response Program Increase the Risk of Cyberattacks*
Final Report No. OIG-23-017-I

Attached for your review is our final report on our evaluation of the Office of the Secretary's (OS') incident response program. The objective of our evaluation was to assess the adequacy of actions taken by the U.S. Department of Commerce (the Department) and its bureaus when detecting and responding to cyber incidents in accordance with federal and Departmental requirements. To address this objective, we utilized open-source security tools to emulate the most current malicious activities performed by relevant threat actors.

Overall, we identified fundamental deficiencies in OS' cybersecurity incident response program that increased the risk of successful cyberattacks. Specifically, we found the following:

I. OS Security Operations Center's (OS SOC)'s security tools were not properly configured to detect incidents.

II. OS SOC did not effectively handle a simulated incident.

III. OS' Office of the Chief Information Officer did not manage its incident detection and response program in accordance with federal requirements.

On February 17, 2023, we received the Department's response to our draft report. In response to our draft report, the Department concurred with all our recommendations and described actions it has taken, or will take, to address them. The Department's formal response is included within the final report as appendix B.

Prior to receiving the Department's response, we met with Department officials to discuss their concerns regarding the public release of the report. Following the discussions, we made minor changes to the report.

Pursuant to Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendations in this report within 60 calendar days. This final report will be posted on the Office of Inspector General's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (recodified at 5 U.S.C. §§ 404 & 420).

We appreciate the cooperation and courtesies extended to us by your staff during our evaluation. If you have any questions or concerns about this report, please contact me at (202) 793-2938 or Dr. Ping Sun, Director for IT Security, at (202) 793-2957.

Attachment

cc: André Mendes, Chief Information Officer
Ryan Higgins, Chief Information Security Officer
MaryAnn Mausser, Audit Liaison, Office of the Secretary
Joselyn Bingham, Audit Liaison, OCIO
Maria Hishikawa, IT Audit Liaison, OCIO
Rehana Mwalimu, Risk Management Officer and Primary Alternate Department GAO/OIG Liaison, Office of the Secretary

Report in Brief

March 22, 2023

Background

The U.S. Department of Commerce (the Department) and its bureaus are required to follow federal laws to secure information technology (IT) systems through the cost-effective use of managerial, operational, and technical controls. This responsibility applies to all IT systems, including those from the Office of the Secretary (OS), which serves as the general management arm of the Department and provides principal support to the Secretary in formulating policy and providing advice to the President. The Office of the Chief Information Officer (OCIO) is responsible for managing OS' information systems and applications.

At the Department, OS and many other bureaus operate independent Security Operations Centers (SOCs), which are responsible for detecting and responding to cybersecurity incidents. OS' SOC (OS SOC) within OCIO manages day-to-day IT security operations. Additionally, the Department has established a separate Enterprise SOC (ESOC) that manages the Department's network perimeter, compiles data from bureau SOCs, and serves as a liaison to government cybersecurity partners such as the Cybersecurity & Infrastructure Security Agency.

Why We Did This Review

Our evaluation objective was to assess the adequacy of actions taken by the Department and its bureaus when detecting and responding to cyber incidents in accordance with federal and Departmental requirements.

OFFICE OF THE SECRETARY

Fundamental Deficiencies in OS' Cybersecurity Incident Response Program Increase the Risk of Cyberattacks

OIG-23-017-I

WE FOUND the following:

I. OS SOC's security tools were not properly configured to detect incidents.

II. OS SOC did not effectively handle a simulated incident.

III. OS OCIO did not manage its incident detection and response program in accordance with federal requirements.

WE RECOMMENDED that the Deputy Secretary of Commerce direct the Department's Chief Information Officer to do the following:

1. Perform a review of all software tools used within OS to ensure that default passwords are not used.
2. Ensure that OS OCIO holds its contractors accountable for implementing Department policy on default passwords.
3. Establish a process to regularly review OS SOC tools and ensure they are configured correctly and operating as intended.
4. Review and revise OS OCIO firewall configurations and rulesets to ensure that they are providing adequate protection to OS systems.
5. Establish processes and procedures to periodically review OS OCIO firewall configurations and rulesets.
6. Obtain the capability for OS OCIO to automatically aggregate security events and data using a tool such as Security Information and Event Management.
7. Review OS's Data Loss Prevention practices, including but not limited to updating the configurations of Data Loss Prevention products and ensuring that incidents are reported to OS SOC and ESOC in a timely manner.
8. Update the existing service-level agreement to define clear responsibilities between ESOC and OS for the incident handling process.
9. Update OS OCIO's cybersecurity incident response plan to include procedures for carrying out digital forensics.
10. Increase communication between the OS SOC and ESOC by allowing reciprocal access to ticketing systems or creating a common system.
11. Establish a timeline to ensure that the systems responsible for endpoint protection are properly authorized.
12. Establish a procedure to ensure sufficient government oversight is provided to contractors who are responsible for OS endpoint protection.
13. Establish tracking and reporting processes to ensure OS OCIO cybersecurity policies and procedures are developed, up to date, and in compliance with federal requirements.
14. Identify which improvement opportunities within the OS OCIO remediation plan should be prioritized to enhance OS' incident detection and response.

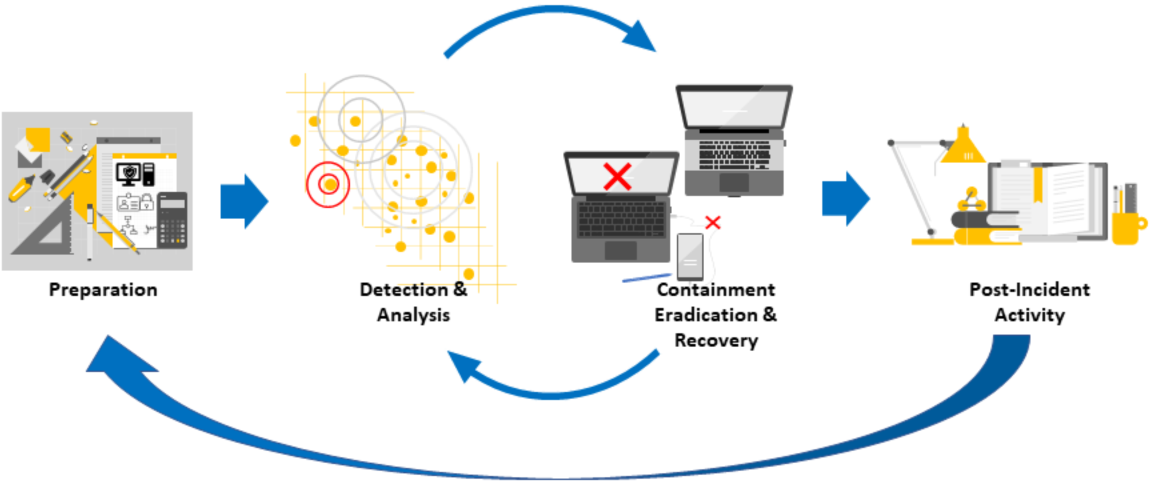
Contents

Cover: Herbert C. Hoover Building main entrance at 14th Street Northwest in Washington, DC. Completed in 1932, the building is named after the former Secretary of Commerce and 31st President of the United States.

Introduction

Cyberattacks[1] frequently compromise personal and business data, and it is critical that organizations respond quickly and effectively when breaches occur. The benefits of having a cyber incident response capability include responding to incidents systematically, helping personnel minimize the loss or theft of information, and reducing service disruptions caused by incidents. Further, an effective incident response program allows an organization to learn from incident handling and prepare for future incidents. Figure 1 illustrates the phases of incident response as defined by the National Institute for Standards and Technology (NIST).

Figure 1. Incident Response Life Cycle



Source: Office of Inspector General (OIG) (derived from NIST)

The U.S. Department of Commerce (the Department) and its bureaus are required to follow federal laws to secure information technology (IT) systems[2] through the cost-effective use of managerial, operational, and technical controls. This responsibility applies to all IT systems, including those from the Office of the Secretary (OS). OS serves as the general management arm of the Department and provides principal support to the Secretary in formulating policy and providing advice to the President. The Office of the Chief Information Officer (OCIO) is responsible for managing OS' information systems and applications.

At the Department, OS and many other bureaus operate independent Security Operations Centers (SOCs), which are responsible for detecting and responding to cybersecurity incidents. OS' SOC (OS SOC) within OCIO manages day-to-day IT security operations. Additionally, the Department has established a separate Enterprise SOC (ESOC) that manages the Department's

[1] Cyberattacks relate to both successful and unsuccessful attempts to leverage and exploit vulnerabilities to compromise computers by malicious threat actors, which may result in negative impact to confidentiality, integrity, or availability.

[2] *See* Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551, *et seq.*

network perimeter, compiles data from bureau SOCs, and serves as a liaison to government cybersecurity partners such as the Cybersecurity & Infrastructure Security Agency (CISA).

Objective, Findings, and Recommendations

The objective of our evaluation was to assess the adequacy of actions taken by the Department and its bureaus when detecting and responding to cyber incidents in accordance with federal and Departmental requirements. The evaluation focused on OS' network, which is monitored by both OS SOC and ESOC. See appendix A for a full description of our scope and methodology.

To evaluate actions taken by both security centers, we utilized MITRE's Caldera[3] security tool and the Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)[4] framework to emulate the most current malicious activities performed by relevant Advanced Persistent Threat (APT)[5] groups. The activities we emulated included the exfiltration of fictitious personally identifiable information (PII), establishing persistent access on endpoints,[6] modifying endpoint protection configurations, and collecting network and system data.

We identified fundamental deficiencies in OS' cybersecurity incident response program that increased the risk of cyberattacks. Specifically, we found that OS SOC had not properly configured its security tools to detect our simulated attacks. Once ESOC independently discovered the attacks, OS SOC struggled to effectively respond to the incident. We also found that OS OCIO did not manage its incident detection and response program in accordance with federal requirements.

While OS OCIO had begun to identify its weaknesses, it had yet to prioritize efforts to improve incident detection and response. As such, OS was unprepared for an actual cybersecurity incident—undermining its ability to protect the Department's mission-critical systems, data, and operations.

I. OS SOC's Security Tools Were Not Properly Configured to Detect Incidents

Before an organization can respond to a cybersecurity incident, it must have an effective method to detect it. OS SOC utilized a combination of hardware and software tools, including an endpoint protection tool, which can provide malware detection and prevention. However, we found during our testing that these tools were misconfigured and ineffective.

[3] Caldera is a cybersecurity software tool built by The MITRE Corporation to easily automate adversary emulation, assist manual red teams, and automate incident response.

[4]The ATT&CK Framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations developed by The MITRE Corporation.

[5] An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and deception. *See* U.S. Department of Commerce National Institute for Standards and Technology Computer Security Resource Center. *Advanced persistent threat (definition)* [online]. https://csrc.nist.gov/glossary/term/advanced_persistent_threat (accessed October 26, 2022).

[6] Endpoints are remote devices connected to a network, such as laptops, servers, routers, switches, and mobile devices.

Specifically, OS' endpoint protection was easy to disable, the endpoint protection tool did not effectively block malware, and OS SOC did not detect most of our simulated attacks.

A. OS' endpoint protection was easy to disable

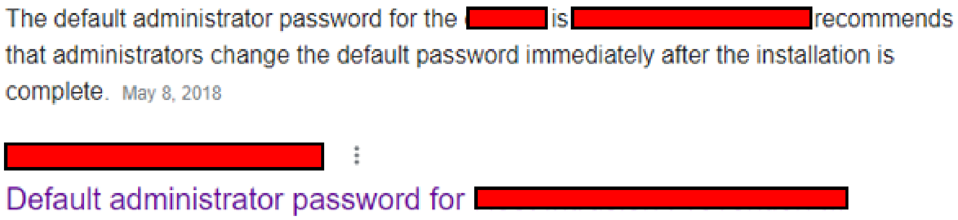
When testing OS endpoints, specifically its standard laptops, we observed that OS SOC was using the vendor's default password to protect access to the local administrator console of its endpoint protection tool.

OS OCIO hired a contractor to maintain the endpoint protection tool. The contract between the two organizations stated that the contractor was responsible for providing expertise on the tool and following Department IT security policy. Department policy and NIST security controls require that default passwords be changed before any software is deployed. Default passwords are only intended for the installation, initial testing, and configuration of a product, as they usually grant access to a system with administrative privileges. As described, the contractor did not change the default passwords.

We initially alerted OS leadership of this issue on March 22, 2022, and issued a formal management alert on April 20, 2022. OS OCIO later reported that it had updated the endpoint protection tool's password on April 15, 2022. During our fieldwork, we validated that the default password was changed; however, taking 24 days to make that change demonstrated that prompt action was not taken to fix a significant security weakness. It is well known that security is only as strong as its weakest links, and default passwords are one of them. Changing a default password is a fundamental security practice and should be quickly prioritized to eliminate an easy path of compromise.

As illustrated here, any OS user could log in to the local administrator console by performing a simple web search to identify the default password. Specifically, searching Google for the product default password revealed the password as the first search result, as displayed in Figure 2. Additionally, in the search result, the endpoint vendor recommended changing the default password immediately after installation.

Figure 2. First Search Result Showing the Product Default Password



The default administrator password for the [redacted] is [redacted] recommends that administrators change the default password immediately after the installation is complete. May 8, 2018

[redacted]

Default administrator password for [redacted]

Source: Google, with OIG redactions

By using the easily found password to log in to the console, attackers could disable safeguards on the endpoint, such as malware protection and monitoring of web browsing, allowing them to circumvent the tool's protections. With the tool effectively disabled, attackers could then perform lateral movement[7] to reach more valuable targets within OS.

Originally, OS OCIO management told us that the default password was used to allow users to run scans during the COVID telework posture. However, we later learned that the default password was used to assist the OS helpdesk and OS SOC with coordinating maintenance activities. And while any password could have been used to allow the two groups to coordinate, according to a SOC contractor, the default password was in use as far back as 2019.

Although Department policy requires changing of default passwords, OS OCIO's contractor did not take action to make a change. This represented a lack of due care by the contractor—and, furthermore, a lack of oversight from OS OCIO management, which is further discussed in finding III.A. The cybersecurity industry has repeatedly identified that default passwords represent a significant and easily remedied source of risk. According to a 2021 report from Verizon, credentials, including passwords, were involved in 61 percent of data breaches.[8] Thus, using a default password poses a major security risk.

B. *The endpoint protection tool did not effectively block malware*

Department policy[9] requires bureaus to (1) employ mechanisms to detect and eradicate malicious code and (2) protect information from unauthorized access, modification, and deletion. However, during our testing, we identified that OS OCIO's contractor had misconfigured the endpoint protection tool and had set one of its modules to observation mode. In this mode, the endpoint protection tool only logged suspected malicious activities but took no actions to block most of them. As a result, the tool only blocked one of our approximately 70 malicious testing activities, which included executing sample malware and malicious commands mimicking known APT actors. We observed this misconfiguration on the laptops provided by OS OCIO for our testing purposes and verified it on an OS employee's laptop. After we notified OS OCIO, it configured the module to provide active detection and blocking.

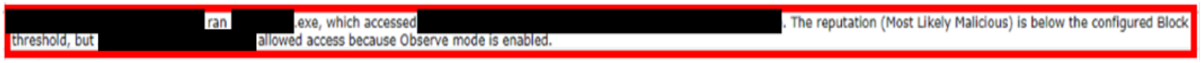
As shown in Figure 3, if the endpoint protection tool's module was properly configured, our actions could have been automatically blocked.

[7] *Lateral movement* is the tactic an adversary would use to navigate a network in an attempt to gain access to sensitive data.

[8] *See* Verizon. *2021 Data Breach Investigations Report* [online]. https://www.verizon.com/business/resources/reports/dbir/ (accessed March 30, 2022).

[9] DOC, June 2019. *Department of Commerce Information Technology Security Baseline Policy*. Washington, DC: DOC. This policy requires agencies to employ malicious code protection (SI-3) and information system monitoring (SI-4) to detect and eradicate malicious code and protect information obtained from intrusion monitoring via unauthorized access.

Figure 3. Example Endpoint Protection Event



[redacted] ran [redacted].exe, which accessed [redacted]. The reputation (Most Likely Malicious) is below the configured Block threshold, but [redacted] allowed access because Observe mode is enabled.

Source: Endpoint screenshot captured by OIG, with redactions

OS OCIO reported that an excess number of conflicting security rules had been created within the endpoint protection tool and that these overlapping rules allowed this vulnerability to occur. However, as part of a system's life cycle, security controls should be regularly assessed to ensure they are implemented effectively. We found that the malicious code protection control was not thoroughly assessed to ensure the tool was performing as intended (see finding III below).

In addition, Department and OS OCIO officials claimed that OS SOC has gone through organizational restructuring several times in recent years, resulting in multiple shifts in responsibilities for security tools. Further, they stated that OS SOC has experienced a high turnover rate for IT security personnel.

Regardless of the causes, our testing demonstrated that the lack of an effective endpoint protection product left OS endpoints vulnerable to many known and avoidable types of malware. This significantly increased the risk of a successful compromise of OS systems, which could lead to the theft of government data.

C. OS SOC did not detect most of the simulated attacks

From March 16–21, 2022, we successfully completed over 70 testing activities, including executing malicious commands to cause unauthorized changes, installing and executing unauthorized software, and exfiltrating PII. OS SOC has deployed firewalls and other detection tools that can automatically block, monitor, and respond to unusual activities on their network. However, it did not detect over 98 percent of our testing activities. In fact, it was ESOC that coincidentally detected one of our tests while performing updates to its Security Information and Event Management (SIEM) tool.[10] Following this detection, ESOC alerted OS SOC on March 23, 2022.

We found that this occurred, in part, because OS OCIO was unaware of its own firewall configurations. During an interview, an OS OCIO official stated that his team does manage firewalls, but that the team did not have knowledge of the firewall rulesets that control network traffic. Failing to block our testing activities was a strong indicator that OS' firewall was misconfigured and that the firewall protection was not fully effective. For example, many organizations configure their firewalls to block unauthorized email traffic. However, we were able to exfiltrate data using a simple email program we developed.

[10] A *SIEM* tool automatically compiles and analyzes data from multiple sources on security events for improved threat detection and incident management.

We also observed that, unlike ESOC, OS SOC did not have a working SIEM tool as the previous one went unmanaged and was misconfigured. SIEMs are an essential part of a SOC's toolkit. Using such a tool makes it easier for an organization to manage IT security by aggregating and filtering the massive amount of security data and by prioritizing security alerts.[11] The lack of a SIEM tool required OS SOC analysts to manually correlate alerts from different tools and increased the possibility of human error, as an analyst may miss a correlation.

Without ESOC's coincidental discovery, it is likely that none of our testing would have been detected. While we executed simple attacks that could be performed by low-skilled attackers, the Department faces APTs with more skilled threat actors equipped with significant resources who can accomplish more discrete attacks. In a real-world incident, a cyber attacker may gain unauthorized access to OS systems and remain undetected for an extended period, placing OS systems and data at greater risk.

Recommendations

We recommend that the Deputy Secretary of Commerce direct the Department's Chief Information Officer to do the following:

1. Perform a review of all software tools used within OS to ensure that default passwords are not used.
2. Ensure that OS OCIO holds its contractors accountable for implementing Department policy on default passwords.
3. Establish a process to regularly review OS SOC tools and ensure they are configured correctly and operating as intended.
4. Review and revise OS OCIO firewall configurations and rulesets to ensure that they are providing adequate protection to OS systems.
5. Establish processes and procedures to periodically review OS OCIO firewall configurations and rulesets.
6. Obtain the capability for OS OCIO to automatically aggregate security events and data using a tool such as a SIEM.

II. OS SOC Did Not Effectively Handle a Simulated Incident

We evaluated OS SOC's response to the alert it received from ESOC based on federal guidelines, such as the *Computer Security Incident Handling Guide*[12] from NIST. It is crucial that OS effectively handles incidents to minimize loss or theft of information and disruption of services caused by an incident. However, we found that OS SOC did not respond to our

[11] Techtarget. *What is SIEM and Why is it Important?* [online]. https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM/ (accessed October 25, 2022).

[12] DOC NIST CSRC. *Computer Security Incident Handling Guide*. Gaithersburg, MD: DOC NIST. Available online at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf (accessed October 6, 2022).

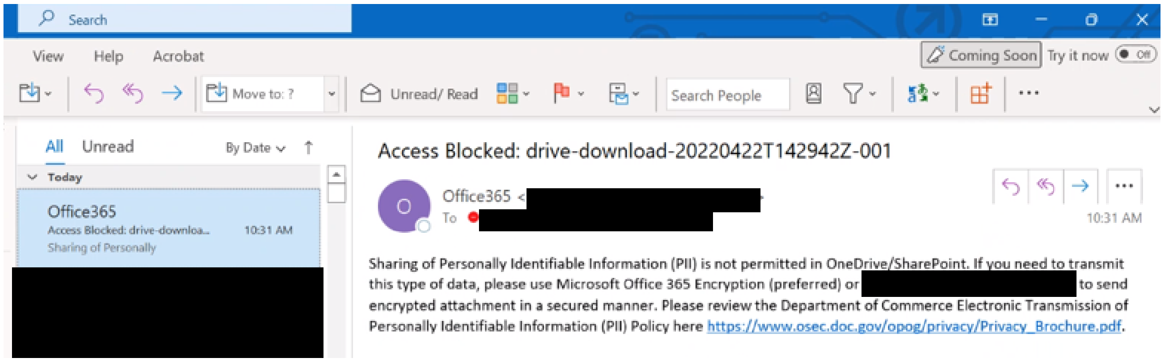
exfiltration of fictitious PII records and did not follow an effective digital forensic process. Furthermore, delays in communication between OS SOC and ESOC lengthened incident response time.

A. OS SOC did not respond to exfiltration of more than 100,000 fictitious PII records

The responsibility for Data Loss Prevention (DLP) security tools[13] was distributed across two OS OCIO groups. One DLP tool was managed by OS SOC, while the OS Local Area Network team (OS LAN) was responsible for another.

While the majority of our testing was performed in March 2022, we also conducted follow-up e-mail exfiltration testing on April 22, 2022. Altogether, we exfiltrated more than 100,000 records that contained fictious PII in formats such as spreadsheets and PDFs. We selected this number because CISA defines a loss of 100,000 records as the threshold for a major incident. Our exfiltration utilized multiple network protocols in both encrypted and plain-text formats. We conducted more than 30 successful exfiltration attempts of varying quantities of records that went undetected, including 10 instances of 100,000 records each. Only one instance was automatically blocked and reported by OS LAN's DLP tool, as shown in Figure 4. However, OS LAN did not take any action in response to this single instance.

Figure 4. Automatic PII Alert



Office365
Access Blocked: drive-downloa...
10:31 AM
Sharing of Personally

[redacted]

Access Blocked: drive-download-20220422T142942Z-001

Office365 <[redacted]

To [redacted]

10:31 AM

Sharing of Personally Identifiable Information (PII) is not permitted in OneDrive/SharePoint. If you need to transmit this type of data, please use Microsoft Office 365 Encryption (preferred) or [redacted] to send encrypted attachment in a secured manner. Please review the Department of Commerce Electronic Transmission of Personally Identifiable Information (PII) Policy here https://www.osec.doc.gov/opog/privacy/Privacy_Brochure.pdf.

Source: Endpoint screenshot captured by OIG, with redactions

Per the Department's Office of Privacy and Open Government, Department employees and contractors are responsible for protecting sensitive PII as well as recognizing and reporting any breaches. The Department's policy also requires bureaus to implement information systems monitoring, which can detect signs of compromise such as the mass exfiltration of sensitive records.

OS SOC stated that its tool was not configured properly and that it was planning to make improvements. OS LAN stated that the DLP alert was missed due to a lack of OS LAN personnel with specific cybersecurity knowledge and further claimed that it had no cybersecurity engineers available to create the secure configuration baselines needed for

[13] DLP tools assist with (1) identifying sensitive data stored, processed, or transmitted through enterprise assets and (2) blocking such data from leaving the enterprise.

effective DLP. We also confirmed that the alert generated by OS LAN's tool was never reported to OS SOC or ESOC. As evidenced by our simulated incident, an attacker or insider within OS' systems could exfiltrate PII records or other sensitive information, possibly without being detected. Additionally, if data exfiltration was detected by DLP tools, it is not apparent that OS OCIO would have reacted appropriately.

B. OS SOC did not follow an effective digital forensic process

Digital forensics is the process of acquiring, analyzing, and preserving electronic data.[14] During our evaluation, we found that OS SOC did not preserve evidence of our testing activities. OS SOC utilized ESOC's assistance in performing digital forensics on the laptops we used to execute malicious testing activities. However, OS SOC had prematurely run anti-malware scans on these laptops, rather than creating forensic clones[15] first, which inadvertently deleted some of the evidence. This action contradicted proper digital forensics by compromising the integrity of the files.

In addition, we observed that OS SOC was not able to efficiently support ESOC's forensic analysis, which delayed the investigation by up to 2 weeks. OS SOC struggled with removing its standard encryption from the laptops, which was needed for ESOC to conduct forensic activities.

When reviewing documentation, we observed that OS OCIO's official incident response plan had no mentions of digital forensics or any procedures on caring for potential evidence. The OS Chief Information Security Officer stated that OS SOC does not have any forensic capabilities and is entirely dependent on ESOC for digital forensics. However, the service-level agreement (SLA) between the two organizations was outdated, and Department leadership stated that it did not accurately reflect services that are provided. OS SOC also struggled with retrieving the encryption keys needed by ESOC to conduct forensics because its team was unfamiliar with the process to do so. This was likely due to the lack of any defined, written forensic process.

Digital forensics allow an incident response team to get a more complete picture of an attack and may reveal critical information such as backdoors,[16] lateral movement, and logic bombs.[17] Failing to correctly perform forensics during incident response could cause irreparable damage to evidence that may be useful in potential criminal investigations or to understand the extent of an attack.

[14] Digital forensics is "the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data." *See* DOC NIST CSRC, August 2006. *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86. Gaithersburg, MD: DOC NIST. Available online at https://csrc.nist.gov/publications/detail/sp/800-86/final (accessed October 6, 2022).

[15] A *forensic clone* is an exact copy of a hard drive.

[16] A *backdoor* is an undocumented way of gaining access to computer system and can be a potential security risk.

[17] *Logic bombs* are pieces of code intentionally inserted into a software system that will set off malicious functions when specified conditions are met.

C. Delays in communication between OS SOC and ESOC lengthened incident response time

ESOC and OS SOC share responsibility for responding to cybersecurity incidents within OS. Thus, efficient communication between the two organizations is critical to effective incident response.[18] As discussed in the previous subfinding, the two organizations did not have an adequate SLA to guide their cooperation. Throughout the response to our simulated incident, we observed lapses in communication between ESOC and OS SOC. During our testing, we observed that ESOC had to repeatedly ask for updates and resend requests to OS SOC. In total, there were 24 instances where ESOC asked for a response or requested an update on outstanding requests. This contributed to almost a week-long delay in OS SOC's request for forensic analysis.

After interviewing ESOC and OS SOC, we found that they utilized different ticketing systems[19] without reciprocal access. While ESOC was able to access OS SOC's ticketing system, OS SOC was unable to access ESOC's system. Therefore, the only method of collaboration between the two groups was via email, which could have resulted in delays due to communication between multiple individuals, collaboration on responses, and the frequency of checking email. Any delay to incident response is significant, as it allows attackers additional time to accomplish their goals.

Recommendations

We recommend that the Deputy Secretary of Commerce direct the Department's Chief Information Officer to do the following:

7. Review OS's DLP practices, including but not limited to updating the configurations of DLP products and ensuring that incidents are reported to OS SOC and ESOC in a timely manner.
8. Update the existing SLA to define clear responsibilities between ESOC and OS for the incident handling process.
9. Update OS OCIO's cybersecurity incident response plan to include procedures for carrying out digital forensics.
10. Increase communication between the OS SOC and ESOC by allowing reciprocal access to ticketing systems or creating a common system.

III. OS OCIO Did Not Manage Its Incident Detection and Response Program in Accordance with Federal Requirements

During our evaluation, we saw a lack of maturity in OS OCIO's incident detection and response program that likely contributed to its poor handling of our simulated incident. This included failing to follow federal requirements, which are designed to ensure that government systems properly account for risk. Additionally, we observed that critical

[18] NIST's *Incident Handling Guide* emphasizes the importance of communication to handle incidents efficiently and effectively.

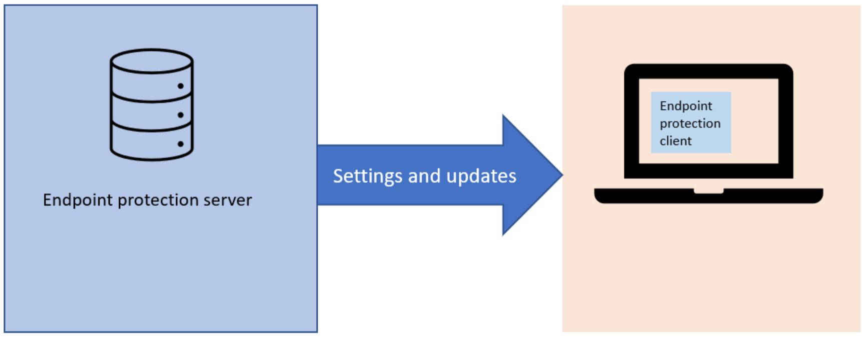
[19] A ticketing system serves as the central location for documenting an incident and sharing relevant information.

policies and procedures relating to incident detection and response were either outdated or missing.

A. *OS OCIO did not consistently adhere to federal requirements to operate its endpoint protection tool*

The endpoint protection tool is an integral system component for OS' incident detection and protection operation. It operates using a client-server architecture, in which individual client software installed on the endpoints connects to a master server and acquires configuration settings and updates (see figure 5).

Figure 5. Endpoint Protection Tool Client-Server Architecture



Source: OIG

We found that OS OCIO did not properly follow the NIST *Risk Management Framework* (RMF) requirement[20] of ensuring all IT systems receive an authorization to operate (ATO). RMF steps include determining which IT components are part of a system and identifying security requirements for the system. Specifically, OS OCIO did not receive an ATO for the server portion of the endpoint protection tool. Additionally, although the client portion of the tool was authorized, OS OCIO did not adequately assess security controls for it.

According to OS OCIO officials, OS SOC underwent several management and organizational changes. As a result, the endpoint protection server was overlooked and was not included as part of an authorized system. Thus, OS OCIO did not conduct any security control assessments of the endpoint protection server. This caused the bureau to overlook significant security weaknesses in the tool's configuration, such as the observation mode issue described in finding I.B.

Furthermore, to determine whether endpoint protection was enabled, contractors assessed the client portion of the tool solely via a personnel interview and a review of the system security plan document, rather than conducting an actual technical review.

[20] DOC NIST CSRC, December 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37, Revision 2. Gaithersburg, MD: DOC NIST. Available online at https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final (accessed October 10, 2022). Office of Management and Budget *Circular A-130* requires all federal executive branch agencies to implement a risk management framework.

This limited security assessment of the endpoints directly contributed to the insecure state in which a default password was used, as shown in finding I.A.

Improper implementation of the RMF can negatively influence leadership decisions by providing an incomplete or inaccurate picture of risks. Indeed, our testing showed that malware could be successfully executed on OS systems. Without following the RMF process, OS OCIO cannot provide adequate management oversight of its IT security operations.

B. OS OCIO incident detection and response policies and procedures either did not exist or were outdated

During the evaluation, we found that OS OCIO lacked policies and procedures across many areas, including incident detection and response. For example, not only did OS OCIO not have a documented incident response plan to efficiently detect, respond to, and recover from security events, it also lacked other closely related policies, such as a contingency plan or a continuous monitoring strategy. Such plans are crucial to identifying and recovering from a significant cybersecurity incident and resuming operations.

We also observed that the existing SLA between OS SOC and ESOC had not been updated since 2017. During interviews, Department leadership stated that this agreement did not support the current state of operations.

OS OCIO conducted a self-assessment in June 2022. The assessment results revealed that its IT security program was immature and underdeveloped.[21] Other than a lack of resourcing, the Department and OS OCIO officials we interviewed were unable to explain why establishing and updating IT security policies, procedures, and SLAs have been neglected. And while OS OCIO officials repeatedly attributed the identified security weaknesses to a lack of resources, they were unable to provide evidence of IT security-related prioritization efforts made during the last 2 years. Nevertheless, OS OCIO has since recognized the immaturity of its program and started taking steps to document suggested remediation actions, such as hiring a policy specialist or technical writer to develop, review, and update cybersecurity policies, processes, and procedures.

The Department requires its bureaus to develop policies and procedures to support its many IT security functions. Defining policies and procedures helps an organization meet requirements and accomplish its goals. For example, a detailed, up-to-date incident response plan may have been able to help OS SOC defend against our simulated attacks. Instead, our work showed that OS OCIO struggled to effectively handle a simple, simulated incident, which indicated that it was not prepared to address a more serious, real-world incident.

[21] Based on the Capability Maturity Model Integration (CMMI), organizations with a low maturity level often spend most of their time reacting to events, rather than developing or following documented standards.

Recommendations

We recommend that the Deputy Secretary of Commerce direct the Department's Chief Information Officer to do the following:

11. Establish a timeline to ensure that the systems responsible for endpoint protection are properly authorized.
12. Establish a procedure to ensure sufficient government oversight is provided to contractors who are responsible for OS endpoint protection.
13. Establish tracking and reporting processes to ensure OS OCIO cybersecurity policies and procedures are developed, up to date, and in compliance with federal requirements.
14. Identify which improvement opportunities within the OS OCIO remediation plan should be prioritized to enhance OS' incident detection and response.

Conclusion

OS' detection and response capabilities were not adequate to handle our simulated incident. OS OCIO needs to take serious action to improve its incident detection and response program. As shown throughout this report, the program lacked the proper security foundations, including tools, policies, and procedures necessary to detect and respond to a cybersecurity incident. While OS OCIO had begun to identify its weaknesses, it had yet to prioritize efforts to improve incident detection and response. As a result, OS was unprepared in the event of an actual cybersecurity incident.

Summary of Agency Response and OIG Comments

On February 17, 2023, we received the Department's response to our draft report. In response to our draft report, the Department concurred with all our recommendations and described actions it has taken, or will take, to address them. The Department's formal response is included in appendix B.

Prior to receiving the Department's response, we met with Department officials to discuss their concerns regarding the public release of the report. Following the discussions, we made minor changes to the report.

We are pleased that the Department recognizes the significance of our findings and recommendations. We look forward to receiving its action plan for implementing the recommendations.

Appendix A: Objective, Scope, and Methodology

Our evaluation objective was to assess the adequacy of actions taken by the Department and its bureaus when detecting and responding to cyber incidents in accordance with federal and Departmental requirements.

To accomplish our evaluation objective, we performed the following actions:

- Reviewed relevant policies and procedures
- Simulated incident(s) within OS, including
    - Emulating activities associated with known threat actors
    - Exfiltrating fictitious, protected data
    - Emulating command and control network traffic
- Evaluated the effectiveness of the actions taken in response to the simulated incident

We reviewed OS' compliance with the following applicable internal controls, provisions of law, and mandatory guidance:

- The Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551, *et seq*.
- U.S. Department of Commerce *Information Technology Security Baseline Policy*
- NIST Special Publications:
    - 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
    - 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*
    - 800-61, Revision 2, *Computer Security Incident Handling Guide*
    - 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
    - 800-171, Revision 2*, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*

Our analysis did not rely on computer-processed data to support our findings, conclusions, or recommendations. We omitted certain technical information in the report for security reasons.

We conducted our review from January 2022 through October 2022 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401-424), and Department Organization Order 10-13, dated October 21, 2020. We performed our work remotely.

We conducted this evaluation in accordance with *Quality Standards for Inspection and Evaluation* (December 2020) issued by the Council of the Inspectors General on Integrity and Efficiency.

Those standards require that the evidence supporting the evaluation's findings, conclusions, and recommendations should be sufficient, competent, and relevant and should lead a reasonable person to sustain the findings, conclusions, and recommendations. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations based on our evaluation objective.

Appendix B: Agency Response

UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

MEMORANDUM FOR: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation
U.S. Department of Commerce
Office of Inspector General

FROM: André V. Mendes
Chief Information Officer
U.S. Department of Commerce

ANDRE MENDES Digitally signed by ANDRE MENDES Date: 2023.02.17 21:04:56 Z

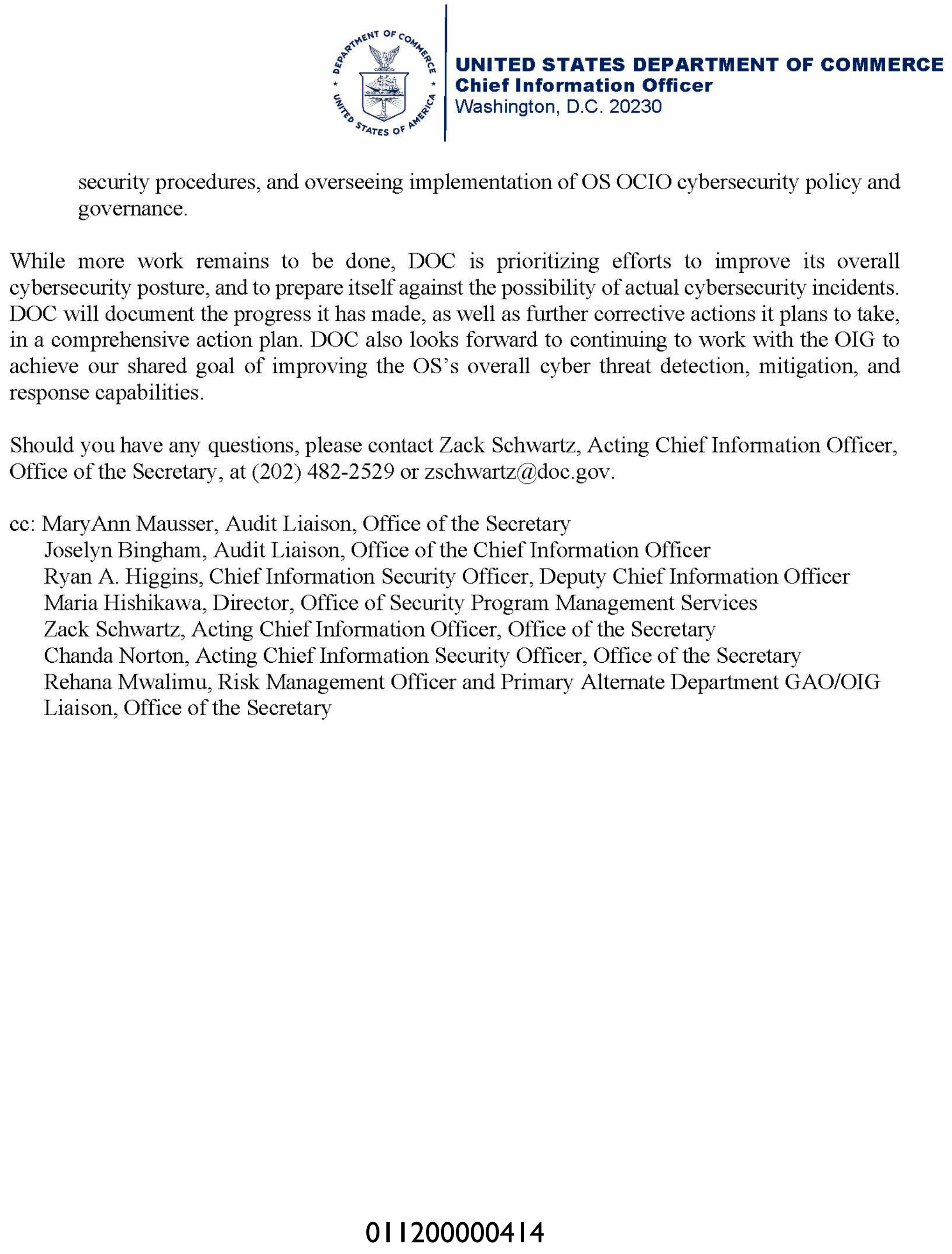
SUBJECT: Department of Commerce Office of the Secretary's Concurrence to the Office of Inspector General's Draft Report, *Fundamental Deficiencies in OS' Cybersecurity Incident Response Program Increase the Risk of Cyberattacks (January 5, 2023)*

DATE: February 17, 2023

This memorandum serves as the Department of Commerce (DOC)'s response to the Office of Inspector General (OIG) draft report entitled *Fundamental Deficiencies in OS' Cybersecurity Incident Response Program Increase the Risk of Cyberattacks (January 5, 2023).* Thank you for the opportunity to review the draft report and provide these comments.

DOC concurs with the draft report's findings and recommendations, which were significant. As a result, both during the Inspector General's evaluation period last year, and since it ended in October 2022, DOC has taken meaningful steps to begin addressing the issues identified in the draft report. Some of the actions DOC has completed to date—offered in summary form to not compromise security—include:

- The Office of the Secretary's Office of the Chief Information Officer (OS OCIO) ensured that default passwords were no longer being used for security tools, and has since performed regular updates to administrative passwords.
- OS OCIO performed a security assessment of its headquarters management network and received an Authorization to Operate.
- OS OCIO adopted modern cybersecurity tools to replace legacy technology at all OS OCIO managed endpoints.
- OS OCIO implemented a daily security maintenance checklist, requiring contractors and federal employees to perform daily checks on critical security tools.
- OS OCIO filled a newly created federal position, the "Governance, Risk, and Compliance (GRC) Information Systems Security Officer." This individual is responsible for, among other things, reviewing, updating, and maintaining Bureau security system policies and



UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

security procedures, and overseeing implementation of OS OCIO cybersecurity policy and governance.

While more work remains to be done, DOC is prioritizing efforts to improve its overall cybersecurity posture, and to prepare itself against the possibility of actual cybersecurity incidents. DOC will document the progress it has made, as well as further corrective actions it plans to take, in a comprehensive action plan. DOC also looks forward to continuing to work with the OIG to achieve our shared goal of improving the OS's overall cyber threat detection, mitigation, and response capabilities.

Should you have any questions, please contact Zack Schwartz, Acting Chief Information Officer, Office of the Secretary, at (202) 482-2529 or zschwartz@doc.gov.

cc: MaryAnn Mausser, Audit Liaison, Office of the Secretary
Joselyn Bingham, Audit Liaison, Office of the Chief Information Officer
Ryan A. Higgins, Chief Information Security Officer, Deputy Chief Information Officer
Maria Hishikawa, Director, Office of Security Program Management Services
Zack Schwartz, Acting Chief Information Officer, Office of the Secretary
Chanda Norton, Acting Chief Information Security Officer, Office of the Secretary
Rehana Mwalimu, Risk Management Officer and Primary Alternate Department GAO/OIG Liaison, Office of the Secretary