

---

# **BIS Needs to Improve Its Incident Response Capabilities to Handle Sophisticated Cyberattacks**

REPORT NO. OIG-25-022-I

JUNE 11, 2025

---





June 11, 2025

**MEMORANDUM FOR:** Jeffrey Kessler  
Under Secretary of Commerce for Industry and Security  
Bureau of Industry and Security

A handwritten signature in black ink, appearing to read "Kevin D. Ryan".

**FROM:** Kevin D. Ryan  
Acting Assistant Inspector General for Audit and Evaluation

**SUBJECT:** *BIS Needs to Improve Its Incident Response Capabilities to Handle Sophisticated Cyberattacks*  
Report No. OIG-25-022-I

Attached is the final report on our evaluation of the Bureau of Industry and Security's detection of and response to cyber incidents. We will post the report on [our website](#) per the Inspector General Act of 1978, as amended (5 U.S.C. §§ 404, 420).

Within 60 calendar days, please provide an action plan addressing the report's recommendations, as required by Department Administrative Order 213-5.

We appreciate your staff's cooperation and professionalism during this evaluation. If you have any questions or concerns about the report, please contact me at 202-695-0791 or Charles Mitchell, Director for Cybersecurity, at 202-809-9528.

Attachment

cc: Brian Epley, Chief Information Officer, Office of the Chief Information Officer  
Ryan A. Higgins, Deputy Chief Information Officer and Chief Information Security Officer, Office of Cybersecurity and IT Risk Management  
Nathan Thweatt, Director, Office of Cybersecurity Operations Services  
Joe Bartlett, Deputy Under Secretary, BIS  
Angela Vicinanza, Chief Information Officer, BIS  
Ida Mix, Chief Information Security Officer, BIS





## BIS Needs to Improve Its Incident Response Capabilities to Handle Sophisticated Cyberattacks

Evaluation Report OIG-25-022-I

June 11, 2025

➤ **What We Audited** | Our objective was to assess the adequacy of actions taken by the Bureau of Industry and Security (BIS) when detecting and responding to cyber incidents in accordance with federal and departmental requirements.

➤ **Why This Matters** | Cyberattacks frequently compromise government and business networks. After attackers gain access to a network, they often bypass traditional security measures, leveraging trusted access to compromise sensitive data and systems. Therefore, defending against threats inside the network, such as insider threats, is as crucial as securing its perimeter.

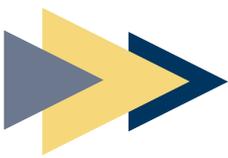
BIS's oversight of export controls helps restrict the proliferation of weapons of mass destruction and the means of delivering them. This makes BIS and the Department attractive targets for sophisticated state-sponsored adversaries.

➤ **What We Found** | We found that:

- BIS lacked effective detection and response capabilities to handle our simulated malicious activities
- BIS misconfigured critical security controls for its export control networks
- BIS mishandled classified and other privileged credentials

Based on our testing, BIS lacked the capabilities, tools, and procedures necessary to detect and respond to our malicious activities. If BIS does not improve its current capabilities, advanced adversaries could significantly harm sensitive U.S. export control efforts, which in turn affects national security.

➤ **What We Recommend** | We made 13 recommendations to BIS to increase endpoint and network protection, proactively seek and mitigate threats, establish procedures to respond to incidents, restrict network and user access, and improve the security of network credentials. BIS concurred with our recommendations and is working to implement them.



# Contents

- Introduction.....1**
  - Objective ..... 2
- Findings and Recommendations .....3**
  - BIS Lacked Effective Detection and Response Capabilities to Handle Our Simulated Malicious Activities..... 4
    - BIS did not effectively detect our malicious activities ..... 4
    - BIS did not effectively respond to our malicious activities ..... 6
    - BIS did not detect or prevent our exfiltration of fictitious sensitive information .. 7
    - Recommendations..... 7
  - BIS Misconfigured Critical Security Controls for Its Export Control Networks ..... 8
    - Recommendations..... 9
  - BIS Mishandled Classified and Other Privileged Credentials .....10
    - BIS users violated requirements for secure credential storage, including instances of classified credentials .....10
    - BIS used default or weak passwords for hundreds of user accounts .....11
    - BIS provided us with the widely reused local administrator password without verifying our eligibility .....12
    - Recommendations.....13
- Conclusion ..... 14**
- Summary of BIS’s Response and OIG Comments..... 15**
- Appendix 1. Scope and Methodology..... 16**
- Appendix 2. BIS’s Response..... 18**

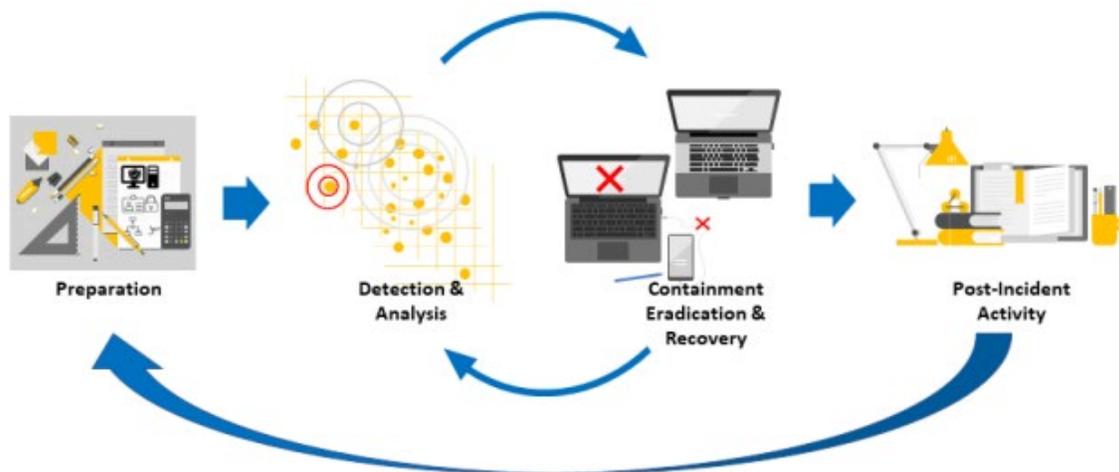


# Introduction

Cyberattacks frequently compromise government and business networks. After attackers gain access to a network, they often bypass traditional security measures, leveraging trusted access to compromise sensitive data and systems. Therefore, defending against threats inside the network, such as insider threats,<sup>1</sup> is as crucial as securing its perimeter.

It is critical that organizations respond quickly and effectively when these attacks 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. Figure 1 illustrates the phases of incident response as defined by the National Institute for Standards and Technology (NIST).

Figure 1. Incident Response Lifecycle



Source: Office of Inspector General (derived from NIST)

Within the U.S. Department of Commerce (the Department), the Bureau of Industry and Security (BIS) and many other bureaus operate independent security operations centers (SOCs), which are responsible for detecting and responding to cybersecurity incidents. In general, incident responders:

- Use information and alerts from incoming and outgoing network traffic, endpoints (such as laptops), and various other security tools to detect an incident

---

<sup>1</sup> The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency defines an insider threat as someone with authorized access to an organization who intentionally or unintentionally harms that organization. See U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency. [Defining Insider Threats](#). Accessed January 7, 2025.

- Investigate the incident
- Contain, eradicate, and recover from the incident as part of the incident response lifecycle

Additionally, the Department has established a separate Enterprise SOC (ESOC) that manages the Department's network perimeter and coordinates incident response across the Department and with other agencies. BIS SOC and the Department's ESOC work together to provide cyber incident response and detection. BIS SOC is responsible for managing day-to-day information technology (IT) security and performing initial triage of cyber incidents within BIS.

BIS's mission is to protect U.S. national, economic, cyber, and homeland security by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. BIS's oversight of export controls helps restrict the proliferation of weapons of mass destruction and the means of delivering them. This makes BIS and the Department attractive targets for sophisticated state-sponsored adversaries. For example, in July 2023, China-based hackers breached Department email accounts, including the Secretary of Commerce and BIS email accounts. This incident underscores the importance of our evaluation for ensuring BIS can effectively handle advanced cybersecurity attacks and continue supporting the bureau's critical mission.

## ➤ **Objective**

The objective of our evaluation was to assess the adequacy of actions taken by BIS when detecting and responding to cyber incidents in accordance with federal and departmental requirements. Appendix 1 details our scope and methodology.



## Findings and Recommendations

**Summary:** Our evaluation focused on BIS’s detection of and response to our simulated cyber incidents on its networks, which are monitored by both BIS SOC and ESOC. Since the BIS networks we discuss in this report contain sensitive information, we do not identify them by name; instead, we refer to them as Network A, Network B, and Network C.

To evaluate BIS’s and the Department’s actions, we used The MITRE Corporation’s Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) framework to simulate malicious activities advanced threat actors currently perform. We conducted our testing under the premise of assumed compromise, acting as either an attacker who had already gained unauthorized access to BIS networks or as an insider threat. The activities we simulated included exfiltrating fictitious personally identifiable information (PII) and business identifiable information (BII), establishing persistent access<sup>2</sup> within BIS networks, making unauthorized changes to BIS computers, conducting lateral movement,<sup>3</sup> and guessing BIS user passwords.

We found that BIS did not effectively detect and respond to our simulated malicious activities. BIS could not detect our attacks until we intentionally acted to trigger alerts. Once BIS was alerted, its response was not effective at containing the potential damage and eradicating our access to its networks. Our testing also revealed additional information security vulnerabilities. Specifically, we found that:

---

<sup>2</sup> *Persistent access* refers to an attacker’s ability to maintain a foothold within a targeted network over time, avoiding detection and ensuring continued access to compromised systems. See Compean, Nancy, June 6, 2023, [What is Persistence in Cybersecurity and How Do You Stop an Advanced Persistent Threat \(APT\)?](#), accessed April 15, 2025; The MITRE Corporation, July 19, 2019, [Persistence](#), accessed April 15, 2025.

<sup>3</sup> *Lateral movement* refers to the technique attackers use to expand their access within a network. Rather than staying confined to the first system they compromise, attackers move through the network, often seeking to escalate privileges, find valuable data, or increase their control over multiple systems. See SentinelOne. August 1, 2022. [What is Lateral Movement? Definition & Examples](#). Accessed January 7, 2025.

- BIS lacked effective detection and response capabilities to handle our simulated malicious activities.
- BIS misconfigured critical security controls for its export control networks.
- BIS mishandled classified and other privileged credentials

Based on our testing, BIS lacked the capabilities, tools, and procedures necessary to detect and respond to our malicious activities. If BIS does not improve its current capabilities, advanced adversaries could significantly harm sensitive U.S. export control efforts, which in turn affects national security. Whether the threat comes from external actors or insiders, BIS must be ready to handle future attacks.

## ➤ **BIS Lacked Effective Detection and Response Capabilities to Handle Our Simulated Malicious Activities**

Before an organization can respond to a cybersecurity incident, it must have an effective method to detect it. BIS SOC uses an endpoint detection and response (EDR) solution,<sup>4</sup> which can provide malware detection and prevention. When an EDR detects a potential malicious activity, it generates an alert, enabling SOC analysts to identify and investigate security threats. However, we found during our testing that BIS's detection and response capabilities were not effective for identifying and addressing our simulated malicious activities.

### **BIS did not effectively detect our malicious activities**

The Department requires<sup>5</sup> its bureaus to monitor network communications to identify any unusual or unauthorized conditions. We conducted simulated malicious activities on three

---

<sup>4</sup> EDR solutions are security tools installed on desktops, laptops, servers, and mobile devices to provide threat detection and prevention, automated incident response, and forensic investigation capabilities. Organizations use these tools to quickly identify and investigate security incidents, reducing the time to detect and respond to threats. See Palo Alto Networks, [What is EDR-as-a-Service Managed Security?](#), accessed January 7, 2025; Sophos, [What is endpoint detection and response \(EDR\)?](#), accessed January 7, 2025.

<sup>5</sup> Commerce OIG. December 2024. *Department of Commerce Enterprise Cybersecurity Policy (ECP) Security and Privacy Control Matrix (SPCM)*, Version 1.4, SI-04(4).

BIS networks, including configuring hidden connections (backdoors<sup>6</sup>) for BIS to detect. Our attacks corresponded with tactics listed in the MITRE ATT&CK framework, examples of which include Credential Access and Exfiltration (see appendix A for a full listing). Overall, we found that BIS did not effectively detect our simulated malicious activity. When our activities caused BIS's EDR tool to generate alerts, BIS security staff responded. However, when no alerts were generated, BIS either had a delayed response—in some cases, up to 9 days—or did not respond at all.

On Network A, BIS did not detect any of our simulated malicious activities, including when we intentionally attempted to trigger security monitoring tools. For example, BIS did not receive an alert when we installed malicious software on the network. Our testing found that Network A did not have an EDR solution installed on any of the servers and endpoints we reviewed. The system security plan for Network A identifies EDR (malicious code protection)<sup>7</sup> as a required control. When BIS management last verified the control in 2022, the plan noted this was an inherited common control from the Department. However, when we reviewed the common control list, it stated, “This security control is not within the scope of BIS COMMON [sic] Controls.” As such, security staff mistakenly assumed the control was being inherited when it was not. Because BIS did not install an EDR solution on Network A, security staff were unable to detect malicious activities on these endpoints. This means Network A would also be more vulnerable to many attacks and avoidable types of malware, reducing BIS's ability to prevent unauthorized access.

Further, we found BIS had an EDR tool capable of conducting threat hunting, exploitation mitigation, and forensic investigation on Network B and Network C. However, our testing revealed that BIS did not use this tool to proactively detect our malicious activity or identify our malicious network persistence. If BIS had used these capabilities, it would not have had to rely solely on EDR alerts.

The Department's security standard<sup>8</sup> includes an optional control to conduct threat hunting, which BIS did not choose to implement as part of its security plan. Unlike traditional reactive security measures that respond to alerts after they are triggered, threat hunting involves security staff deliberately seeking out hidden threats that automated tools may not have detected or that might have bypassed existing defenses. Although this control is optional, our testing demonstrated the risk of reactively relying on alerts. While the use of an EDR may help detect less advanced threats, more sophisticated

---

<sup>6</sup> “An undocumented way of gaining access to computer system. A backdoor is a potential security risk.” See National Institute of Standards and Technology Computer Security Resource Center. “[Backdoor.](#)” Accessed February 3, 2025.

<sup>7</sup> Commerce Security and Privacy Control Matrix, SI-03. The Department currently uses an EDR solution for SI-3 (Malicious Code Protection).

<sup>8</sup> Commerce Security and Privacy Control Matrix, RA-10.

adversaries—like the ones whose actions we simulated—can bypass security capabilities and avoid triggering alerts. For instance, on Network B and Network C, BIS did not discover our simulated activities until we intentionally performed actions we suspected would generate EDR alerts, about 9 days after the start of our attack. After the EDR generated an alert, BIS responded.

Our tests showed that an EDR solution, while important, is only the starting point because it will not always catch and generate an alert for malicious activity. We found that if an alert was not generated, then BIS was either not aware of or was severely delayed in detecting our attacks. Under these conditions, sophisticated attackers who have gained access to BIS's networks would be able to remain undetected.

### BIS did not effectively respond to our malicious activities

BIS's Incident Response Plan<sup>9</sup> describes the containment and eradication steps BIS security staff must take when attempting to contain and eradicate threats, as illustrated in figure 1. Among other things, security staff should eliminate the vulnerability the attacker used and remove any installed malware.

During our testing of networks A, B, and C, we found BIS did not effectively contain and eradicate our simulated attacks. For example, during our testing, security staff attempted to stop our simulated attack by disabling the administrator account we were using to make our system connection. However, we had set up alternative access methods prior to their response. Because BIS did not identify the root cause of the attack, which was our ability to install and hide malicious software, its attempts to contain and eradicate our access to the system were not effective. Furthermore, BIS inconsistently applied remediation efforts. In one example, after detecting some of our malicious activities, BIS SOC disabled the account we were using. However, that same user account had an associated administrator account that BIS did not disable. In a second example, BIS blocked one of our Internet Protocol<sup>10</sup> (IP) addresses on Network B, but did not block that same IP address on Networks A and C. In a third example, BIS SOC disabled all administrator accounts it thought were compromised in an attempt to stop us. However, while its response disabled the administrator accounts, our connection remained active, allowing us continued access. While disabling or deleting accounts to contain malicious activity is an important part of incident handling, identifying the root cause of the malicious activity is crucial for stopping a sophisticated attacker.

---

<sup>9</sup> Bureau of Industry and Security. May 22, 2023. *Security Incident Response Plan*.

<sup>10</sup> An IP address is a unique identifier assigned to each device connected to a computer network. This enables different devices to identify and communicate with each other across networks and the internet. See Fortinet. [What Is An IP Address? How Does It Work?](#) Accessed January 7, 2025.

When we reviewed BIS's incident response plan, we noted that the response steps were written at a high level and did not provide detailed procedures. The document listed bullet points such as "remove any rootkits the attacker installed," but did not provide steps for how to complete that task. When we reviewed the procedures document, we noted that it consisted of NIST security control implementation statements, which also do not provide step-by-step instructions. Without detailed procedures, each responder would need to determine the steps to take, resulting in an inconsistent and potentially incomplete response.

During a real incident, BIS's current response methods would likely not stop a skilled attacker, placing BIS networks and data at great risk. It is imperative that BIS improve incident handling to identify and defend against these advanced threats.

### BIS did not detect or prevent our exfiltration of fictitious sensitive information

Department policy requires BIS to identify and prevent the exfiltration of PII, BII, and other sensitive data from BIS networks. However, during our testing, BIS did not detect or prevent our exfiltration of thousands of fictitious PII and BII records. Specifically, we exfiltrated over 100,000 fictitious records, including Social Security numbers, birthdates, and passport numbers, from all three networks via email and other communication protocols. We were able to do this because BIS did not have a solution to detect our exfiltration and prevent sensitive data from leaving the network. One example of a technology that could help BIS prevent data exfiltration is a data loss prevention (DLP) solution. A DLP solution is a technical control to protect sensitive information from being leaked, misused, or lost. Since BIS did not have a DLP, BIS SOC only discovered that we had exfiltrated this data during its post-incident analysis 4 days later. Using the same methods, an attacker could exfiltrate PII or other sensitive information without being detected. This could lead to financial harm, identity theft or fraud, damage to BIS's reputation, and a potential loss of public trust in BIS.

## Recommendations

We recommend the Undersecretary of Commerce for Industry and Security direct BIS's Chief Information Officer to:

1. Implement an EDR on Network A.
2. Adopt the threat hunting security control and use existing BIS SOC tools to proactively hunt threats and mitigate malicious or unauthorized network activity.
3. Establish and implement detailed incident response procedures to detect, contain, eradicate, and recover from threats.

4. Implement a method to identify and prevent the exfiltration of PII, BII, and other sensitive data from BIS networks.

## ► **BIS Misconfigured Critical Security Controls for Its Export Control Networks**

To protect against lateral movement and prevent attackers from learning how to exploit a system, the Department requires least functionality<sup>11</sup> for systems, least privilege<sup>12</sup> for system users, and network boundary protection. Through our simulated attacks on Networks A, B, and C, we identified network and system security misconfigurations—instances where software or hardware configurations were not secure—on BIS networks. This allowed us to extract information related to the systems’ software components, user accounts, network hardware, available communication ports,<sup>13</sup> and location of sensitive data. This form of information extraction, known as enumeration, gives attackers a roadmap for exploiting a system when they gain entry.

Network B contains more sensitive data than the other networks we tested. Accordingly, BIS’s system security plan required that Network B have controlled internet connectivity that only allowed limited connections into the network. To implement this requirement, BIS deployed a technical control to restrict external connections. However, we found that we could bypass those limitations due to a misconfiguration of the technical control. Additionally, our testing took advantage of another misconfiguration that allowed regular user accounts to run system commands and scripts—privileges typically reserved for system administrators. Combining these misconfigurations allowed us to bring in and execute malicious software with our regular user accounts and exfiltrate fictitious PII and BII records—attacks that a threat actor could also perform.

In addition to the security misconfigurations we found in Network B, we saw similar issues in Networks A and C. According to BIS, these networks should not be able to freely communicate with each other, allowing for limited exceptions. However, we found that Network A could communicate with Networks B and C due to improperly configured

---

<sup>11</sup> Least functionality is a configuration control that requires information systems to employ only the minimum functionality or capabilities necessary for proper use. See CSF Tools, [PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities](#), accessed January 7, 2025; Georgetown University Information Security Office, [UIS.203.7 Least Functionality Guidelines](#), accessed January 7, 2025.

<sup>12</sup> Least privilege is an account management control that requires system users to have only the privileges or permissions that are relevant and required. See NIST CSRC. [Least privilege](#). Accessed January 7, 2025.

<sup>13</sup> The entry or exit point from a computer for connecting communications or peripheral devices. See NIST CSRC. [“Port.”](#) Accessed January 7, 2025.

network restrictions, which allowed us to move laterally across these three networks. This lateral movement would allow a threat actor from Network A to access the sensitive data on other BIS networks, including the more sensitive data on Network B.

Finally, we also found an issue with a mission-critical trade application residing on Network B. This application was used for processing export license applications and other compliance-related activities. According to the principle of least privilege, users should only be able to view data relevant to their assigned duties—in this case, documents related to the cases they are assigned. However, our testing found that users had access to records outside of their areas of responsibility. Specifically, the user we observed could access files from another office. BIS management confirmed that, although user responsibilities may include investigations that could require broad access, the system is not capable of restricting user access. This system limitation prevents the principle of least privilege from being implemented and provides an insider threat or a malicious actor a way to read all sensitive trade application data with a single user account.

BIS eventually detected some of our testing on Networks B and C, as we noted in finding I. However, based on the results of our testing, significant security misconfigurations existed across Networks A, B, and C. These misconfigurations allowed us to set up hidden connections to transfer malicious software into BIS networks, run privileged system commands and scripts, exfiltrate sensitive data, and move laterally across networks. When we briefed BIS management on these issues, they informed us that they have started to resolve the misconfigurations. However, until the misconfigurations are fully mitigated, sensitive data will be at greater risk from external and insider threats.

## Recommendations

We recommend the Undersecretary of Commerce for Industry and Security direct BIS's Chief Information Officer to:

5. Properly configure network security devices to prevent unauthorized connections from outside BIS networks.
6. Properly restrict BIS networks to prevent unauthorized lateral movement between BIS networks.
7. Implement a security control to allow only approved software on Network B and consider implementing this control for all BIS networks.
8. Review all BIS user access, for networks and applications, to ensure each user is assigned the correct levels of access according to the principle of least privilege.

## ► **BIS Mishandled Classified and Other Privileged Credentials**

Credentials, like a username and password, verify that a user is who they claim to be. Authenticating users with a credential is a fundamental part of IT security. However, threat actors can exploit lost or stolen usernames and passwords. Therefore, it is essential for users and organizations to protect and carefully manage passwords. We found that BIS users had stored classified credentials on an unclassified network, and that BIS mismanaged both regular and privileged user credentials on multiple unclassified networks. Additionally, after guessing weak and default passwords, we had the ability to access other user accounts across BIS networks.

### **BIS users violated requirements for secure credential storage, including instances of classified credentials**

Storing credentials in plain text, without any attempt to obscure them, presents a major security risk because it is easier for attackers to steal them. During our testing, we created scripts to scan for plain-text passwords stored on the BIS network, demonstrating abilities available to attackers. As a result, we found 20 files that contained approximately 120 plain-text credentials for accessing federal systems, as well as highly sensitive personal web services. Further, we found three BIS employees stored documents in those files with plain-text credentials for a classified system on an unclassified network. Two BIS users had stored their full credentials, and the third BIS user stored a portion of their credentials, on unclassified Network C. These credentials were required to be protected as classified data for 10 years after being created.

Storing credentials in plain text violated departmental<sup>14</sup> and federal<sup>15</sup> requirements for secure credential storage and for storing classified credentials outside of their classified system. Our review of the classified accounts determined that they were either inactive or had expired passwords, and the Department concluded that the risk of the classified credential spill was low. Although the Department determined these accounts were low-risk when we discovered them, it is likely at some point the saved credentials were active and could have been used. Furthermore, according to a study performed by a cybersecurity research firm,<sup>16</sup> users often make small changes to old passwords when updating them, which could make guessing an active password easier. Moreover, knowing expired

---

<sup>14</sup> Commerce Security and Privacy Control Matrix, IA-5.

<sup>15</sup> Executive Office of the President, December 29, 2009. Executive Order 13526: Classified National Security Information. The order states that “[c]lassified information may not be removed from official premises without proper authorization.”

<sup>16</sup> See Truta, Filip. November 3, 2023. [Protecting Your Important: Is It Safe to Use Variants of the Same Password for Different Accounts?](#) Accessed March 19, 2025.

passwords could give an attacker insight into the system’s password rules for length and complexity.

Additionally, we observed that BIS was not taking the precaution of performing self-assessments to safeguard classified information, such as reviewing users’ files for classified materials. As required by Executive Order 13587, BIS must self-assess its compliance with policy and standards relating to the classified networks it uses. BIS management told us it believed this was a user behavior issue and has since sent a message to all users reminding them of password storage best practices. However, BIS security staff were unaware of the plain-text credentials until we alerted them during our testing. While users may make mistakes, BIS could have run scripts to identify potential classified information spills and plain-text passwords. As we demonstrated during our testing, proactive steps to identify plain-text credentials or other sensitive data types are important.

### BIS used default or weak passwords for hundreds of user accounts

BIS has implemented strong multifactor authentication via personal identity verification (PIV) cards and hard tokens.<sup>17</sup> However, before employees receive a PIV, their accounts are set up with a username and password. We found that account passwords remained enabled even after the users received their PIV cards or hard tokens, meaning those passwords were still available to bypass BIS’s otherwise strong multifactor authentication. Passwords are inherently weaker than PIV cards and hard tokens because they can be stolen through phishing, reused across multiple sites, and guessed using brute force<sup>18</sup> or other attacks.

In fact, across the three networks we tested, we were able to guess passwords for 847 of 6,638 accounts (13 percent),<sup>19</sup> 814 of which were using the default password originally

---

<sup>17</sup> Hard tokens are physical objects that generate one-time passwords to authenticate a user’s access to a system. See CDW, August 11, 2022, [Hard Tokens vs. Soft Tokens](#), accessed January 7, 2025; 1Kosmos, [What Is a Hardware Security Token? Explained](#), accessed January 7, 2025.

<sup>18</sup> An attack that involves trying all possible combinations to find a match. See NIST CSRC. [“Brute Force Password Attack.”](#) Accessed January 7, 2025.

<sup>19</sup> To avoid exposing a sensitive password, Microsoft Active Directory stores user passwords in a secure, unintelligible format called a “hash.” A hash is a one-way mathematical function that turns data into a string of nondescript text that cannot be reversed or decoded. The hashed version of a password is not usually accepted through typical authentication operations, such as login prompts. Therefore, an attacker would attempt to “crack” the hash (through methods like brute force, dictionary attacks, rainbow tables, and exploiting weaknesses in older hash algorithms) prior to usage. See U.S. Department of the Interior Office of Inspector General, January 3, 2023, [P@s\\$w0rds at the U.S. Department of the Interior: Easily Cracked Passwords, Lack of Multifactor Authentication, and Other Failures Put Critical DOI Systems at Risk](#), 4-5, accessed January 7, 2025; Vaidesswaran, Narendran, January 16, 2024, [Hashing in Cybersecurity](#), accessed January 7, 2025.

created by the BIS helpdesk. This was possible because BIS did not assign a random password during initial account setup but instead used the same easily guessed password for all user accounts. The remaining 33 passwords were weak enough that our password testing tool could easily guess them. Furthermore, the BIS helpdesk did not configure the account to require a password change after a user used the account for the first time. Therefore, attackers could abuse the weak default password assigned by the helpdesk to access other user accounts. The Department’s requirements for managing passwords emphasize that users must change passwords assigned to them after first use.<sup>20</sup> However, BIS had not implemented this control, which gave us the ability to log in to any of these accounts because BIS did not properly enforce multifactor authentication. With the guessed passwords, we also correctly guessed that regular users and administrators were assigned the same default password on account creation.

The cybersecurity industry has repeatedly identified default passwords as a significant and easily remedied source of risk. For example, the U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) has identified default credentials as a top weakness that threat actors exploit to gain access to systems, including those within U.S. critical infrastructure. CISA also found that “threat actors . . . have been successful in compromising critical infrastructure systems in the United States by exploiting operational technology (OT) products sold by manufacturers with passwords set to a static default.”<sup>21</sup>

### BIS provided us with the widely reused local administrator password without verifying our eligibility

In addition to the large number of easily guessed passwords, we also found that the BIS helpdesk did not have validation procedures to follow when helping users with access issues. BIS helpdesk employees sometimes share the device’s local administrator<sup>22</sup> account credentials with BIS users when troubleshooting certain issues. However, the procedures did not require helpdesk employees to validate BIS users before providing local administrator credentials, which we exploited during our fieldwork. After BIS SOC locked us out of our accounts for malicious activity, we called the BIS helpdesk and it gave us a local administrator account and password without verifying our user status. This allowed

---

<sup>20</sup> Commerce, *Rules of Behavior*, Version 1.0; and Commerce, October 2024, *Rules of Behavior for Non-Privileged Users*, Version 1.1.

<sup>21</sup> DHS CISA. [Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords](#). Accessed January 7, 2025.

<sup>22</sup> A local administrator account is a user account with elevated privileges. Local administrator accounts are specific to the device and do not require an internet connection or central server for authentication. They allow users to install software, change system settings, and perform other administrator actions. See Microsoft. September 6, 2024. [“Local Accounts.”](#) Accessed January 22, 2025.

us to continue our malicious activity and provided us with a completely different account to use to remotely connect to various devices on the network.

We also found that BIS does not change passwords after giving users local administrator credentials. This provided us with an additional method to move between systems, because BIS configured the local administrator account on many devices to use the same password. If a threat actor gains access to the local administrator credentials, that actor can misuse them to cause serious harm to all the systems that share that same password.

We are concerned by the lack of proper account and credential management practices at BIS. External threat actors and insider threats would be able to cause significant harm to BIS networks and data by exploiting these conditions. If BIS does not improve the access controls for BIS systems, considerable risk to its security posture will remain.

## Recommendations

We recommend the Undersecretary of Commerce for Industry and Security direct BIS's Chief Information Officer to:

9. Immediately search BIS networks for classified credentials and establish a procedure to regularly search for plain-text credentials.
10. Ensure passwords are disabled for all user accounts as soon as operationally possible.
11. Establish and implement BIS helpdesk procedures for user access issues, including a user verification process.
12. Implement an automated solution to change local administrator credentials after sharing them with BIS users and use different local administrator passwords for each system.
13. Implement a technical control to generate unique, strong passwords for each account created.



## Conclusion

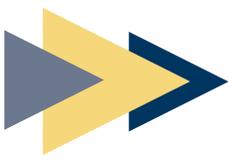
BIS's detection and response capabilities were not adequate to handle our simulated malicious activities. The BIS incident response program lacked the capabilities, tools, and procedures necessary to detect and respond to the cybersecurity incidents we tested. Further, BIS's handling of classified and other privileged credentials allowed us to expand our attacks and avoid containment. While BIS SOC was quick to respond to some alerts, BIS needs to improve its capabilities to be more proactive and thorough in detecting and responding to sophisticated cyber incidents.



## Summary of BIS's Response and OIG Comments

BIS reviewed a draft version of this report and responded to our findings and recommendations. In its response, BIS concurred with all of our recommendations and described actions it has taken or plans to take to address them. BIS's complete response, which also included general comments, is included in this report as appendix 2.

We are pleased that BIS concurs with our recommendations. We look forward to receiving BIS's action plan, which will provide details on its corrective actions.



## Appendix 1. Scope and Methodology

Our objective was to assess the adequacy of actions taken by BIS when detecting and responding to cyber incidents in accordance with federal and departmental requirements.

To accomplish our objective, we:

- Reviewed system-related artifacts, including policies and procedures, planning documents, and security control documentation
- Worked extensively with Department and BIS trusted insiders to coordinate our technical testing
- Simulated incidents within BIS, including
  - Emulating activities associated with known threat actors
  - Exfiltrating fictitious protected data
  - Emulating command and control network traffic
- Retrieved, analyzed, and correlated system logs and other SOC artifacts for Networks A, B, and C to evaluate the effectiveness of the actions taken in response to the simulated incident
- Interviewed BIS officials, including system owners, IT security and operations staff, and management

The MITRE Corporation's ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. We used this framework to help structure the stages of our technical testing so that each stage was aligned with real-world adversarial behavior. Specifically, we simulated the following 11 tactics:

1. Execution
2. Persistence
3. Privilege Escalation
4. Defense Evasion
5. Credential Access
6. Discovery
7. Lateral Movement
8. Collection

9. Command and Control
10. Exfiltration
11. Impact

We also reviewed BIS' 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 *Enterprise Cybersecurity Policy*, October 2022
- OMB M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, December 4, 2023
- OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022
- OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, August 27, 2021
- OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017
- US-CERT, *Federal Incident Notification Guidelines*, effective April 1, 2017
- BIS *Incident Response Plan*, May 22, 2023
- NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, updated December 2020

We 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 evaluation from May 2024 through April 2025 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 fieldwork 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 and conclusions 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 review objective.



## Appendix 2. BIS's Response

BIS's response to our draft report begins on the next page.



UNITED STATES DEPARTMENT OF COMMERCE  
Under Secretary for Industry and Security  
Washington, D.C. 20230

May 15, 2025

TO: Kevin D. Ryan  
Acting Assistant Inspector General for Audit and Evaluation  
Office of Inspector General

FROM: Jeffrey Kessler

SUBJECT: **Audit Report: BIS Needs to Improve Its Incident Response Capabilities to Handle Sophisticated Cyberattacks, Draft Report**

**Report Date:** May 15, 2025

**Audited Entity:** Bureau of Industry and Security

Thank you for the opportunity to respond to the OIG draft report entitled *BIS Needs to Improve Its Incident Response Capabilities to Handle Sophisticated Cyberattacks*.

BIS concurs with the recommendations and will prepare a formal action plan upon issuance of OIG's final report.

**OIG's Recommendation #1:** Implement an EDR on Network A.

*RESPONSE: Concur. BIS understands the importance of having an EDR agent on all endpoints and has begun working with DOC to ensure Network A has full coverage. BIS is currently 40% of the way through installation.*

**OIG's Recommendation #2:** Adopt the threat hunting security control and use existing BIS SOC tools to proactively hunt threats and mitigate malicious or unauthorized network activity.

*RESPONSE: Concur. BIS understands the need for proactive threat hunting to protect BIS assets given the constantly evolving cyber threat landscape. BIS analysts have completed the training offered by the DOC ESOC. BIS is evaluating the effectiveness of its threat hunting using various scenarios that will be incorporated into a playbook on threat hunting.*

**OIG's Recommendation #3:** Establish and implement detailed incident response procedures to detect, contain, eradicate, and recover from threats.

*RESPONSE: Concur. BIS will update the Incident Response plan and develop incident response runbooks. BIS has conducted incident response training with its operations and helpdesk staff. BIS will test the incident response capability using scenario-based tabletop exercises.*

**OIG's Recommendation #4:** Implement a method to identify and prevent the exfiltration of PII, BII, and other sensitive data from BIS networks.

*RESPONSE: Concur. In the near term, as BIS continues to modernize its cybersecurity infrastructure, BIS will plan to deploy a network DLP capability to prevent PII, BII and sensitive data exfiltration. BIS will need to evaluate the cost of fully deploying, configuration, and maintaining a DLP solution to determine if it can be supported within current funding levels.*

**OIG's Recommendation #5:** Properly configure network security devices to prevent unauthorized connections from outside BIS networks.

*RESPONSE: Concur. BIS has completed this action and has blocked unauthorized connections identified as part of this audit. The deployment of the secured next generation firewalls (NGFW) will prevent future unauthorized connections. The effort to deploy these NGFW is expected to begin in FY25 Q3.*

**OIG's Recommendation #6:** Properly restrict BIS networks to prevent unauthorized lateral movement between BIS networks.

*RESPONSE: Concur. The accelerated migration from on-premises hosting to the current cloud environment removed the historic network segmentation. In the short term, BIS will reestablish network security groups to prevent lateral movement. This is expected to be completed in FY25.*

**OIG's Recommendation #7:** Implement a security control to allow only approved software on Network B and consider implementing this control for all BIS networks.

*RESPONSE: Concur. BIS understands the risk that unauthorized software can introduce. Today, BIS only allows system administrators to install software. BIS will establish procedures and alerting for software installations. Additionally, BIS will evaluate enabling technology, such as privileged access management technologies, to prevent unauthorized installations by administrators. Introduction of a privileged access management solution would be dependent on overall cost and funding levels.*

**OIG's Recommendation #8:** Review all BIS user access, for networks and applications, to ensure each user is assigned the correct levels of access according to the principle of least privilege.

*RESPONSE: Concur. In the short term, BIS will conduct a user audit for each network and application and will conduct a regular recertification process for users of all networks and applications. To fully solve this problem and automate user access and privileges, BIS must modernize the identity and access management solution as well as the BIS applications.*

**OIG's Recommendation #9:** Immediately search BIS networks for classified credentials and establish a procedure to regularly search for plain-text credentials.

*RESPONSE: Concur. As part of its security awareness messaging, BIS OCIO sent a broadcast email to all BIS staff with reminders of password best practices and highlighting the risk of storing plain text credentials. Furthermore, the BIS SOC has established scanning across BIS networks to detect keywords that indicate the presence of classified or plain text credentials. BIS will establish procedures, in collaboration with DOC, for managing the response, reporting, and remediation of any classified or plain text credentials found through that scanning.*

**OIG's Recommendation #10:** Ensure passwords are disabled for all user accounts as soon as operationally possible.

*RESPONSE: Concur. BIS has begun an account clean up on all networks and applications. BIS will*

*implement a new account management process and will also conduct regular recertification for all users.*

**OIG's Recommendation #11:** Establish and implement BIS helpdesk procedures for user access issues, including a user verification process.

*RESPONSE: Concur. BIS understands the importance of establishing a user verification process. BIS has begun exploring options for providing the BIS helpdesk unique identifiers for employees and contractors.*

**OIG's Recommendation #12:** Implement an automated solution to change local administrator credentials after sharing them with BIS users and use different local administrator passwords for each system.

*RESPONSE: Concur. BIS will develop the means to reset these passwords automatically. In the interim, BIS will establish procedures to ensure unique passwords are used for each system and reset after sharing them with BIS users.*

**OIG's Recommendation #13:** Implement a technical control to generate unique, strong passwords for each account created.

*RESPONSE: Concur. BIS has completed this action and has implemented a system to generate unique, strong passwords for each account.*

# REPORT

# FRAUD & WASTE ABUSE



## HOTLINE



Department of Commerce

**Office of Inspector General Hotline**

[www.oig.doc.gov](http://www.oig.doc.gov) | 800-424-5197