Data Quality Challenges and Ineffective Program Management Hinder the Department's Enterprise Cybersecurity Capabilities

FINAL REPORT NO. OIG-25-006-A
DECEMBER 17, 2024

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

December 17, 2024

MEMORANDUM FOR: Don Graves
Deputy Secretary of Commerce

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

SUBJECT: *Data Quality Challenges and Ineffective Program Management Hinder the Department's Enterprise Cybersecurity Capabilities*
Final Report No. OIG-25-006-A

Attached for your review is our final report on our audit of the U.S. Department of Commerce's (the Department's) Enterprise Continuous Diagnostics and Mitigation (ECDM) program. Our audit objective was to assess the effectiveness of the Department's ECDM program. To address this objective, we assessed data quality, data security, and aspects of program management in a recent ECDM tool procurement decision.

We found the following:

I. ECDM data quality does not fully support Department oversight and reporting needs.
II. The National Institute of Standards and Technology (NIST) does not consistently control and thoroughly test the ECDM program's information system changes.
III. The ECDM program's information system is relatively secure but has some internal security weaknesses.
IV. Deficiencies in ECDM program management place future enterprise cybersecurity tool deployments at risk.
V. The Department does not fully incorporate bureau-incurred costs in its ECDM project cost tracking.

On November 8, 2024, 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 the Department and NIST have taken, or will take, to address them. The Department also provided technical comments from NIST. We considered those comments and made changes to the report where appropriate. Appendix D contains the full text of the Department's response and NIST's technical comments.

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 our website pursuant to the Inspector General Act of 1978, as amended (5 U.S.C. §§ 404 & 420).

We appreciate the cooperation and courtesies extended to us by your staff during this audit. If you have any questions or concerns about this report, please contact me at (202) 793-2938 or Chuck Mitchell, Director for Cybersecurity, at (202) 809-9528.

Attachment

cc: Brian Epley, Chief Information Officer, OCIO
Ryan Higgins, Chief Information Security Officer, OCIO
Param Soni, Chief Information Officer, BEA
Angela Vicinanza, Chief Information Officer, BIS
Luis Cano, Chief Information Officer, Census Bureau
Hannah Brown, Chief Information Officer, NIST
Zachary Goldstein, Chief Information Officer, NOAA
Catrina Purvis, Chief Information Officer, NTIA
Gary Haney, Interim Chief Information Officer, Office of the Secretary
Jamie Holcombe, Chief Information Officer, USPTO
May Cheng, Acting Chief Information Officer, ITA
Jim Gwinn, Chief Information Officer, FirstNet Authority

Report in Brief

December 17, 2024

Background

The Enterprise Continuous Diagnostics and Mitigation (ECDM) program is a critical part of the U.S. Department of Commerce's (the Department's) strategy for meeting its cybersecurity modernization goals and transitioning to a Zero Trust Architecture by the end of fiscal year 2024. ECDM is the Department's implementation of the Continuous Diagnostics and Mitigation (CDM) program in collaboration with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). The Department deploys security tools procured via CISA's CDM program across all Department bureaus to provide enterprise-wide visibility into security for reporting, risk management, continuous monitoring, and incident response. CISA uses the Department's cybersecurity data collected via ECDM to assess, track, and respond to cybersecurity threats across all federal agencies. The Department operates the ECDM program through a National Institute of Standards and Technology (NIST)-managed information system.

Our previous audit work found the Department faces challenges in meeting ECDM program goals. The Department and CISA told us the biggest risk the ECDM program currently faces is a deficiency in asset visibility. Effective cybersecurity efforts hinge on accurate asset discovery and management—the Department cannot secure unseen and untracked assets, and subsequent cybersecurity capabilities, such as vulnerability management and incident response, are built on this cornerstone.

Why We Did This Review

Our audit objective was to assess the effectiveness of the Department's ECDM program.

OFFICE OF THE SECRETARY

Data Quality Challenges and Ineffective Program Management Hinder the Department's Enterprise Cybersecurity Capabilities

OIG-25-006-A

WHAT WE FOUND

We found that the Department has not yet adequately strengthened its cybersecurity posture by fully implementing its ECDM program. Specifically, we found the following:

I. ECDM data quality does not fully support Department oversight and reporting needs.

II. NIST does not consistently control and thoroughly test the ECDM program's information system changes.

III. The ECDM program's information system is relatively secure but has some internal security weaknesses.

IV. Deficiencies in ECDM program management place future enterprise cybersecurity tool deployments at risk.

V. The Department does not fully incorporate bureau-incurred costs in its ECDM project cost tracking.

Remediating these deficiencies is important to ensure the ECDM program achieves the goals of reducing the Department's threat surface, increasing cybersecurity visibility, improving response capabilities, and streamlining reporting.

WHAT WE RECOMMENDED

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

- Develop and implement oversight mechanisms to manage and track whether bureaus meet hardware asset management, software asset management, configuration security management, and vulnerability management data collection and reporting requirements. Implementing this recommendation will lead to funds being put to better use.
- Develop and implement oversight mechanisms to ensure Department cybersecurity data reported in the CDM agency dashboard and used in Chief Information Officer Federal Information Security Modernization Act metric reporting accurately reflects the Department's cybersecurity posture.
- Incorporate the Office of Acquisition Management's project management best practices into the ECDM program and ensure program and project managers overseeing the ECDM program obtain a level I Federal Acquisition Certification for Program and Project Managers.
- Design and implement a process to track and report bureau-incurred ECDM program costs for improved cost reporting and analysis of cost-saving opportunities.

We recommended that the Deputy Secretary of Commerce direct the Department's Chief Information Officer and NIST's Chief Information Officer to:

- Design and implement a technical control to prevent changes to the production environment without proper configuration change control processes and testing.
- Implement logging for the security policy changes identified by our testing.
- Review our detailed technical report and develop and implement a corrective action plan to resolve the issues we identified in our penetration testing.

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

Today's dynamic and increasingly sophisticated cyber threat environment makes cybersecurity modernization essential to national and economic security. The Enterprise Continuous Diagnostics and Mitigation (ECDM) program is a critical part of the U.S. Department of Commerce's (the Department's) strategy for meeting its modernization goals and transitioning to a Zero Trust Architecture[1] by the end of fiscal year (FY) 2024.

CISA's CDM program

The U.S. Department of Homeland Security's (DHS's) Cybersecurity and Infrastructure Security Agency (CISA) developed the Continuous Diagnostics and Mitigation (CDM) program in 2012 to support the government's efforts to provide risk-based, consistent, and cost-effective cybersecurity solutions for federal civilian networks. CDM defines five capabilities:

- dashboard,
- asset management,
- identity and access management,
- network security management, and
- data protection management.

Of these, dashboard and asset management are CISA's current focus areas, with additional capabilities rolling out in phases over time. "Dashboard" refers to a data visualization tool that provides an easy-to-understand overview of the Department's cybersecurity posture. The dashboard portion of CDM contains an agency-specific dashboard and CISA's federal government-wide dashboard. While the Department provides data to both dashboards, CISA is responsible for dashboard implementation. "Asset management" involves tracking information technology (IT) hardware and software inventories, security configurations, and software vulnerabilities.[2]

The Department's ECDM program

ECDM is the Department's implementation of the CDM program in collaboration with CISA. The Department deploys security tools procured via CISA's CDM program[3] across all Department bureaus to provide enterprise-wide visibility into security for reporting, risk

[1] This is a strategy based on the acknowledgement that threats exist both inside and outside traditional network boundaries. *See* U.S. Department of Commerce National Institute of Standards and Technology Computer Security Resource Center, December 2021. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, NIST SP 800-160 Vol. 2 Rev. 1. Washington, DC: DOC NIST. Available online at https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final (accessed June 14, 2024).

[2] Vulnerabilities refer to weaknesses in a system that cyber attackers can exploit to gain unauthorized access or cause harm. These can include software bugs, misconfigurations, or insecure network protocols.

[3] For the purposes of this report, we use "ECDM" to describe the Department's responsibilities and implementation of CISA's CDM program.

management, continuous monitoring, and incident response. CISA uses the Department's cybersecurity data collected via ECDM to assess, track, and respond to cybersecurity threats across all federal agencies.[4] The Department uses the ECDM program to meet Office of Management and Budget (OMB) and CISA cybersecurity requirements. The Department oversees ECDM and procures enterprise-wide security tools. Individual Department bureaus operate and maintain the security tools within their own environments.

The Department operates the ECDM program through a National Institute of Standards and Technology (NIST)-managed information system. The ECDM program's information system is important because it processes and stores sensitive cybersecurity data used by the Department and its bureaus.

ECDM program challenges and risks

As the ECDM program expands, it will cover more aspects of cybersecurity, requiring robust program management, future procurements, and increased coordination across the Department's bureaus. Our previous audit work found the Department faces challenges in meeting ECDM program goals. For instance, the misconfiguration of an ECDM vulnerability scan tool led to inaccurate reporting of critical vulnerabilities on one of the Department's high value assets (HVAs).[5] Additionally, due in part to the Department's noncompliance with CISA's asset management reporting threshold, we reported that the Department's cybersecurity risk management program maturity was ineffective.[6]

Deficiencies in asset discovery and management pose especially significant risks. During an early planning meeting, both the Department and CISA told us the biggest risk the ECDM program currently faces is a deficiency in asset visibility. Effective cybersecurity efforts hinge on accurate IT asset discovery and management—the Department cannot secure unseen and untracked assets, and subsequent cybersecurity capabilities, such as vulnerability management and incident response, are built on this cornerstone. Accordingly, the Department must effectively manage its ECDM program to improve the Department's cybersecurity posture.

[4] See appendix C for a breakdown of how the Department's cybersecurity data flows into agency and federal cybersecurity reporting dashboards.

[5] DOC Office of Inspector General, September 28, 2023. *Security Weaknesses in the Department's Mission-Critical High Value IT Assets Leave the Assets Vulnerable to Cyberattacks*, OIG-23-030-A. Washington, DC: DOC OIG.

[6] DOC OIG, July 25, 2023. *FY 2023 Federal Information Security Modernization Act Annual Report*, OIG-23-023-A (nonpublic report). Washington, DC: DOC OIG.

Objective, Findings, and Recommendations

Our audit objective was to assess the effectiveness of the Department's ECDM program. We assessed data quality, data security, and aspects of program management in a recent ECDM tool procurement decision. See appendix A for a full description of our scope and methodology.

Overall, we found that the Department has not yet adequately strengthened its cybersecurity posture by fully implementing its ECDM program. Specifically, we found the following:

I. ECDM data quality does not fully support Department oversight and reporting needs.

II. NIST does not consistently control and thoroughly test the ECDM program's information system changes.

III. The ECDM program's information system is relatively secure but has some internal security weaknesses.

IV. Deficiencies in ECDM program management place future enterprise cybersecurity tool deployments at risk.

V. The Department does not fully incorporate bureau-incurred costs in its ECDM project cost tracking.

Remediating these deficiencies is important to ensure the ECDM program achieves the goals of reducing the Department's threat surface,[7] increasing cybersecurity visibility, improving response capabilities, and streamlining reporting. The Department considers the ECDM program mission-critical and strategically important. The Department's *FY 2023 – 2025 Cybersecurity Strategy* notes "that as the risks to the Department's information and information systems from sophisticated threat actors continue to evolve, it is critical that [the Department] modernize and grow cybersecurity capabilities to keep pace and build on the foundation of the [ECDM] program."[8] If the Department has an ineffective foundation, it will face challenges in implementing cybersecurity modernization requirements placed on federal agencies. Additionally, reporting to CISA will be difficult and time-consuming compared to the automation that ECDM would provide.

I. ECDM Data Quality Does Not Fully Support Department Oversight and Reporting Needs

ECDM data is essential for a variety of users, including bureau security personnel, the Department's Office of the Chief Information Officer (OCIO), and external federal stakeholders like CISA and OMB. Early in our audit, the Department and CISA both stated that the accuracy and completeness of cybersecurity data collected by ECDM was their

[7] A threat surface includes information system circumstances or events that could harm people or organizations through unauthorized access, destruction, disclosure, modification, or denial of service. *See* Committee on National Security Systems, March 7, 2022. *Committee on National Security Systems (CNSS) Glossary*, CNSSI 4009. Available online at https://www.cnss.gov/CNSS/issuances/Instructions.cfm (accessed July 12, 2024).

[8] DOC, September 2022. *FY 2023 – 2025 Cybersecurity Strategy*. Washington, DC: DOC.

main concern. Our testing found that ECDM data is not accurate and complete, making it difficult to use and reducing its effectiveness for oversight and reporting activities. Without accurate data, the Department will find it difficult to meet CISA reporting and program requirements.

A. Important cybersecurity data is not available in the Department's IT asset inventory

The Department's internal ECDM policy memo dated December 2022[9] requires Departmental bureaus to associate every hardware asset they use (laptops, desktops, servers, networking devices, etc.) with the specific federal information systems to which they belong. Additionally, CISA requires the Department to report an asset's authorization status and HVA status to the ECDM agency dashboard.[10] Knowing which information system an asset belongs to, whether that asset is authorized to be on the network, and whether the asset is mission-critical enables risk analysis and appropriate response to security incidents.

To determine how well the Department associates assets to the information systems the assets belong to, we mapped assets found in ECDM's cybersecurity data to the Department's official Federal Information Security Modernization Act of 2014 (FISMA)-reportable[11] system inventory as of April 2024. We found that of the 10 bureaus tested, 8 have not met their responsibilities of associating assets with their information systems (see figure 1). Only 23 percent (69 of 303) of the FISMA-reportable information systems had assets associated to them in ECDM. Most critically, that number accounts for only 5 of 32 high-impact[12] systems and 4 of 40 HVAs.[13] As such, the Department has a considerable gap in cybersecurity visibility of its most critical information systems.

[9] DOC, December 2022. *Required Actions in Support of the Department's Continuous Diagnostics and Mitigation Program and Automated Reporting Requirements* (internal Department document). Washington, DC: DOC.

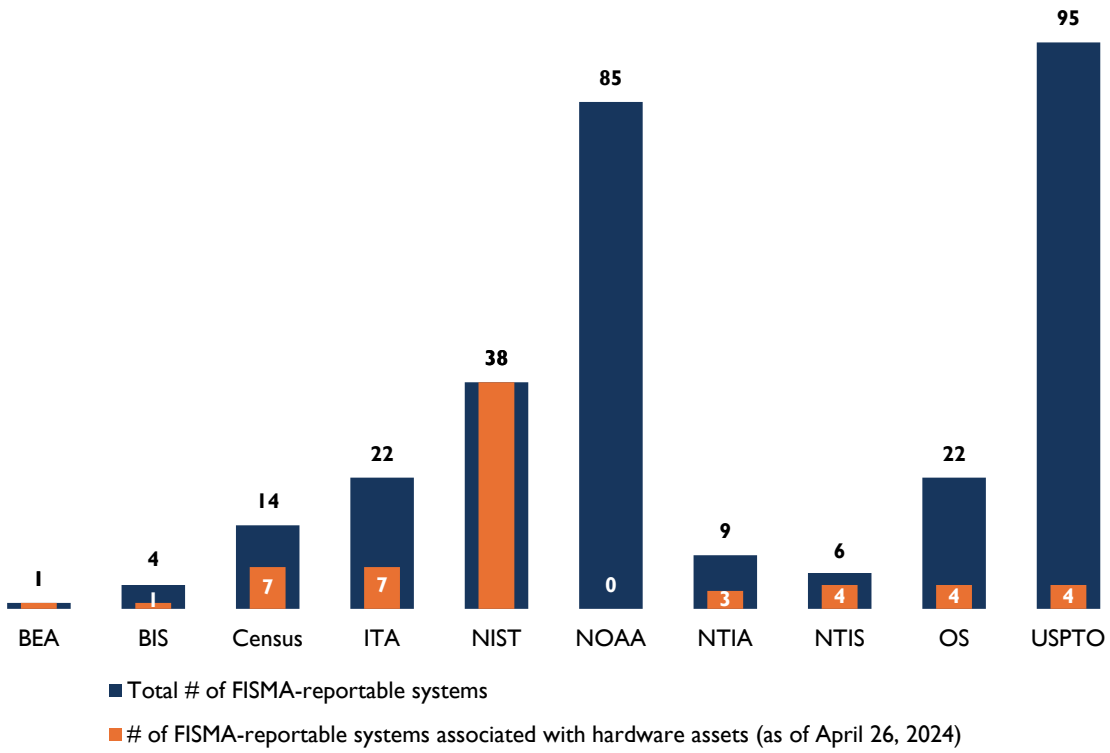
[10] U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency, October 2023. *Continuous Diagnostics and Mitigation (CDM) Program Architecture*, Version 4.1.1. Arlington, VA: DHS CISA. Available online at https://www.cisa.gov/resources-tools/resources/cdm-data-model-document-411 (accessed May 23, 2024).

[11] This is any information system used or operated by an agency, a contractor of an agency, or other organization on behalf of an agency. 44 U.S.C. 3554 a(1)(A)(ii).

[12] Cybersecurity incidents involving the Department's high-impact systems could be expected to have a severe or catastrophic adverse effect on Department operations, assets, or individuals. *See* DOC NIST, February 2004. *Standards for Security Categorization of Federal Information and Information* Systems, FIPS PUB 199. Gaithersburg, MD: DOC NIST. Available online at https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf (accessed June 18, 2024).

[13] HVAs represent systems of particular interest to potential adversaries because they contain high-value information or are considered critical to the Department's mission. *See* DOC NIST, May 2020. *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*, NIST Special Publication 800-137A. Gaithersburg, MD: DOC NIST. Available online at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-137A.pdf (accessed June 20, 2024).

Figure 1. FISMA-reportable Systems Associated with Hardware Assets in ECDM (by Bureau)



Source: OIG analysis of CDM Agency Dashboard data, April 26, 2024

Note: 100 percent of BEA's and NIST's systems were mapped to hardware assets, while none of NOAA's systems were. At the time of our fieldwork, NOAA was not reporting security data to ECDM, so we consider this to be a zero mapping.

This gap occurred due to the Department's delay in providing guidance to bureaus on how to associate assets with their respective information systems. Although the Department issued the requirement to identify which information systems an asset resides on, a process known as asset tagging, in December 2022, it did not provide standard operating procedures for asset tagging to the bureaus until February 2024. We asked the Department why the asset tagging standard operating procedure was published 14 months after the Department's initial asset tagging policy, and Department management explained they initially attempted to tag assets using the Department's hardware management tool, but later focused on its new ECDM data integration tool as it made the tagging process easier.

The resulting gap impacts the Department's ability to determine an asset's authorization status, since authorization[14] is inherited from the system when assets are properly

[14] This is a process by which a senior federal official or executive assumes the responsibility of operating an information system and authorizes its use for a specified period. *See* DOC NIST, December 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*,

associated. CISA guidance specifies that not knowing an asset's authorization status could lead to high exposure to cyber threat actions.[15] Department management acknowledged the lack of compliance in this area affects the Department's ability to address issues such as asset discovery, vulnerability management, cyber threat hunting, and FISMA reporting.

Without complete data in these key data fields, the Department cannot readily associate assets with information systems. Because the Department's overall view of risk is tied to the criticality of the information system, not the individual assets, it is essential to understand that relationship. Until the relationship is formed, the Department will have an incomplete picture of risk posed by individual high-risk assets.

B. *ECDM data is unreliable due to collection, transmission, and reporting problems*

To ensure federal agencies have visibility over internal assets, OMB requires[16] that agencies report at least 90 percent of government-furnished equipment through the CDM program. OMB's guidance, in conjunction with various CISA binding operational directives,[17] outlines CDM federal dashboard reporting requirements for security configuration settings and asset discovery frequency.

Collection Data Quality

Our data quality testing revealed substantial issues with the reliability of ECDM asset management data, including missing values and data outside valid time frames (see figure 2).

NIST SP 800-37 Rev. 2. Gaithersburg, MD: DOC NIST. Available online at https://csrc.nist.gov/pubs/sp/800/37/r2/final (accessed July 18, 2024).

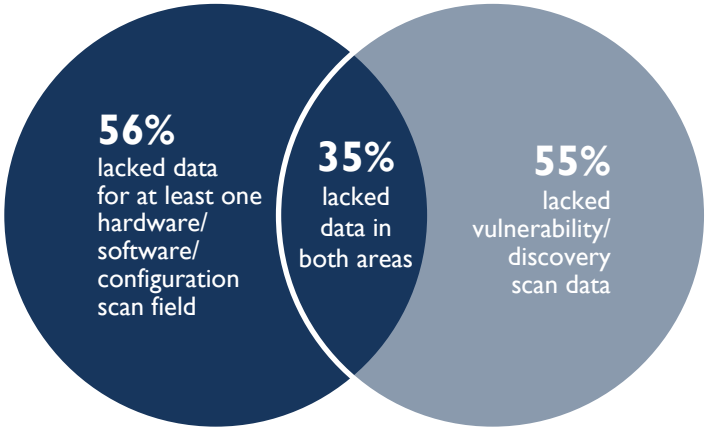
[15] DHS CISA, January 2022. *CDM Asset Management Metrics Development for Ongoing Assessment and Monitoring Guide*, version 3.1. Arlington, VA: DHS CISA.

[16] Office of Management and Budget, December 4, 2023. *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, M-24-04. Available online at https://www.whitehouse.gov/wp-content/uploads/2023/12/M-24-04-FY24-FISMA-Guidance.pdf (accessed June 13, 2024).

[17] A binding operational directive is a compulsory cybersecurity mandate by CISA that states requirements for safeguarding federal information systems and data.

Figure 2. ECDM Asset Management Data Reliability

Of the Department's **117,576** assets:



Source: OIG analysis of Department asset management data, May 7, 2024

Without data for these fields, asset management data within ECDM is not reliable for oversight and provides an incomplete view of system risk. For example, one of the most important aspects of security is identifying and resolving vulnerabilities. However, due to incomplete ECDM cybersecurity data, the Department does not have an enterprise view of vulnerabilities and thus is not able to efficiently track vulnerability resolution.

Outside of our data quality testing, we noted that the National Oceanic and Atmospheric Administration (NOAA), which hosts approximately 30 percent of the Department's IT assets, has not provided its asset management data to the Department's ECDM program. Since those assets make up such a large percentage of the Department's overall assets, this omission significantly impacts data collection quality. NOAA management told us they were hesitant to participate in ECDM until they could verify NOAA's data would be secure and informed us that they are working with the Department to integrate NOAA data into ECDM by the end of FY 2024.

Further, at the time of our audit, we found that the data integration platform could not yet collect and report security configuration data to CISA due to a limitation in the tool. Security configuration data is one of the five main categories of data within asset management, and CISA requires it to be included. Department management acknowledged awareness of this issue and stated that they were working to resolve it. In the meantime, the absence of configuration data poses a significant challenge to cybersecurity data reporting.

Transmission and Reporting Data Quality

ECDM provides data to external reporting tools such as CISA's cyberscope tool for FISMA reporting and the CISA agency dashboard, which feeds the federal dashboard. Our testing found errors in both the Chief Information Office (CIO) FISMA metrics data and agency dashboard data. Combined, these data quality issues affect how external

parties, such as CISA, view the Department's ECDM data and their ability to use that data for oversight.

- In the FISMA data,[18] we found that CISA only sees, on average, about 45 percent of the Department's assets per fiscal quarter through automated ECDM reporting mechanisms—approximately half of OMB's 90 percent reporting threshold. Further, we found data transmission errors in ECDM led to the Department reporting inaccurate asset discovery data in CIO FISMA metrics for at least two fiscal quarters. Additionally, CISA vulnerability dashboards showed no assets were being scanned for vulnerabilities even though internal ECDM data had vulnerability scanning results. The reporting issues we identified were not resolved until we notified staff about them during our testing.
- Our limited follow-up testing confirmed inconsistent asset management data between the internal ECDM system and the agency dashboard.[19] Our testing found examples of hardware, software, configuration, or vulnerability data in ECDM that did not appear in the dashboard.

We notified NIST of the reporting issues. NIST worked with CISA contractors and determined that not all data fields were being fed to CISA. NIST remediated the issue during our fieldwork. However, the Department's ECDM data integration tool could not report secure configuration compliance data to CISA due to system limitations during our testing in May 2024.

Due to the pervasiveness of the data quality issues we identified, we determined that the Department does not have an effective process to review and resolve data quality issues. Although the Department's data integration solution went live in May 2023, our testing continued to find significant data quality issues almost a year later. As a result, we concluded that the Department cannot rely on the ECDM asset management program for accurate Department-level risk analysis and CIO FISMA metric reports do not accurately reflect the Department's cybersecurity posture, limiting CISA's ability to assess and respond to security incidents.

Until quality issues are resolved, the integration solution will not be able to produce reliable data for oversight, reducing the system's usefulness to the government. In FY 2024, the Department and its bureaus spent approximately $2.69 million on licensing, operations, and maintenance costs for the Department's data integration solution (see appendix B). We calculated the $2.69 million by requesting and totaling FY 2024 cost data from the Department and its bureaus. Using that total, and accounting for inflation, we project that the solution will cost the Department approximately $5.6 million over the next 2 years (FYs 2025 and 2026). The Department could use these funds more efficiently by improving data quality.

[18] FISMA requires each agency's Chief Information Officer to report the status and implementation of NIST standards and cybersecurity-related initiatives.

[19] We did not conduct full testing, as the Department is not responsible for the CISA dashboard's implementation.

Recommendations

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

1. Develop and implement oversight mechanisms to manage and track whether bureaus meet hardware asset management, software asset management, configuration security management, and vulnerability management data collection and reporting requirements. Implementing this recommendation will lead to funds being put to better use.
2. Develop and implement oversight mechanisms to ensure Department cybersecurity data reported in the CDM agency dashboard and used in CIO FISMA metric reporting accurately reflects the Department's cybersecurity posture.

II. NIST Does Not Consistently Control and Thoroughly Test the ECDM Program's Information System Changes

The ECDM program relies on its information system (the system) to store, process, and transmit essential cybersecurity data while hosting various types of security software. NIST manages the system on behalf of the Department. As the ECDM program's capabilities expand, its information system must change accordingly. This requires proper management to ensure that system changes are authorized, tested, and implemented in a way that does not disrupt operations or reduce security. This process is called configuration change management. According to the ECDM system security plan, NIST implements its standard configuration change management process for all system changes.[20]

However, during our penetration testing of the system, we encountered several instances where changes were not properly controlled and tested, resulting in reduced security. Specifically, during simulated attacks, we leveraged poorly executed system changes and found two instances where an insider could exploit lapses in the change control process.

The first instance occurred when NIST made a system configuration change that inadvertently provided system users with unauthorized access to the internet. While most internet access is blocked for this system's users, this specific change accidentally allowed much wider internet access. Our penetration testing team noticed this and downloaded additional security tools from the internet. We alerted NIST management, and they promptly corrected the issue. However, this incident demonstrated how a system change without sufficient testing created a vulnerability that allowed us to attack the system.

In a follow-up meeting with NIST management, we determined that this issue arose because of a transition to a new network device that manages user access to the internet. NIST management learned after the transition that the new device processed filtering rules differently than the old one, leading to a conflict that yielded internet access. NIST management stated they had conducted prior planning and testing but did not perform testing in a scenario that integrated all the relevant systems due to technical complexity.

[20] DOC NIST, 2023. *System Security and Privacy Plan* (internal NIST document). Washington, DC: DOC NIST.

When we asked for standard records documenting the change management process, such as requests, testing, and approvals, we found that none existed, and there was no documented evidence of the testing that management described. As a result, we could not verify the nature and extent of the testing or whether the testing had occurred.

In the second instance, we noticed a security-relevant change in the system that occurred without management's knowledge. During testing, our team exploited a weakness and noticed a day later that our testing accounts were restricted from exploiting that same weakness. While blocking real attacks is important, NIST management told us they did not make the account changes and could not prove how they occurred. We found that the account restriction resulted from a change in a security policy. However, NIST management could not determine the source of that change due to a lack of security logs, which are required by Department policy. Without these logs and the information they are intended to provide, it is at least possible that an attacker with system administrator privileges could have made unauthorized changes to the system's server and avoided detection. Further, it is very difficult to determine who made the changes, as no direct accounting is available. In short, in the absence of logs and standard change management documentation, we could not verify who made the change or whether it was authorized.

Additionally, a vulnerability from a September 2023 security assessment was still present and exploitable during our testing, although it was officially marked as resolved in the tracking system. The standard NIST change process required testing to validate whether the vulnerability was successfully remediated. However, the continued existence of the vulnerability demonstrated that this did not occur. We found that validation only occurred on a single computer, instead of NIST validating the removal of the vulnerability across the entire system. Because NIST did not fully verify the remediation, the system continued to be vulnerable to attack.

Based on the results of our testing, we concluded that the security of the ECDM program's information system was reduced when NIST did not properly control and thoroughly test changes. Two instances we identified during testing directly led to us performing additional system exploitation, such as elevating our user permissions. In a real attack scenario, such lapses in change management could provide an attacker with additional resources to compromise the system.

Recommendations

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

3. Design and implement a technical control to prevent changes to the production environment without proper configuration change control processes and testing.
4. Implement logging for the security policy changes identified by our testing.

III. The ECDM Program's Information System is Relatively Secure but Has Some Internal Security Weaknesses

NIST has effectively reduced external access to the ECDM program's system, restricting an attacker's ability to move from the internet to the internal network. Further, over the last year, NIST has implemented several changes that made the internal footprint of the system more secure by strengthening user access controls in the Virtual Desktop Infrastructure (VDI),[21] enhancing external defenses, refining privilege management for significant accounts, and integrating advanced incident response tools. However, our penetration testing demonstrated there are still areas of weakness. Those weaknesses allowed a user to gain control of system administrator-level accounts for the VDI servers and hosts, which serve as the foundation for user access and interaction with the system.

A. The ECDM program's information system is relatively secure from an external perspective and effectively limits access

The ECDM program's *System Security Privacy Plan* states that the system is limited to internal Department connections. Our testing found that external access is limited as intended. Our scans did not connect to the system from any points other than the allowed locations. We did identify some open-source information about the system through internet searches. While this information may be useful to an adversary, we assessed that it was not notably sensitive.

B. We gained full control of ECDM's VDI environment through system administrator privileges

FISMA mandates that agencies (1) ensure information security measures align with the risks and potential harm and (2) implement essential security controls, periodic reviews, and timely remediation of vulnerabilities.

After verifying the system's external security controls, we performed internal penetration testing to determine if the system implemented essential security controls internally. Our testing simulated attacks used by real-world adversaries, such as exploiting vulnerabilities and taking advantage of security misconfigurations. NIST was aware of our testing and provided us with accounts, allowing us to access the system like a typical user. From there, we leveraged a series of vulnerabilities in the system to escalate access privileges to those of a system administrator and ultimately a VDI administrator.

First, we identified two methods of escalating our system access from a standard user to a system administrator.

1. A redundant but still-active system administrator account using older and weaker security policies had excessive system permissions. We identified an account with an older password policy that made it susceptible to a password

[21] VDI is a virtual desktop that users can connect to and interact with as if they were using a physical desktop computer. It allows users to work in a remote environment. *See* Citrix. *What is VDI?* Available online at https://www.citrix.com/glossary/what-is-vdi-virtual-desktop-infrastructure.html (accessed July 16, 2024).

guessing attack. Rather than delaying testing on performing the guessing attack, we agreed with NIST management that the account was vulnerable, and they provided us with the password to assume the identity and privileges of the system administrator.

2. A second attack was possible through outdated software with known security weaknesses. Specifically, one weakness allowed us to gain access to other users logged into the system at the same time. From there, we would wait for a system administrator to log into the system.

Once either of these attacks was successful, we used a third attack to impersonate any other user or administrator accounts (except for the more powerful administrator accounts noted below). The VDI system administrator had the ability to control the VDI environment, which is the primary environment where users interact with the system. While using the VDI system administrator account, we managed security settings, servers, hosts, and local users within the VDI environment. However, recent security improvements implemented by NIST limited access to other parts of the system and to more powerful administrator accounts. Due to those improvements, we were unable to modify other computers outside of the VDI environment.

Overall, our internal penetration testing efforts identified 11 security weaknesses of varying severity. Vulnerabilities discovered during penetration testing can be categorized as having low, medium, high, or critical impact, depending on their level of risk to the affected system. This categorization helps prioritize remediation efforts, with critical impact potentially being the most harmful and requiring priority remediation (see table 1).

Table 1. ECDM System Security Weaknesses

Severity	Count
Critical	1
High	7
Medium	1
Low	2

Source: OIG analysis of ECDM system penetration test report, May 20, 2024

We provided Department and NIST management with a detailed technical report to help them understand the security issues and take appropriate action. In a subsequent meeting, management indicated that they are already addressing the weaknesses.

Our testing revealed security lapses where general users accessed restricted functionalities due to poorly implemented controls. Insufficiently restricted user access, alongside outdated configurations and software, allowed an insider to escalate their privileges to a system administrator level, taking control of the VDI environment. If

unaddressed, these vulnerabilities pose a threat, potentially compromising the confidentiality, integrity, and availability of the ECDM program's VDI system.

Recommendation

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

5. Review our detailed technical report and develop and implement a corrective action plan to resolve the issues we identified in our penetration testing.

IV. Deficiencies in ECDM Program Management Place Future Enterprise Cybersecurity Tool Deployments at Risk

ECDM continues to expand as the Department procures new enterprise-wide cybersecurity capabilities.[22] This requires mature program management to reduce costs, meet deployment deadlines, ensure bureau operational needs are met, and deliver on expected outcomes. Improvements to ECDM program management processes will impact current and future capability deployments. We performed a case study of the procurement and deployment of ECDM's latest capability to determine the effectiveness of ECDM program management processes. Our case study focused on whether the Department met its deployment deadlines and cost estimates and included gathering feedback from Department bureaus, analyzing cost data, and reviewing the current state of the new ECDM capability against the Department's objectives.

Executive Order 14028[23] and OMB Memorandum 22-01[24] required federal agencies to select and implement an endpoint detection and response (EDR) capability to proactively detect cybersecurity incidents and support incident response while ensuring sufficient resources, staffing, and compliance with privacy and statistical laws. In response, the Department's December 2022 CDM memo required bureaus to implement the Department's new EDR capability by the end of FY 2023, effectively giving the bureaus 9 months for implementation. Additionally, the Department's *Commerce Acquisition Manual* requires managers of programs between $10 million and $75 million to hold the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) level 1 certification

[22] The Department's ECDM program will expand to incorporate new capabilities delivered by CISA's CDM program and meet new federal cybersecurity mandates from CISA and OMB.

[23] The White House, May 12, 2021. *Executive Order on Improving the Nation's Cybersecurity*. Available online at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed May 23, 2024).

[24] OMB, October 8, 2021. *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, M-22-01. Available online at https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf (accessed May 23, 2024).

to support Department programs and acquisitions with adequate plans, procedures, and best practices.[25]

Missed Deployment Deadlines

We found that the Department encountered challenges during the enterprise-wide EDR capability selection and deployment. After the Department announced its selection, three bureaus—accounting for approximately 40 percent of the Department's information systems—submitted requests to be excluded from implementing the new capability. Several Department bureaus, including the three that requested waivers, had already implemented EDR capabilities of their own by the time the Department announced its enterprise solution. Further, the exclusion requests and feedback we received from Department bureaus explained why the bureaus had concerns about the Department's enterprise-wide EDR capability:

- NOAA had a significant number of high-impact information systems, and at the time of NOAA's exclusion request, the Department's capability was not authorized to operate for high-impact systems. It did not have an authorization to operate for high-impact systems until October 2023—10 months after the Department directed the bureaus to use its enterprise solution.
- The U.S. Census Bureau cited legal protections from providing statistical data to law enforcement agencies–DHS, in this case—and concerns about introducing complications and excessive access to its systems.
- The International Trade Administration (ITA) used another EDR solution and had not broadly deployed the Department's EDR due to functionality gaps.
- The Bureau of Industry and Security (BIS) manages high-impact information systems and planned to evaluate the Department's enterprise EDR solution before deciding on a full transition. BIS also noted the Department's solution lacked a security capability included in BIS' previous EDR. BIS had to deploy an additional security tool to cover the loss.
- The United States Patent and Trademark Office (USPTO) retains independent control and responsibility over protecting its assets due to statutory and Department Organization Order protections and did not plan to deploy the Department's enterprise-wide EDR capability. USPTO asserts it is not required to participate in enterprise-wide offerings and already had its own EDR capability in place.

We also found that, in response to a CISA data call in May 2021, the Department did not identify any challenges or barriers to an enterprise EDR adoption. However, barriers and

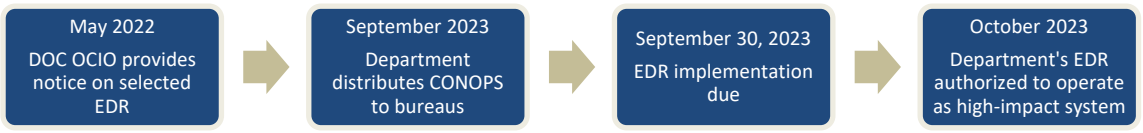
[25] DOC, January 2023. *Commerce Acquisition Manual 1301.671, Department of Commerce Program and Project Manager Certification Program*. Washington, DC: DOC, 5. Available online at https://www.commerce.gov/sites/default/files/2023-01/Revised%20CAM%201301.671_vF.pdf (accessed May 15, 2024). According to the manual, level 1 program and project managers should have "general understanding of project management practices, including risk management, budgeting, scheduling, technology management, performance-based business practices, cost management, stakeholder relations, program control and governance."

challenges the Department faced in adopting an enterprise-wide EDR capability led to missed deployment milestones. By the Department's deployment deadline of September 30, 2023, four bureaus,[26] accounting for approximately 71 percent of the Department's information systems, had not deployed the Department's EDR capability. CISA had vetted and approved the bureaus' EDR capabilities, but CISA and the Department both preferred an enterprise-wide approach instead of several EDR solutions for the bureaus. Until a unified EDR solution—which also addresses the Census Bureau's unique requirements—is in place, the Department will face obstacles in responding quickly to an active cyberattack because it will need to query multiple tools across the bureaus.

Project Planning, Cost Tracking, and Communication

We also found the Department did not follow its own best practices in program management when selecting and deploying its enterprise-wide EDR capability. One of the best practices the Department's project management guidance describes[27] is the drafting of a concept of operations (CONOPS) document. The CONOPS describes the operational view of a proposed capability from the user's perspective. It is a critical early project planning document and a key step in gathering and communicating input from stakeholders and end users. The Department did not share a draft CONOPS with the bureaus until September 2023—the same month as the EDR deployment deadline and approximately 18 months after the Department finalized its EDR capability selection (see figure 3).

Figure 3. Timeline of EDR



Source: OIG analysis

The Department cited non-communication from several bureaus as an ongoing challenge, and the bureaus in turn described communication issues with the Department during EDR selection and deployment. We faced similar issues when we requested EDR cost data. We issued several data calls to the Department during a 4-month period and encountered difficulties in obtaining accurate, thorough, and timely responses—difficulties that we attribute to project management weaknesses.

Another best practice in the Department's project management guidance is to develop a life cycle cost estimate to ensure funding stability, as budgets formed without proper cost estimates may not accurately assess affordability and the impact of changes. In line with an existing Department best practice to develop life cycle costs during planning, OMB directed the Department to confirm its enterprise-wide EDR capability has sufficient funding to maintain the capability through its lifespan. The Department's EDR cost analysis did not,

[26] NOAA, the Census Bureau, USPTO, and ITA.

[27] DOC, October 5, 2023. *DOC Acquisition Program and Project Management Guidebook*. Washington, DC: DOC. Available online at https://www.commerce.gov/sites/default/files/2023-05/Guidebook%20v.%202.0_2023-03-29%20-%20FINAL%20%284%29.pdf (accessed May 15, 2024).

however, include a comprehensive life cycle cost estimate or an assessment of each bureau's needs. We also learned the Department's OCIO does not budget for lifespan costs, but rather for the FY.

To date, the Department's EDR has cost the Department and CISA more than $4 million, excluding duplicative costs from bureau EDR solutions. Although the Department could not provide a comprehensive life cycle cost analysis, we were able to obtain cost data and perform our own analysis. We determined that the Department's initial $3.7 million estimated cost for its 119,000 total endpoints[28] did not account for delayed implementation of the EDR. Using FY 2024 actual costs, the total to cover all endpoints would have been approximately $5.2 million, or $1.5 million more than estimated in April 2022 (see table 2).

Table 2. Department EDR Costs

	Initial Estimate (April 2022)	FY 2024 (Actual)[a]	FY 2025 (Expected)
Number of Covered Endpoints	119,000	50,000	79,000
Cost	$3.7 million	$2.1 million	~$3 million
Cost for 119,000 endpoints	$3.7 million for 119,000	~$5.2 million for 119,000 (calculated)	~$4.6 million for 119,000 (calculated)

Source: OIG analysis of cost estimates and invoices provided by the Department

[a] This assumes the Department does not incur additional EDR procurement costs in the fourth quarter of FY 2024.

Based on the results of our case study, we found that the Department did not follow the Office of Acquisition Management's (OAM's) project management best practices, such as producing life cycle costs and generating a CONOPS early in planning.[29] When we asked the Department about using OAM's project management guidebook for the ECDM program, the Department stated that this was not a requirement because the procurement contracts for ECDM capabilities are managed by CISA, and the ECDM program does not meet the cost threshold that would require use of the guidebook. However, OAM staff told us they recommend all Department programs follow the guidebook's best practices for program management. Additionally, the program was not overseen by someone with the appropriate FAC-P/PM level 1 certification,[30] which helps to ensure effective management of the Department's assets. The Department requires the program manager of any Department program that costs between $10 million and $75 million to hold a FAC-P/PM level 1 certification. As the Department's annual ECDM program budget was $16.1 million—before the addition of an enterprise-wide EDR capability—it should have had an appropriately

[28] Endpoints include networked computing devices such as workstations, mobile phones, and servers.

[29] DOC *Guidebook*.

[30] The Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) is for acquisition professionals in the government performing program and project management activities and functions. See Federal Acquisition Institute. *Program and Project Managers (FAC-P/PM)*. Available online at https://www.fai.gov/certification/fac-ppm (accessed May 24, 2024).

certified program manager. We reached out to Department personnel and confirmed no one managing the ECDM program holds the FAC-P/PM level 1 certification.

In short, we determined that the Department needs improved program management that effectively identifies challenges and considers the needs of stakeholders. Using best practices, such as producing life cycle costs to help demonstrate long-term value and generating a CONOPS earlier in the process to engage with stakeholders, may have helped to address the bureaus' concerns and prompt more cooperative engagement. In particular, that engagement may have enabled the Department to identify and potentially address the specific technical and organizational concerns that NOAA, BIS, USPTO, and the Census Bureau articulated. It may have also enabled better coordination with those bureaus that had separate CDM programs in place. Instead, as of May 2024:

- Four bureaus have not deployed the Department's solution.
- Two bureaus do not currently plan to deploy the Department's EDR solution and will continue to use their existing EDR solutions.
- Three bureaus incurred duplicate EDR tool costs because they are, or will be, operating the Department's solution in addition to their own EDR solutions.
- One bureau plans to transition to the Department's solution by the end of FY 2025 at the earliest for most endpoints and will incur its own EDR costs until the transition is complete.

Recommendation

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

6. Incorporate OAM's project management best practices into the ECDM program and ensure program and project managers overseeing the ECDM program obtain a FAC-P/PM level 1 certification.

V. The Department Does Not Fully Incorporate Bureau-incurred Costs in Its ECDM Project Cost Tracking

According to an OMB memo,[31] "Chief Financial Officers Act of 1990[32] agencies are responsible for the operations and maintenance costs of their CDM-related tools and capabilities and are required to submit separate, CDM-specific line items in their annual budget documents." The Department's 2022 CDM memo[33] emphasizes the importance of leveraging cost-saving opportunities presented by CISA to support enterprise-wide solutions amid fiscal constraints. Additionally, the Department's information security

[31] OMB, M-24-04.

[32] Public Law No. 101-576. This act gave OMB new authority and responsibility for directing federal financial management, modernizing the government's financial management systems, and strengthening financial reporting. There are 24 agencies that fall under this act, including the Department.

[33] DOC, *Required Actions*.

policies mandate that bureaus implement ECDM tools, such as vulnerability scanning and EDR, as prescribed by the Department.

We reviewed the CDM budget information and found that it incorporated bureau costs only to the extent that they were included as part of the centralized funding pool, called the working capital fund. The ECDM program director and OCIO budget team stated that other than the cost of NIST hosting services, the Department does not track bureau-incurred ECDM costs. However, the ECDM program architecture requires bureaus to manage and operate ECDM tools in their environments. As such, those costs would constitute operations and maintenance—which, according to OMB guidance, should be included in the CDM-specific budget line items.

To estimate bureau-incurred costs, we requested ECDM-related cost data from the bureaus. Seven bureaus tracked those costs and provided them to us. Based on bureau responses, total costs were approximately $2.54 million in FY 2024. Variations in how each bureau tracks ECDM costs and responded to our request means the data may not represent a complete picture. However, the bureau-incurred costs equate to approximately 14 percent in additional ECDM costs ($2.54 million above the Department's tracked ECDM program costs of $16.1 million) that the Department does not track. The Department reasoned that since bureaus make their own decisions on how to best tailor ECDM capabilities in their environment, bureau-incurred costs are separate from those for the Department's ECDM program.

As a result, the Department's efforts to report ongoing CDM-related costs are incomplete. This limits the Department's ability to measure whether the ECDM program produces the intended cost savings.

Recommendation

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

7. Design and implement a process to track and report bureau-incurred ECDM program costs for improved cost reporting and analysis of cost-saving opportunities.

Summary of Agency Response and OIG Comments

On November 8, 2024, we received the Department's response to our draft report. In response to our draft report, the Department generally concurred with our recommendations and described the actions the Department and NIST have taken, or will take, to address them.

The Department also provided technical comments from NIST. The first and second comments provided information on a network device transition and a statement from NIST management on the technical complexity of the ECDM information system. We made changes to the report in those areas.

The third comment related to a lack of change request documentation and audit logs for the network device transition. Specifically, management disagreed with our conclusion that none existed. While we acknowledge that NIST's technical comments provided additional context, we reviewed the cited documents during our fieldwork and concluded that our finding required no modifications, as the documents did not address the issues we identified.

The fourth comment related to security changes made in the information system we reviewed. Specifically, NIST took exception to our assessment of its state of knowledge regarding the source of the changes and what could be determined from existing logs. Further, NIST asserted that this was a logging issue, not a change control issue, because the change was automated application activity (which is not a change management event). However, NIST's discussion of these issues does not fully address the aspects of the change that prompted our concern. In particular, the automated portion of the change happened *after* a security change that had to be initiated by a system administrator. That security change is a change management event. This is significant because our finding focuses on a system administrator's ability to make configuration changes without attribution. As we described in finding II, our testing verified this was possible. As we also discussed previously, the logs NIST cited showed that a change occurred but only logged that the system made the change, not the specific user account responsible. While NIST's logging capabilities were robust, its audit logs did not capture the event we described. In addition, NIST was unable to provide us with standard change management documentation related to the original source of the change. This information is critical to attributing an action to a user. While NIST's technical comments provided additional context, we determined that no changes to the final report were needed.

Appendix D contains the full text of the Department's response and NIST's technical comments. We are encouraged by the Department's efforts to improve its ECDM program, and we look forward to reviewing its action plan for implementing our recommendations.

Appendix A: Objective, Scope, and Methodology

Our audit objective was to assess the effectiveness of the Department's ECDM program. To accomplish our objective, we performed the following actions:

- Interviewed ECDM program and Department leadership, bureau leadership, DHS technical integrators, ECDM system security staff, and administrative staff.
- Analyzed Department and bureau records related to:
    - ECDM's enterprise cybersecurity capabilities.
    - The Department's procurement of an EDR tool.
    - The ECDM program's information system security documentation.
- Reviewed Department and bureau compliance with the following applicable internal policies, provisions of law, and mandatory guidance:
    - The Department's *Enterprise Cybersecurity Policy* and related handbooks
    - The Department's memo on CDM reporting requirements: *Required Actions in Support of the Department's Continuous Diagnostics and Mitigation Program and Automated Reporting Requirements*, December 2022
    - CISA *Binding Operational Directive 22-01*
    - CISA *Binding Operational Directive 23-01*
    - OMB *Memorandum M-24-04*
    - OMB *Memorandum M-22-01*
- Analyzed cybersecurity data found in the Department's ECDM integration layer and agency dashboard.
    - To determine how well ECDM tied Department assets to FISMA boundaries, we mapped devices accounted for in ECDM to the Department's official FISMA-reportable system inventory. We reviewed all the Department's 13 bureaus (the Office of the Secretary hosts the IT infrastructure for the Minority Business Development Agency, the U.S. Economic Development Administration, and the Office of the Under Secretary for Economic Affairs):
        - the Bureau of Economic Analysis,
        - BIS,
        - the Census Bureau,
        - ITA,
        - NIST,
        - NOAA,

  - the National Telecommunications and Information Administration,
  - the U.S. National Technical Information Service,
  - the Office of the Secretary, and
  - USPTO.
- Performed penetration testing of the NIST-hosted ECDM information system.

Our review of internal security controls fell into the Control Environment, Risk Assessment, Control Activities, and Monitoring components defined in the U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*.[34]

We employed a comprehensive methodology to review internal and external IT security requirements within the context of our audit objective to determine the effectiveness of the Department's ECDM program. Our work was broken down into the following sub-objectives:

- Sub-Objectives A and B: to determine whether the ECDM program's asset management capabilities meet program operations and reporting requirements, we performed data reliability testing on asset management data in the ECDM data integration layer and the Department's CDM dashboard and performed a cost analysis of the Department's data integration solution.
- Sub-Objective C: to determine the trustworthiness of the ECDM information system, we conducted security penetration testing of the ECDM program's information system.
- Sub-Objective D: to determine whether ECDM program management meets CISA requirements and supports the Department's cybersecurity strategy, we conducted a case study of the Department's enterprise EDR tool, the most recent security tool purchase made under the program, and analyzed ECDM program cost data, including a request to Department bureaus for ECDM-related costs.

We conducted our audit from October 2023 through October 2024 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 performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[34] U.S. Government Accountability Office, September 2014. *Standards for Internal Control in the Federal Government*, GAO-14-704G. Washington DC: GAO. Available online at https://www.gao.gov/assets/gao-14-704g.pdf (accessed July 6, 2023).

Appendix B: Potential Monetary Benefits

The table below presents the estimated costs of the ECDM program for FYs 2025 and 2026. Implementing recommendation 1 will enable the Department to better utilize the cybersecurity data collected via ECDM, putting these funds to better use.

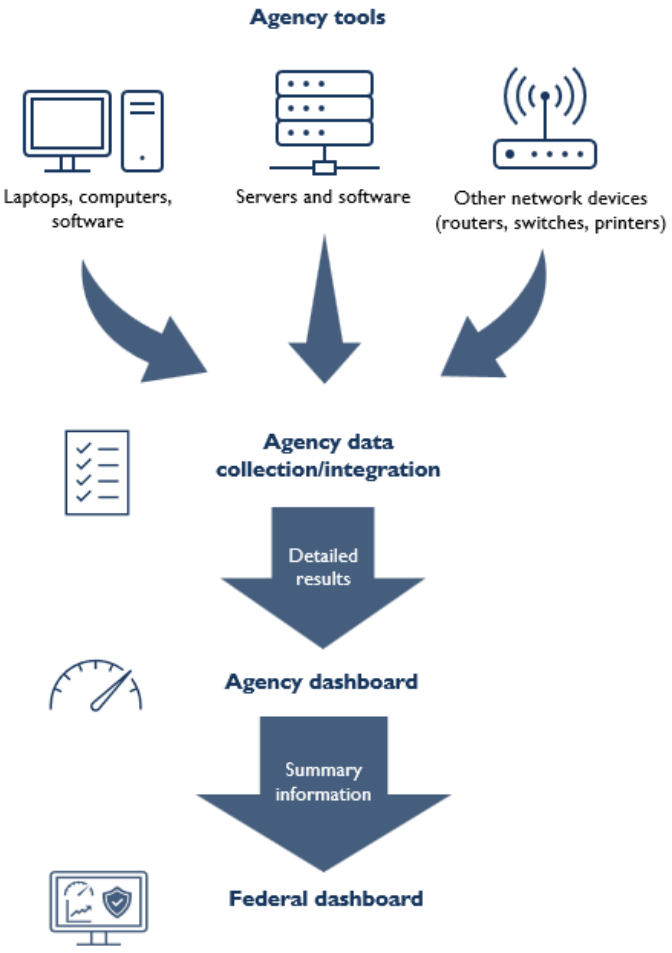
Finding and Recommendation	Questioned Costs	Unsupported Costs	Potential Funds to Be Put to Better Use
Finding 1 and **Recommendation 1**	$0	$0	$5,619,299.88

Source: OIG analysis of Department and bureau cost data

Appendix C: CISA CDM Program Data Layers

As depicted in figure C-1, automated tools send information they have collected about hardware devices, including any associated software, connected to an agency's network to a collection point that compares the information with expected outcomes, such as whether actual device configuration settings meet agency or federal core benchmarks. The results of these comparisons are then sent to an electronic visual display at an agency, referred to as the agency dashboard. The agency dashboard summarizes the information and sends it to a federal dashboard that is managed by CISA. The federal dashboard includes summary information about the security of agencies' networks.

Figure C-1. CISA CDM Program Data Flow



Source: Adapted from CDM Data Model Document, Version 4.1.1

Appendix D: Agency Response

The Department's response and NIST's technical comments begin on the next page.

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

MEMORANDUM FOR: Jill Baisinger
Acting Inspector General

FROM: Brian Epley GARY HANEY Digitally signed by GARY HANEY Date: 2024.11.08 14:20:33 -05'00'

SUBJECT: The Department of Commerce Concurrence on the Office of Inspector General Draft Report, *Data Quality Challenges and Ineffective Program Management Hinder the Department's Enterprise Cybersecurity Capabilities* (October 9, 2024)

We appreciate that the Office of the Inspector General (OIG) presented the Department of Commerce (DOC) with an opportunity to review the draft report, *Data Quality Challenges and Ineffective Program Management Hinder the Department's Enterprise Cybersecurity Capabilities* (October 9, 2024).

The DOC Office of the Chief Information Officer (OCIO) reviewed the draft report and generally concurs with the findings and recommendations. The Department appreciates OIG's support in protecting our mission and critical information systems by identifying strengths and weaknesses in our security controls. The DOC OCIO recognizes the need to increase visibility and insight, address gaps in people, processes, and technology, and reduce overall risk.

Should you have any questions, please contact Ryan A. Higgins at (202) 868-2322 or RHiggins@doc.gov.

Attachments

cc: MaryAnn Mausser
Joselyn Bingham
Aditi Palli
Ryan Higgins
Lateef Gbadegesin
Maria Hishikawa
Shavon Moore

Department of Commerce Technical and Editorial Comments
on the OIG Draft Report: *Data Quality Challenges and Ineffective Program Management Hinder the Department's Enterprise Cybersecurity Capabilities*
(OIG-24-472, October 9, 2024)

The Department of Commerce has reviewed the draft report and we offer the following comments for OIG's consideration. Page numbers refer to page numbers in the draft report unless otherwise stated.

NIST

General Comments

Page 11, Paragraph 3, No changes, however NIST has completed and verified the remediation of this finding.

Page 11, Paragraph 4, "Design and implement a technical control to prevent changes to the production environment without proper configuration change control processes and testing." NIST has reviewed all products in the ECDM environment. Only one offers a technical control which requires the sign off of a second administrator before Commerce wide changes can be implemented. This control is already implemented. All other products do not offer any comparable technical control.

NIST is recommending instead, that staff take a refresher training on the NIST Change Management Process, review use of standard change controls, and establish procedures for minimum testing documentation.

Page 11, Paragraph 4, Nearly all items from the technical report are resolved. The remaining are being actively worked on and will be tracked in a POA&M.

Recommended Changes for Factual/Technical Information

Page 10, Paragraph 7, "In a follow-up meeting with NIST management, we determined that this issue arose due to **what we found to be a rushed transition** to a new network device that manages user access to the internet." Recommend replacing, "what we found to be a rushed transition" with "an emergency change due to a failing network device". The prior network device was failing. The alternatives were to either completely remove the failing device, providing no access restrictions or move to a known performant device, understanding there might be untested scenarios. A risk managed decision was made to move forward, accepting the risk that we would be able to monitor and correct any issues, while still providing some level of access restriction to this high impact system.

Page 10, Paragraph 7, "NIST management stated they had conducted prior planning and testing but did not perform testing in a scenario that integrated all the relevant systems." Recommend adding "as that is not technically possible due to the complexity of the system", as that was the complete statement that NIST management made.

Page 11, Paragraph 1, "asked for standard records documenting the change management process, such as requests, testing, and approvals, **we found that none existed, and there was no documented evidence of the testing that management described**. As a result, we could not verify the nature and extent of the testing or whether the testing had occurred." The bolded statement is inaccurate, recommend replacing with ". A formal approved Change request CHG0052764 for the implementation of the new device in the environment was provided. The impacting change in the prior paragraph, was due to staging of an upcoming general (non-ECDM) change. Audit logs of that activity were also provided. Staging a content for a future change does not require a change ticket, per the OISM Change Management policy. As you identified on Page 9 Paragraph 10, "the new device processed filtering rules differently than the old one, leading to a conflict that yielded internet access", the risk of this type of issue was part of the accepted risk of implementing the new device. Due to your notification, the issue was corrected in less than a business day and has not recurred due to better understanding of the new device.
Testing is performed by staff subject matter experts, and is often done in meetings. NIST management is examining our change management policies to determine what would be sufficient documentation of evidence of testing for changes.

Page 11, Paragraph 2, "*"In the second instance, we noticed a security-relevant change in the system **that occurred without management's knowledge***. During testing, our team exploited a weakness and noticed a day later that our testing accounts were restricted from exploiting that same weakness. **While blocking real attacks is important, NIST management told us they did not make the account changes and could not prove how they occurred***. We found that the account restriction resulted from a change in a security policy. However, **NIST management could not determine the source*** of that change due to a lack of security logs, which are required by Department policy. **Without these logs and the information they are intended to provide, it is at least possible that an attacker with system administrator privileges could have made unauthorized changes to the system's server and avoided detection**. Further, it is very difficult to determine **who*** made the changes, as no direct accounting is available. In short, **in the absence of logs and standard change management documentation***, we could not verify **who*** made the change or whether it was **authorized.***"*

Specific misleading language

The bolded statements are inaccurate. These are not a change control issue; but an audit issue. During the audit, NIST asserted that application native functionality was making the system changes. NIST later confirmed with the vendor that this was typical application functionality and provided OIG this response. NIST also provided OIG the EDR reporting on the registry key changes which directly impacted the OIG pentester. OIG cited the EDR product results report in the internal technical report which described the audit finding. Based on the evidence provided from the vendor this was automated application activity, which is not a change managed event.

NIST provided evidence that the EDR product did capture the activities in question. These events are captured and provided to DOC ESOC, and DHS CISA Threat Hunting teams. While a specific audit event was not configured, the activity was captured and is reviewable by NIST, DOC, and DHS CISA teams. "We request the removal of "*it is at least possible that an attacker with system administrator privileges could*

have made unauthorized changes to the system's server and avoided detection" and are visible to threat hunting teams across the Federal Civilian government.

NIST requests either the removal of the whole paragraph or the bolded statements and a rephrasing to identify this as an audit issue based on the evidence that was provided. Automated application specific registry and filesystem changes are not human controlled events and are not subject to change management.

NIST is implementing additional audit logging and reviewing whether the additional logs or the EDR logs are a more effective location to identify malicious activity.