Capstone Report: Effective Reviews Are Needed to Enhance the Security Posture of the Department's Active Directories

FINAL REPORT NO. OIG-23-013-A

March 08, 2023

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

Report in Brief

March 08, 2023

Background

The U.S. Department of Commerce (the Department) and its bureaus are required to comply with federal law to secure information technology (IT) systems through the cost-effective use of managerial, operational, and technical controls.

Active Directories—critical components of IT infrastructure—maintain logical structures, known as domains, to manage network resources, including network users, workstations, servers, printers, databases, and system configurations. Across the Department, there are more than 100 Active Directory installations of varying sizes. Active Directories contain sensitive information.

We previously conducted audits of Active Directories at three Department bureaus: United States Patent and Trademark Office, Census Bureau, and National Oceanic and Atmospheric Administration. We found similar deficiencies at all three bureaus, resulting in Active Directories being susceptible to cyberattacks.

Although each bureau has since taken action to implement our recommendations, we are publishing this capstone report to better inform the Department of the recurring issues we observed in these audits.

Why We Did This Review

Our objective was to identify the remaining Department Active Directories, which have not been reviewed by the Office of Inspector General (OIG), and summarize past OIG work related to the management of Active Directories.

OFFICE OF THE SECRETARY

Capstone Report: Effective Reviews Are Needed to Enhance the Security Posture of the Department's Active Directories

OIG-23-013-A

WHAT WE FOUND

We found the following:

I. A lack of adequate Active Directory security reviews caused similar issues across multiple Department bureaus.

II. The Department does not have a policy for regular Active Directory security reviews.

Additionally, we noted that bureau Active Directories were using outdated password settings that conflict with zero trust requirements (we discuss this in an "Other Matter" section of the report).

WHAT WE RECOMMEND

We recommend that the Deputy Secretary of Commerce:

1. Direct the Department's Chief Information Officer to establish a Department-wide policy for periodic reviews of Active Directories to include frequency of review and use of specialized tools.

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

March 08, 2023

MEMORANDUM FOR: Don Graves
Deputy Secretary of Commerce

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

SUBJECT: *Capstone Report: Effective Reviews Are Needed to Enhance the Security Posture of the Department's Active Directories*
Final Report OIG-23-013-A

Attached for your review is the final report on our audit of the U.S. Department of Commerce's (the Department's) Active Directories. Our audit objective was to identify the remaining Department Active Directories, which have not been reviewed by the Office of Inspector General (OIG), and summarize past OIG work related to the management of Active Directories. To address this objective, we summarized three of our previous audits concerning the United States Patent and Trademark Office, Census Bureau, and National Oceanic and Atmospheric Administration. We also issued a survey to the Department's bureaus to determine whether they operated Active Directories, and if so, whether they had policies for regular Active Directory security reviews.

We found that a lack of adequate Active Directory security reviews caused similar issues across multiple Department bureaus and that the Department does not have a policy for regular Active Directory security reviews.

Additionally, we noted that bureau Active Directories were using outdated password settings that conflict with zero trust requirements and discuss this in an "Other Matter" section.

In response to our draft report, the Department generally concurred with our findings and recommendation. The Department's response, including technical comments, is included in appendix B.

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

NOTICE: Pursuant to Pub. L. No. 117-263, Section 5274, non-governmental organizations and business entities specifically identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Any response must be submitted to Dr. Ping Sun, Director for IT Security at PSun@oig.doc.gov and OAE_Projecttracking@oig.doc.gov within 30 days of the report's publication date. The

response will be posted on our public website. If the response contains any classified or other non-public information, those portions should be identified as needing redaction in the response and a legal basis for the proposed redaction should be provided.

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

Attachment

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

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

The U.S. Department of Commerce (the Department) and its bureaus are required to comply with federal law to secure information technology (IT) systems[1] through the cost-effective use of managerial, operational, and technical controls.

Active Directories[2]—critical components of IT infrastructure—maintain logical structures, known as domains,[3] to manage network resources, including network users, workstations, servers, printers, databases, and system configurations, as illustrated in figure 1. Across the Department, there are more than 100 Active Directory installations of varying sizes.

Figure 1. The Concept of Active Directory

Source: OIG

Active Directories contain sensitive information, such as users' credentials and network topologies,[4] and authenticate access to mission-critical applications. Therefore, Active Directories are prime targets for cyber attackers. If attackers gain control of an Active Directory, they have near total access to the IT infrastructure and can perform malicious activities to compromise and disrupt organizations' missions, systems, and operations. Further, attackers can also leverage such access to remain undetected, while gradually stealing confidential information over an extended period.

[1] Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551, et seq., defines a framework of guidelines and security standards to protect government infrastructure.

[2] *Active Directory* is a proprietary product from Microsoft. Our work did not examine other directory software.

[3] A *Domain* is a networked group of users, workstations, servers, printers, software applications (for example, databases and websites) as well as other network devices. Everything within the domain is controlled by the Active Directory.

[4] A *network topology* describes or shows how computers or network devices are connected to each other.

We previously conducted audits of Active Directories at three Department bureaus: United States Patent and Trademark Office (USPTO),[5] Census Bureau (Census),[6] and National Oceanic and Atmospheric Administration (NOAA).[7] We found similar deficiencies at all three bureaus, resulting in Active Directories being susceptible to cyberattacks. Unaddressed security deficiencies like those we observed can lead to the exploitation of systems as shown by the Colonial Pipeline hack using the DarkSide ransomware. In this attack, hackers were able to gain unauthorized remote access to a U.S. pipeline system and disrupt access to fuel across the East Coast.

Although each bureau has since taken action to implement our recommendations, we are publishing this capstone report to better inform the Department of the recurring issues we observed in these audits.

[5] U.S. Department of Commerce (DOC) OIG, June 13, 2019. *Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk,* OIG-19-014-A. Washington, DC: DOC OIG.

[6] DOC OIG, January 7, 2021. *Fundamental Security Safeguards Were Not In Place to Adequately Protect the IT Systems Supporting the 2020 Census,* OIG-21-018-A. Washington, DC: DOC OIG.

[7] DOC OIG, February 3, 2022. *NOAA Inadequately Managed Its Active Directories That Support Critical Missions,* OIG-22-018-A. Washington, DC: DOC OIG.

Objective, Findings, and Recommendation

Our objective was to identify the remaining Department Active Directories, which have not been reviewed by the Office of Inspector General (OIG), and summarize past OIG work related to the management of Active Directories. To accomplish our objective, we summarized our previous three audits at USPTO, Census, and NOAA. We also issued a survey to the Department's 11 bureaus[8] to determine whether they operated Active Directories and, if so, whether they had policies for regular Active Directory security reviews. See appendix A for a full description of our scope and methodology.

We found that a lack of adequate Active Directory security reviews caused similar issues across multiple Department bureaus and that the Department does not have a policy for regular Active Directory security reviews. Without effective security reviews, deficiencies will likely continue to exist within the Department, providing threat actors with additional potential attack paths to undermine the sensitive data and applications that are supported by Active Directories.

I. A Lack of Adequate Active Directory Security Reviews Caused Similar Issues Across Multiple Department Bureaus

In our proactive efforts to ensure that the Department and its bureaus are properly securing Active Directories, we conducted a series of targeted audits using specialized methodologies and assessment tools. Within the past 4 years, we examined USPTO's Active Directory, and most recently examined those of Census, and NOAA. In each of these reports, we made similar recommendations.

Although each bureau managed its Active Directories independently, we identified and reported common issues among them. Most notably, each bureau had accounts with management issues and excessive privileges, which adversaries could potentially leverage for lateral movement.[9] To comply with the principle of least privilege,[10] a user's privileges should be restricted to only those required by their roles and responsibilities.

USPTO (June 2019)

Our first audit utilized an open-source tool to determine whether USPTO adequately managed its Active Directory to protect mission critical systems and data. This tool helped us determine that USPTO had not adequately separated its users into groups and had not properly encrypted credentials (usernames and passwords).

[8] Although there are 13 bureaus at the Department, the Office of the Secretary's Office of the Chief Information Officer is responsible for the IT Security of the Minority Business Development Agency and the Economic Development Administration.

[9] *Lateral movement* is a tactic adversaries utilize to move through a network to attempt to reach their primary objective.

[10] The principle of least privilege states that an account should be given access privileges only to relevant function areas required by users' roles and responsibilities.

Because USPTO had not properly grouped users based on their job functions, some users were granted excessive access privileges. In some cases, users would have been able to create, modify, and delete accounts, or access sensitive information, such as other users' credentials. Compromise of an account with these escalated privileges can also lead to the disclosure of sensitive information, lateral movement, and persistence.[11] Further, we noted that the bureau did not adequately review and remove privileges for users who no longer needed them. We concluded that a review of Active Directory accounts could have helped identify these issues.

In response to our report, USPTO confirmed that it had begun separating users into groups based on job functions and had implemented a process to vet whether administrative privileges are continually needed.

Additionally, we observed that there were effectively more than 200 user accounts at risk due to weak or insecure encryption. Passwords were stored using reversible encryption, which was easily cracked[12] using our tools. We found that this encryption issue was largely related to USPTO's legacy systems. However, each insecurely stored password can provide an opportunity for attackers to compromise USPTO systems and information.

Census (January 2021)

As part of our audit of Census's Decennial IT systems, we used Bloodhound to find vulnerabilities and identify possible attack paths. Bloodhound is an open-source tool that can uncover the paths that attackers could take in the event of a compromise. It does so by creating a visualization of an Active Directory's devices and relationships, which is easier to understand than the traditional commands issued by administrators. Using this tool, we again found accounts that had excessive access privileges as well as accounts that were inadequately managed.

Specifically, we identified user groups that had been configured to grant unneeded local administrator privileges. In addition, we uncovered an exploitable service account[13] and a server configured with unconstrained delegation.[14]

[11] *Persistence* is a tactic used by attackers to maintain their foothold on a system.
[12] Password cracking is the process of recovering secret passwords stored in a computer system or transmitted over a network.
[13] Service accounts are generally not used by regular users and are used by software applications running within Windows operating system environment, known as services, such as web or email servers. Service accounts, usually given higher privileges, act as a security identity to grant access to local and network resources, and allow Active Directory administrators to manage the associated running applications.
[14] Unconstrained delegation is a Microsoft Windows privilege that domain administrators can assign to a domain computer or user. Once configured, it allows the server to acquire all the rights of a user who logged into it; therefore, user rights are delegated to the server. If an attacker compromises a server with unconstrained delegation, this feature can be used to steal credentials (usernames and passwords) and potentially gain further unauthorized access to other resources.

We also noted that the bureau failed to disable or remove inactive users from its Active Directory in a timely manner as required by the Department's policy.[15] Although there were only a small number of inactive accounts, keeping these accounts increases the attack surface[16] and risk of system compromise.

Once more, we found that the reason for these deficiencies was that Census did not perform adequate reviews of Active Directory. Census conducted several reviews of its Active Directory via a vendor contract, but the reviews were high-level and did not identify any of the weaknesses that we identified. Once we informed the bureau, it took prompt action to remediate them.

NOAA (February 2022)

At NOAA, we continued use of Bloodhound to assess the security posture of Active Directories at each of the three selected line offices. Yet again, we found both accounts with excessive privileges and inadequately managed accounts.

When we analyzed Active Directory configurations, we found excessive privileges given to accounts across all selected Active Directories. Specifically, we found user accounts that were given unneeded privileges and service accounts that were vulnerable to Kerberoasting.[17] We also discovered servers that had been configured with unconstrained delegation. Furthermore, we identified poor account management practices. For example, we noted inactive accounts and a lack of standardized password requirements for service accounts.

For a third time, we determined that the reason for these deficiencies was the lack of an adequate review of Active Directory accounts. Following our work, NOAA officials expressed appreciation for the high value of our Active Directory audit and stated that the findings and use of the specialized tool would help NOAA improve security on their Active Directories. After our audit concluded, NOAA began immediately using Bloodhound as part of their Active Directory review process.

Across the three bureaus, the root cause of the undetected security vulnerabilities was a lack of adequate reviews of Active Directories and effective use of specialized software tools. Adequate, periodic reviews and remediation of identified security weaknesses are paramount to ensure that Active Directories are properly secured. We consistently recommended implementation of periodic reviews of Active Directory configurations and accounts to ensure consistent adherence to the principle of least privilege. In addition, our latest reports urged the bureaus to consider the feasibility of using specialized tools as part

[15] The policy at the time, the DOC Information Technology Security Program Policy, required users to be disabled after 60 days of inactivity and that passwords are changed every 90 days.

[16] *Attack surface* refers to the number of entry points exposed to a potential hacker.

[17] The Kerberoasting attack cracks weak password encryption utilized by Windows to brute force their way into any system, service or network the account is entitled to. Kerberoasting is identified as one of the well-known adversarial attacks by MITRE in its ATT&CK knowledge base (Attack ID: T1558.003). MITRE, October 20, 2020. *Steal or Forge Kerberos Tickets: Kerberoasting* [online]. https://attack.mitre.org/techniques/T1208/ (accessed November 15, 2022).

of their reviews. Each bureau concurred with our recommendations, and all recommendations have since been implemented. However, the lessons learned from these reports need to be applied Department-wide to ensure that all bureaus have secure Active Directories.

II. The Department Does Not Have a Policy for Regular Active Directory Security Reviews

The Federal Information Security Modernization Act of 2014 emphasizes the importance of continuously monitoring information system security, which is critical to protect IT systems such as Active Directories.[18] Information Security Continuous Monitoring (ISCM)[19] enables an organization to ensure that its IT security controls are working effectively. For example, a common control is to implement the principle of least privilege, as keeping accounts with privileges beyond what is necessary increases the risk of system compromise. An organization that adopts an ISCM strategy may routinely verify that the privileges for each Active Directory account do not extend beyond the needs of its respective user.

The Department's governing cybersecurity policy in effect during our fieldwork was the *Department of Commerce Information Technology Security Baseline Policy (DOC ITSBP)*,[20] which did not have a comprehensive approach to ISCM. Specifically, the Department's policy had suggested "minimum continuous monitoring" controls, but it ultimately allowed for each bureau to create its own ISCM plan. Furthermore, the policy did not contain any specific guidance on Active Directories or other account management software.

As part of our audit, we surveyed bureaus on how often they performed reviews of their Active Directories. Based on the results, we found that bureaus did not have uniform review frequencies, as shown on the next page in table 1.

[18] *See* 44 U.S.C. § 3551(4).

[19] NIST SP 800-137, 2011. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, vi, defines ISCM as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

[20] DOC, June 2019. *Department of Commerce Information Technology Security Baseline Policy (DOC ITSBP), Version 1.0*.

Table 1: Active Directory Review Frequencies

Bureau	Frequency of Formal Reviews
Bureau of Economic Analysis	Annually
Bureau of Industry and Security	Quarterly
Census Bureau	Every 2 Years
FirstNet Authority	Annually
International Trade Administration	Quarterly
National Institute of Standards and Technology	Annually
National Oceanic and Atmospheric Administration	Annually
National Telecommunications and Information Administration	Annually [a]
National Technical Information Service	Quarterly
Office of the Secretary	None
United States Patent and Trademark Office	Every 2 Years

Source: OIG

[a] National Telecommunications and Information Administration did not have a defined frequency for formal Active Directory reviews but contracted with Microsoft to perform a review in both 2021 and 2022.

Due to the lack of centralized guidance, each bureau had developed its own timeline and approach to reviewing and monitoring Active Directories. For example, the Office of the Secretary—which is also responsible for Economic Development Administration and Minority Business Development Agency—did not perform any routine reviews of Active Directories while FirstNet contracted with Microsoft's Detection and Response Team to perform reviews. Overall, 7 out of 11 bureaus indicated that they used Microsoft services to review Active Directories in some capacity.

Although review frequencies and approaches differed, we noted that all 11 bureaus reported that they used some form of specialized, third-party tool. As shown by our previous work, using specialized tools can improve the quality of an Active Directory review. In fact, the Cybersecurity and Infrastructure Security Agency (CISA) previously recommended using tools such as Bloodhound as part of Emergency Directive 21-02.[21] However, even with the use of tools, a lack of consistent, periodic Active Directory reviews may lead bureaus to miss security weaknesses such as excessive privileges, unconstrained delegation, and Kerberoasting. Further, the use of specialized tools without procedures could lead to the tool being used ineffectively, as noted in our audit of USPTO.[22] These

[21] CISA, March 3, 2021. Emergency Directive 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*. Emergency Directive 21-02 was issued to combat a vulnerability in Microsoft Exchange, which provides email infrastructure services.

[22] DOC OIG, June 13, 2019. *Inadequate Management of Active Directory Puts USPTO's Mission at Significant Cyber Risk,* OIG-19-014-A. Washington, DC: DOC OIG, p. 8.

weaknesses can be exploited to undermine the sensitive data and applications that are supported by Active Directories.

The Department has made progress in improving its ISCM strategy. In September 2022, the Office of Cybersecurity and IT Risk Management released the *Enterprise Cybersecurity Policy (ECP),*[23] which replaced the *DOC ITSBP* and established Department-wide cybersecurity requirements. This policy requires bureaus to monitor "core controls" on IT systems to ensure their continued effectiveness, but these controls have yet to be defined. The Department reported that it expects that these controls will be defined with the upcoming release of a supporting ISCM standard. These supporting standards also represent an opportunity for the Department to improve its approach to Active Directory security by defining minimum review periods and recommended assessment tools.

We expect that, once defined and enforced, the *ECP* will improve Active Directory security. Until then, bureaus may continue to follow an ad hoc approach to reviewing Active Directories, which puts them at risk for cyberattacks.

Recommendation

We recommend that the Deputy Secretary of Commerce:

1. Direct the Department's Chief Information Officer to establish a Department-wide policy for periodic reviews of Active Directories to include frequency of review and use of specialized tools.

[23] DOC, September 2022. *Enterprise Cybersecurity Policy (ECP), Version 1.1*.

Other Matter

The Department May Need a More Concerted Effort to Meet Office of Management and Budget's New Password Requirements Related to Active Directories

As noted in the *Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2023* report,[24] making the shift to zero trust[25] architecture will be a considerable challenge for the federal government over the next several years. Office of Management and Budget's (OMB's) memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022, mandates many new cybersecurity requirements. For example, agencies must remove password requirements related to special characters and rotations by January 26, 2023, to better secure enterprise-managed identities and accounts.

Although agencies were given a year to comply, OMB M-22-09 states that the outdated requirements "should be removed by agencies as soon as is practical and should not be contingent on adopting other protections." This is due to evolving best practices surrounding passwords as security researchers discover that, in practice, users will write down passwords or create ones that are easily guessable. OMB M-22-09 states, "If outdated password requirements lead agency staff to reuse passwords from their personal life, store passwords insecurely, or otherwise use weak passwords, adversaries will find it much easier to obtain unauthorized account access—even within a system that uses MFA [multifactor authentication]."

The Department established a working group to begin implementing zero trust architecture. By June 30, 2022, the group had developed guidance related to the required actions within OMB M-22-09, including password requirements. Because Active Directories are used to manage user accounts, enforce password requirements, and store credentials, they are critical in implementing the updated requirements. Yet, during our fieldwork, we observed that none of the Department bureaus had implemented the updated password requirements on their Active Directories. Rather, they were continuing to follow long-standing password complexity and rotation practices by requiring user passwords to contain special characters and be changed every 90 days. Although this implementation has been the standard for IT organizations, it is important for the Department to adapt to the new best practices.

Within the Department, Active Directories are used to support a variety of mission-critical services such as email, satellite activities, law enforcement case management, and even the workstations that Department employees use each day. Using an Active Directory to continue enforcing ineffective password requirements places these applications at a higher risk. The Department had stated that it planned to meet the January 26, 2023, deadline established by OMB for its Active Directories, but was unlikely to meet the deadline for some of its other

[24] DOC OIG, October 13, 2022. *Top Management and Performance Challenges Facing the Department of Commerce in Fiscal Year 2023,* OIG-23-001. Washington, DC: DOC OIG.
[25] The core idea of zero trust is to remove any implicit trust from an IT security strategy and continuously validate interactions between users and resources on the network.

applications. However, during our audit, we became concerned that the Department had yet to transition to zero trust password requirements for any Active Directory. Therefore, we believe that the Department should monitor bureaus' progress toward meeting these requirements to improve its security posture.

Conclusion

Active Directories are considered prime targets for cyber attackers because of the sensitive information they contain. If attackers compromise an Active Directory, they gain near complete control of an organization's IT infrastructure, making it imperative to properly protect them. Our previous work has repeatedly illustrated the need for periodic evaluations of Active Directories. This capstone audit showed that the Department's bureaus have varying approaches to Active Directory security; some of which expose them to additional risk. The Department has begun to make improvements by releasing its *Enterprise Cybersecurity Policy (ECP)*, but it still has additional opportunities to enhance the security of Active Directories.

In addition, we commend the Department's commitment to implementing zero trust architecture through its working group. However, we believe that the Department should review the progress of its bureaus in meeting the new password requirements mandated by OMB M-22-09.

Summary of Agency Response and OIG Comments

In response to our draft report, the Department generally concurred with all of our findings and recommendation, as well as generally described plans it has taken or will take to implement the recommendation. The Department's response, including technical comments, is included in appendix B. Although we considered the Department's comments, we determined that changes to the final report were not warranted.

We are pleased that the Department agrees with our recommendation and look forward to receiving its action plan for implementing the recommendation.

Appendix A: Objective, Scope, and Methodology

Our audit objective was to identify the remaining Department Active Directories, which have not been reviewed by the OIG, and summarize past OIG work related to the management of Active Directories.

To accomplish our objective, we:

- Reviewed vendor best practices for securing Active Directories.
- Issued a survey to each Department's bureau to determine whether they operated Active Directories and, if so, their relevant policies and practices.
- Interviewed Department officials to determine the status of IT security policies.

The bureaus surveyed were the Bureau of Economic Analysis, Bureau of Industry and Security, Census, International Trade Administration, National Institute of Standards and Technology, NOAA, National Technical Information Service, National Telecommunications and Information Administration, USPTO, and Office of the Secretary.[26]

We also reviewed 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. dated December 18, 2014
- OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, dated January 26, 2022
- U.S. Department of Commerce, *Enterprise Cybersecurity Policy*, dated October 2022
- U.S. Department of Commerce, *Information Technology Security Baseline Policy,* dated June 2019
- CISA, Emergency Directive 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, dated March 3, 2021
- NIST Special Publications:
  - 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* dated December 2018
  - 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* dated September 2020

[26] The Office of the Secretary's Office of the Chief Information Officer is also responsible for the Active Directories of the Minority Business Development Agency and the Economic Development Administration.

- 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* dated September 2011

Our analysis did not rely on computer-processed data to support our findings, conclusion, or recommendation.

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

We conducted this performance audit in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on its audit objective.

Appendix B: Agency Response

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

MEMORANDUM FOR: Peggy E. Gustafson
Inspector General

FROM: André V. Mendes ANDRE MENDES Digitally signed by ANDRE MENDES Date: 2023.02.06 14:58:55 -05'00'

SUBJECT: Department of Commerce's Concurrence to the Office of Inspector General's Draft Report, *Capstone Report Effective Reviews Are Needed to Enhance the Security Posture of the Department's Active Directories (OIG-22-426, January 9, 2023)*

We appreciate that the Office of the Inspector General (OIG) presented the Department of Commerce (DOC) with an opportunity to review the Draft Report, *Capstone Report Effective Reviews Are Needed to Enhance the Security Posture of the Department's Active Directories (OIG-22-426, January 9, 2023).*

The DOC Office of Chief Information Officer (OCIO) has reviewed the draft report and generally concurs with the finding and recommendation. The DOC OCIO has issued the new Enterprise Cybersecurity Policy, Security and Privacy Control Baseline, and is prepared take further action to address recurring issues to enhance the security posture of the Department's Active Directories. The DOC is providing the attached comments for OIG's consideration.

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

Attachment

cc: MaryAnn Mausser, DOC
Joselyn Bingham, Audit Liaison, DOC
Ryan A. Higgins, Chief Information Security Officer, DOC
Maria Hishikawa, IT Audit Liaison, DOC

Department of Commerce Technical and Editorial Comments
on the OIG Draft Report entitled *Capstone Report: Effective Reviews Are Needed to Enhance the Security Posture of the Department's Active Directories*
(OIG-22-426, January 09, 2023)

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.

US Patent and Trademark Office (USPTO)

Page 4, Paragraph 2, Sentence 1: *"addition."* In response to our report, USPTO confirmed that it had begun separating users into groups based on job functions and had implemented a process "from December 2020" to vet whether administrative privileges are continually needed.

Page 4 Paragraph 3, Sentence 5: *"addition."* The last sentence should read, "USPTO is working continuously to enforce secure encryption, and reduced the account with weak or insecure encryption to 20 user accounts."

011200000426