The Department Needs to Fully Implement Strong Multifactor Authentication for Its High Value Assets to Protect Them from Cyberattacks

FINAL REPORT

JANUARY 22, 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

January 22, 2024

MEMORANDUM FOR: Ryan A. Higgins
Acting Chief Information Officer
Department of Commerce

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

SUBJECT: *The Department Needs to Fully Implement Strong Multifactor Authentication for Its High Value Assets to Protect Them from Cyberattacks*
Final Report No. OIG-24-009-A

Attached for your review is our final report on the audit of the U.S. Department of Commerce's (the Department's) implementation of multifactor authentication (MFA) on its high value assets (HVAs). Our objective was to determine whether the Department has implemented MFA on its HVAs in accordance with zero trust architecture principles. To address this objective, we judgmentally selected five HVAs from four bureaus and tested whether they met the requirements for strong MFA as established in the Office of Management and Budget's memorandum, M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,* January 26, 2022.

We found the following:

I. The National Telecommunications and Information Administration (NTIA) did not implement adequate MFA to protect an HVA against phishing attacks.

II. Selected bureaus had not fully implemented MFA for their HVAs in accordance with zero trust architecture principles.

In its response to our draft report, the Department generally concurred with our findings and recommendations and described actions it has taken, or will take, to address them. The Department's formal response is included within this final report as appendix B.

The Department also provided bureau-specific technical and editorial comments. NTIA provided separate technical comments. Where appropriate, we made a minor revision to the final report. Additionally, the National Institute of Standards and Technology (NIST) provided evidence that its HVA has now fully implemented application-layer MFA. Accordingly, we consider recommendation 8 closed.

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. The final report will be

posted on the Office of Inspector General's 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 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: Param Soni, Chief Information Officer, BEA
Luis Cano, Chief Information Officer, Census Bureau
Chandan Sastry, Chief Information Officer, NIST
Catrina Purvis, Chief Information Officer, NTIA
Maria Hishikawa, Director, Office of Security Program Management Services, OCIO
MaryAnn Mausser, Audit Liaison, Office of the Secretary
Joselyn Bingham, Audit Liaison, Office of the Chief Information Officer

Report in Brief

January 22, 2024

Background

To fulfill its mission of promoting economic growth, the U.S. Department of Commerce (the Department) and its bureaus operate hundreds of information systems. Among these are mission-critical systems designated as high value assets (HVAs), which are systems so critical that their loss or corruption would have a serious impact on the Department's ability to meet its mission or conduct business. Accordingly, the Department must use modern security practices to protect HVAs from malicious cyberattacks.

On January 26, 2022, the Office of Management and Budget (OMB) issued memorandum M-22-09, which marked a dramatic shift in the federal government's cybersecurity strategy and set a deadline of the end of fiscal year 2024 for agencies to meet specific cybersecurity standards and objectives.

Rather than focusing on a strong network perimeter, agencies were instructed to shift towards a zero trust architecture (ZTA) strategy. A core component of the federal government's ZTA strategy is multifactor authentication (MFA).

MFA is a fundamental security control that requires users to log in with at least two of the three types of authentication factors: something you know, something you have, or something you are.

OMB requires agencies to use strong MFA—a key part of ZTA—throughout their enterprise.

Why We Did This Audit

Our objective was to determine whether the Department has implemented MFA for its HVAs in accordance with ZTA principles.

OFFICE OF THE SECRETARY

The Department Needs to Fully Implement Strong Multifactor Authentication for Its High Value Assets to Protect Them from Cyberattacks

OIG-24-009-A

WHAT WE FOUND

We examined five HVA systems from four selected Department bureaus: the Bureau of Economic Analysis (BEA), the U.S. Census Bureau (Census), the National Institute of Standards and Technology (NIST), and the National Telecommunications and Information Administration (NTIA). We found the following:

I. NTIA did not implement adequate MFA to protect an HVA against phishing attacks.

II. Selected bureaus had not fully implemented MFA for their HVAs in accordance with ZTA principles.

WHAT WE RECOMMEND

We recommend that the Department's Chief Information Officer (CIO) do the following:

1. Work with BEA and other federal agencies to determine a resolution to the OMB and IRS password policy conflict.
2. Evaluate current Department cybersecurity policies to determine if specific HVA guidelines are needed for phishing exercises, including exercise frequency.

We recommend that the Department's CIO direct the NTIA CIO to do the following:

3. Require regular phishing exercises as part of security awareness training for HVA users.
4. Implement phishing-resistant and application-layer MFA on both NTIA HVAs.
5. Update and implement password policies in accordance with OMB requirements.

We recommend that the Department's CIO direct the BEA CIO to do the following:

6. Implement application-layer MFA on the BEA HVA.

We recommend that the Department's CIO direct the Census CIO to do the following:

7. Identify a feasible solution to adopt phishing-resistant MFA internally on the Census HVA.

We recommend that the Department's CIO direct the NIST CIO to do the following:

8. Identify a feasible solution to adopt application-layer MFA on all components of the NIST HVA.

We provided a draft of this report to the Department for review and response. The Department generally concurred with our recommendations.

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

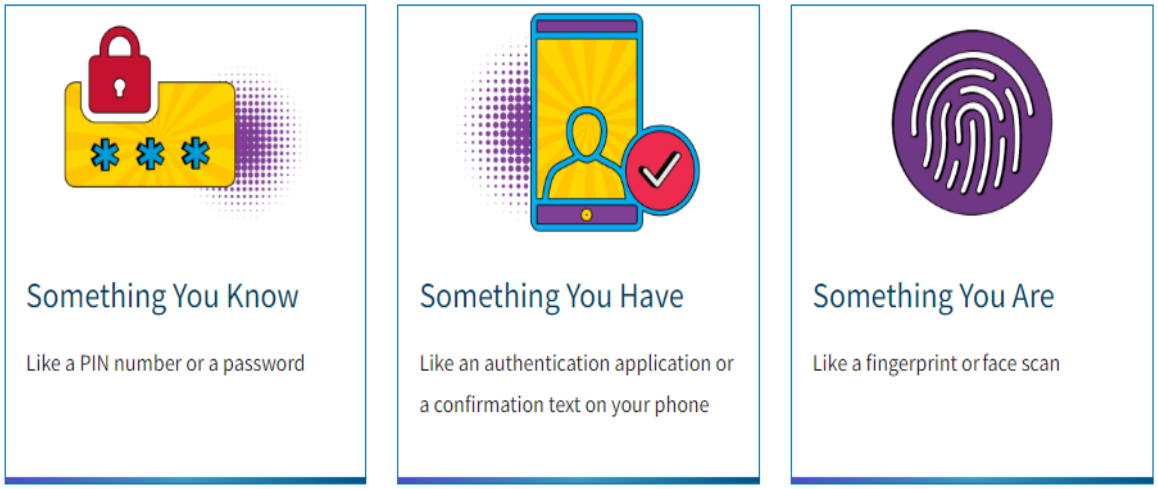
To fulfill its mission of promoting economic growth, the U.S. Department of Commerce (the Department) and its bureaus operate hundreds of information systems. Among these are mission-critical systems designated as high value assets (HVAs), which are systems so critical that their loss or corruption would have a serious impact on the Department's ability to meet its mission or conduct business.[1] Accordingly, the Department must use modern security practices to protect HVAs from malicious cyberattacks.

On January 26, 2022, the Office of Management and Budget (OMB) issued memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, which marked a dramatic shift in the federal government's cybersecurity strategy and set a deadline of the end of fiscal year 2024 for agencies to meet specific cybersecurity standards and objectives. Rather than focusing on a strong network perimeter, agencies were instructed to shift towards a zero trust architecture (ZTA) strategy. The key principle of ZTA is that "no actor, system, network, or service operating outside or within the security perimeter is trusted."[2] Everything and everyone must be verified when seeking access. Multifactor authentication (MFA) is a core component of the federal government's ZTA strategy.

MFA is a fundamental security control that requires users to log in with at least two of the three types of authentication factors: something you know, something you have, or something you are (see figure 1). MFA has been a long-standing federal requirement because it can significantly reduce the likelihood that a user account will be compromised by attackers. The federal government often implements MFA through Personal Identity Verification (PIV) cards.[3] When logging in, the PIV acts as something you have, and a user-defined personal identification number (PIN) acts as something you know.

[1] See U.S. Department of Commerce (DOC), National Institute of Standards and Technology Computer Security Resource Center. *High Value Asset (definition)* [online]. https://csrc.nist.gov/glossary/term/high_value_asset (accessed November 6, 2023).
[2] OMB M-22-09, page 2.
[3] OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management,* May 21, 2019, instructs agencies to use PIV cards as the "primary means of identification and authentication to Federal information systems," page 3.

Figure 1. The Three Types of Authentication Factors



Source: CISA www.cisa.gov/MFA

OMB requires agencies to use strong MFA—a key part of ZTA—throughout their enterprise.[4] Strong MFA meets the following three requirements:

1. Uses authentication factors that are resistant to phishing attacks. This is known as phishing-resistant MFA and provides protection against attacks in which malicious actors attempt to trick users into sharing sensitive information or giving access to accounts, computers, or networks.

2. Enforces MFA when accessing an individual application instead of when entering the network. This is known as application-layer MFA and ensures that an attacker cannot compromise an entire system by gaining access to a single component.

3. Does *not* force users to include special characters in their passwords or regularly change passwords. The National Institute of Standards and Technology (NIST) has noted that these well-intentioned requirements often lead users to reuse or create easy-to-guess passwords. [5]

[4] OMB M-22-09, page 5.
[5] NIST, June 2017. NIST Special Publication 800-63B, *Digital Identity Guidelines Authentication and Lifecycle Management.* Gaithersburg, MD: NIST.

Objective, Findings, and Recommendations

The objective of this audit was to determine whether the Department has implemented MFA for its HVAs in accordance with ZTA principles. Specifically, we determined the extent to which four selected bureaus had implemented MFA for their HVAs in accordance with OMB requirements. The four selected bureaus were the Bureau of Economic Analysis (BEA), the U.S. Census Bureau (Census), NIST, and the National Telecommunications and Information Administration (NTIA). See appendix A for a full description of our scope and methodology.

We examined five HVA systems from the four selected Department bureaus. We were able to exploit a weak MFA implementation to gain access to one NTIA system through a simulated phishing attack. We also found that none of the five selected HVAs had fully implemented all three OMB requirements:

1. phishing-resistant MFA,
2. application-layer MFA, and
3. modern password policies.

Until the Department fully implements OMB's requirements for MFA, its HVAs will be more susceptible to common attack types, including phishing. A strong MFA implementation can prevent an internal or external threat actor from gaining unauthorized access to user accounts and sensitive data.

I. NTIA Did Not Implement Adequate MFA to Protect an HVA Against Phishing Attacks

NTIA is responsible for expanding broadband Internet access and adoption in America, expanding the use of spectrum by all users, and ensuring that the Internet remains an engine for continued innovation and economic growth. Given its mission, some of the selected NTIA HVAs are publicly accessible, placing them at higher risk compared to others. In fact, NTIA has previously been the target of sophisticated cyberattacks.

For these reasons, we conducted a simulated phishing attack against 73 users of an NTIA HVA to validate the effectiveness of its MFA implementation. All our attempts to send phishing emails to the users were blocked by NTIA's email filters, which showed that the bureau has an effective first layer of defense. However, the intent of this limited exercise was to test the susceptibility of the HVA's MFA implementation to phishing rather than email filters. Although the filters were successful in preventing our attempt, a dedicated adversary would likely be able to craft an email that bypasses filters. For example, in 2016, Russian hackers successfully phished members of the Democratic National Committee,

bypassing email filters and accessing thousands of emails.[6] We worked with NTIA to allow our phishing emails through its filter solely to test the effectiveness of its MFA implementation.[7]

We ultimately circumvented the MFA implementation for one NTIA HVA as it was not phishing resistant. In addition, we found that a high number of users were deceived by our phishing email and NTIA had not properly configured some user accounts.

A. An Office of Inspector General (OIG) simulated phishing attack circumvented the MFA implementation and resulted in access to an NTIA HVA

As part of our simulated phishing attack, we were able to deceive one high-ranking user into completing the HVA's login process. This included completing MFA, which granted full access to the user's HVA account. Using this account, we had the ability to access sensitive documentation within the HVA such as proprietary or business information. We were able to accomplish this because NTIA used an older implementation of MFA that was not phishing resistant.

Prior to our simulated phishing attack, we validated the authentication process of the NTIA HVA. The HVA required users to enter a standard username and password to log in. Users then received a system-generated phone call, which prompted them to enter their PIN using the keypad.

We sent a phishing email to direct users to a fake website that mirrored the actual HVA login page. Through this fake site, we captured usernames and passwords and used them to log in to the actual HVA site. Any user that submitted credentials would already be expecting a phone call to enter their PIN. After entering their PIN, the MFA process was complete, and we were granted access to the NTIA HVA.

OMB requires implementation of phishing-resistant MFA, which would have prevented our simulated attack. For example, using a PIV card rather than a phone call as an additional factor would have made our attack impossible. PIV cards securely store user credentials in a security chip. The card must be directly connected to a computer before a user can enter a PIN to complete MFA. In our attack, even if we captured a user's PIN, we would not have been able to use it without also acquiring their PIV card.

B. NTIA users responded to an OIG phishing email at a high rate, increasing the risk of compromise

Our phishing emails instructed users to log in through our malicious link to maintain their access to the HVA. This is a common technique used in phishing attacks. Such

[6] Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 Election Volume 5: Counterintelligence Threats and Vulnerabilities*. Available online at https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf (accessed October 16, 2023).
[7] The scope of our audit did not include testing email filtering as would be done in a full penetration test.

attacks often urge users to take immediate action, preventing them from taking time to question the authenticity of the email.

During our phishing attack, we observed a higher-than-average clickthrough rate.[8] Although this was not the focus of our work, a high clickthrough rate is concerning because it increases the likelihood of a successful attack by giving attackers more opportunities to gain access. Furthermore, most of those users that clicked our link also entered credentials. These credentials could be used as part of "credential stuffing," in which attackers use stolen credentials to try to access other systems and applications.[9] Key statistics from our simulated phishing attack are shown in figure 2.

Figure 2. NTIA HVA Phishing Results

73 Emails Sent

29 Users Clicked the Link in the Email

21 Users Entered Credentials

39.7 % **Clickthrough Rate**

Source: OIG-generated from data obtained during the phishing attack

NTIA's clickthrough rate of approximately 40 percent was 12 percent higher than an average rate for similar-sized government agencies.[10] We noted that, prior to our July 2023 test, NTIA had not conducted a phishing exercise since September 2022 and did not require it as part of its HVA System Security Plan. The goal of a phishing exercise is to test employees' ability to detect a phishing email and often includes follow-up training. These exercises are used to keep users vigilant if a phishing attack bypasses email filters.

The Cybersecurity and Infrastructure Security Agency recommends that organizations with HVAs conduct practical exercises with users, such as phishing exercises. A recent NIST study also noted that 48 of the 64 surveyed federal organizations that conduct

[8] A clickthrough rate is calculated by dividing the number of users that clicked the malicious website link within the phishing email by the total number of emails sent.

[9] MITRE ATT&CK. *Brute Force: Credential Stuffing* [online]. www.attack.mitre.org/techniques/T1110/004/ (accessed November 1, 2023).

[10] KnowBe4's *Phishing by Industry Benchmarking Report,* 2023, states that baseline phishing test results for government agencies with 1 to 249 employees had an average clickthrough rate of 27.7 percent. Available online at https://www.knowbe4.com/hubfs/2023-Phishing-by-Industry-Benchmarking-Report-Research-EN_US.pdf (accessed July 26, 2023).

phishing exercises do so either monthly or quarterly.[11] NTIA's lack of regular phishing exercises may have contributed to the high clickthrough rate and credential entries seen in our results. Currently, Department policy has no specific requirement for conducting such exercises.

C. NTIA had not properly configured user accounts, reducing the effectiveness of MFA for its HVA

NTIA's implementation of MFA required that HVA users enter a PIN on their phone after submitting a username and password on the website. However, some users were permitted to satisfy this MFA requirement by entering the same single character on their phone as opposed to a unique, multidigit PIN. This occurred because NTIA administrators had improperly configured some user accounts by not following NTIA's standard procedure for account creation.

This resulted in a weakened authentication process for the HVA. If a user's phone number was stolen,[12] an attacker with stolen credentials would only need to press a single key, rather than also needing to know the user's PIN. After we informed NTIA of this issue, NTIA reissued the procedure to its administrators. NTIA also took steps to fix the incorrectly configured accounts and ensure that they were required to use PINs.

Our successful phishing attack and the improperly configured user accounts show that NTIA needs to better manage and implement a key cybersecurity control for its HVA. MFA is just one piece of the comprehensive shift to ZTA. NTIA will need to devote time and resources to meet the OMB's end of fiscal year 2024 deadline for complete implementation.

II. Selected Bureaus Had Not Fully Implemented MFA for Their HVAs in Accordance with ZTA Principles

Overall, none of the four bureaus we selected had fully implemented MFA in accordance with the ZTA principles required by OMB. Each of the five selected HVAs lacked one or more of the required traits: phishing-resistant MFA, application-layer MFA, and modern password policies. Table 1 shows the status of each bureau's implementation of OMB requirements for our selected HVAs.

[11] NIST, March 2022. *Approaches and Challenges of Federal Cybersecurity Awareness Programs,* 21. Available online at https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8420A.pdf (accessed October 3, 2023).
[12] A common attack known as "SIM swapping" in which attackers trick a mobile provider into transferring a victim's phone number to a device that they control.

Table 1. Status of Bureau Implementation of OMB Requirements for HVAs

Bureau	Phishing-Resistant MFA	Application-Layer MFA	Modern Password Policies
BEA	Implemented	Not Implemented	Not Implemented
Census	Not Implemented	Implemented	N/A[1]
NIST	Implemented	Partially Implemented	Implemented
NTIA System 1	Not Implemented	Implemented	Not Implemented
NTIA System 2	Not Implemented	Not Implemented	Not Implemented

[1]The Census HVA uses a password-less approach to authentication.

A. For three of five HVAs, bureaus had not implemented phishing-resistant MFA

As demonstrated by our simulated phishing attack in Finding I, MFA configurations that are not phishing resistant can be circumvented, allowing unauthorized access to an HVA. In addition to the HVA described in Finding I (System 1), NTIA operated a second HVA (System 2), which also had not implemented phishing-resistant MFA. Furthermore, we found that the Census HVA was also not compliant with this requirement.

Both NTIA's System 2 and Census' HVA required users to use a physical token as a second form of authentication. These tokens display a rotating code that changes after a short time. Unfortunately, the tokens are also susceptible to phishing. Attackers can intercept codes and other credentials through a malicious website like the one used in our simulated phishing attack. By acting quickly or using automated tools, the attackers can enter stolen codes to gain access to a user's account.

Although it is not phishing resistant, the token-based approach used by Census for its HVA is compensated for by several other controls. Access to the system is heavily restricted to a small subset of administrators, reducing the potential for compromise. Furthermore, these administrators must access the network using a phishing-resistant PIV card before reaching the HVA. Still, Census officials acknowledged that the current implementation is not fully compliant and that phishing-resistant MFA can improve the security of a critical system.

In contrast, we found that NTIA did not enforce any form of MFA on System 2 for users already on the NTIA network. A token was only required if users were accessing System 2 externally. NTIA leadership stated that they were preparing for a bureau-wide MFA project that would address the MFA implementation issues on both of its HVAs. However, according to NTIA officials, the architecture of System 2 poses significant technical challenges in implementing compliant, phishing-resistant MFA.

B. For three of five HVAs, bureaus had not fully implemented application-layer MFA

Application-layer MFA is a core component of ZTA. The traditional approach to authentication was for users to authenticate to a network, such as through a virtual

private network (VPN),[13] and then they would have complete access to enterprise resources. In application-layer MFA, users are authenticated at each application; therefore, a system can prevent a vulnerability in one application from compromising others.

NIST had implemented application-layer MFA for all but one of the applications on the selected HVA. This application is used only by a small number of NIST system administrators, and the HVA maintains additional protections, such as jump servers.[14] NIST plans to work with the vendor to implement application-layer MFA during FY 2024.

BEA had implemented MFA authentication for its network and devices but not at the application layer. None of the internal applications within BEA's HVA were compliant. The HVA has many different applications, including legacy password-based applications, which BEA officials stated cannot implement application-layer MFA without significant technical work. BEA has engaged with the Department in preparation for this substantial project.

As noted previously, the System 2 architecture poses significant technical challenges in implementing MFA for NTIA internal users. The system also relied on a noncompliant VPN for external access, which had been targeted in a previous attack. Again, NTIA reported that it was planning a bureau-wide MFA project to address these issues, but we remain concerned that this project will require significant effort to bring the HVA into compliance, leaving the HVA vulnerable in the interim.

C. For three of five HVAs, bureaus had not implemented modern password policies

As part of the shift to ZTA, OMB encourages agencies to use password-less MFA options, such as PIVs. However, when passwords are used as part of MFA, OMB M-22-09 states that agencies must not require the use of special characters or regular password rotation.[15] In practice, requiring users to include special characters and to frequently change passwords led to worse security outcomes. Users were more likely to write down passwords or to create passwords that were easily guessed. We found that NTIA and BEA had not implemented a modern password policy for their HVAs.

In August 2023, NTIA stated that it was waiting for its next policy update cycle before updating its password policies. However, the Department had revised its *Security and Privacy Control Matrix* in January 2023 to reflect OMB's password policy requirements. Later, NTIA officials told us that they would update password policies by the end of 2023.

[13] A VPN enables a device to securely connect to a private or enterprise network through the Internet.
[14] Jump servers are specially monitored devices that provide a controlled means of access to sensitive applications. NIST has also implemented PIV-based MFA on its jump servers.
[15] M-22-09, page 8.

BEA reported that it was required to follow the guidelines from the Internal Revenue Service (IRS).[16] This publication was issued prior to the OMB requirement and includes both the use of special characters in passwords and password rotation. The opposing mandates forced BEA to be out of compliance with either OMB or the IRS. BEA ultimately decided to follow the IRS requirements. However, the Department will still need to resolve the conflict between policies.

Conclusion

Evidently, the Department still has significant work to do to implement secure and compliant MFA for its HVAs. Although some bureaus were further along than others, none were fully compliant. The results of our simulated phishing attack against an NTIA HVA showed why strong MFA is important.

In June 2023, the Department procured an identity management system. This identity management system could assist bureaus with meeting OMB's ZTA requirements, including strong MFA. As it begins to roll out the system, the Department should prioritize the protection of its most critical assets.

Recommendations

We recommend that the Department's Chief Information Officer (CIO) do the following:

1. Work with BEA and other federal agencies to determine a resolution to the OMB and IRS password policy conflict.
2. Evaluate current Department cybersecurity policies to determine if specific HVA guidelines are needed for phishing exercises, including exercise frequency.

We recommend that the Department's CIO direct the NTIA CIO to do the following:

3. Require regular phishing exercises as part of security awareness training for HVA users.
4. Implement phishing-resistant and application-layer MFA on both NTIA HVAs.
5. Update and implement password policies in accordance with OMB requirements.

We recommend that the Department's CIO direct the BEA CIO to do the following:

6. Implement application-layer MFA on the BEA HVA.

We recommend that the Department's CIO direct the Census CIO to do the following:

7. Identify a feasible solution to adopt phishing-resistant MFA internally on the Census HVA.

[16] Department of Treasury, IRS, November 2021. *Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information*. IRS Publication 1075, Revision 11-2021. Available online at https://www.irs.gov/pub/irs-pdf/p1075.pdf (accessed November 3, 2023).

We recommend that the Department's CIO direct the NIST CIO to do the following:

8. Identify a feasible solution to adopt application-layer MFA on all components of the NIST HVA.

Summary of Agency Response and OIG Comments

On January 2, 2024, we received the Department's formal response to our draft report. The Department generally concurred with our findings and recommendations and described actions it has taken, or will take, to address them. The Department's formal response is included within this final report as appendix B.

The Department also provided bureau-specific technical and editorial comments. NTIA provided separate technical comments on January 1, 2024. Where appropriate, we made a minor revision to the final report. Additionally, NIST provided evidence that its HVA has now fully implemented application-layer MFA. Accordingly, we consider recommendation 8 closed.

We are pleased that the Department generally concurred with our recommendations and look forward to reviewing its proposed audit action plan.

Appendix A: Objectives, Scope, and Methodology

This report is a continuation of our work relating to the Department's management of HVAs. Our audit objective was to determine whether the Department has implemented multifactor authentication on its high value assets in accordance with zero trust architecture principles.

To accomplish our audit objective, we judgmentally selected five HVAs from bureaus that had not been tested by OIG in our previous HVA audit. We then

- interviewed system administrators and bureau management,
- reviewed relevant MFA policies and configurations of selected HVAs to verify whether bureaus implemented the following:
    - use of a phishing-resistant form of MFA,
    - enforcement of MFA at the application-layer,
    - removal of requirements to use special characters or rotate passwords regularly, and
- performed a simulated phishing attack against one HVA to demonstrate the importance of implementing phishing-resistant measures.

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

- OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,*
- OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management,*
- Executive Order 14028, *Improving the Nation's Cybersecurity,* May 12, 2021,
- Federal Information Security Modernization Act of 2014,
- NIST Special Publications:
    - 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,*
    - 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,*
- U.S. Department of Commerce *Enterprise Cybersecurity Policy*, and
- U.S. Department of Commerce *Security and Privacy Control Matrix*.

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

We conducted our audit from March 2023 through October 2023 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401–424), and Department Organization Order 10-13, dated October 21, 2020. We performed our work remotely.

We conducted this 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 our audit objective.

Appendix B: Agency Response

The Department's response to our draft report follows on page 15.

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

MEMORANDUM FOR: Peggy E. Gustafson
Inspector General

FROM: Ryan A. Higgins
Acting Chief Information Officer

SUBJECT: The Department of Commerce Concurrence on the Office of Inspector General Draft Report, *The Department Needs to Fully Implement Strong Multifactor Authentication for Its High Value Assets to Protect Them from Cyberattacks (December 1, 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, *The Department Needs to Fully Implement Strong Multifactor Authentication for Its High Value Assets to Protect Them from Cyberattacks (December 1, 2023).*

The DOC Office of the Chief Information Officer (OCIO) reviewed the draft report and generally concurs with the findings and recommendations. The Department appreciates the 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.

Many of the weaknesses noted in the report are actively being addressed and mitigated. DOC leadership will continue to engage with Bureau stakeholders to prioritize resources to protect High Value Assets (HVAs). The National Institute of Standards and Technology (NIST) has confirmed implementation of application layer multifactor authentication for the system cited in the OIG report. Additionally, the DOC OCIO confirmed that the US Department of Treasury will update policies to adhere to modern password policies, which resolves the policy conflicts cited by the Bureau of Economic Analysis (BEA). Lastly, the DOC HVA Handbook is in its final approval processes, which will define specific HVA guidelines such as those recommended in the report.

While the Department is committed to cooperating with the OIG, we ask for consideration to the aggregate impact and potential for adverse effects to mission programs and national interests through the collection of reports made available to the public and adversaries alike.

Should you have any questions, please contact Maria Hishikawa at (202) 893-2508 or mhishikawa@doc.gov.

cc: MaryAnn Mausser, Audit Liaison
Joselyn Bingham, Audit Liaison
Aditi Palli, Chief of Staff, Office of the Chief Information Officer
Maria Hishikawa, Director, Office of Security Program Management Services
Shavon Moore, IT Audit Liaison

01 12000 00 452

REPORT

FRAUD & WASTE & ABUSE

HOTLINE

Department of Commerce

Office of Inspector General Hotline

www.oig.doc.gov | 800-424-5197