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.