Report in Brief

September 28, 2023

Background

To fulfill its mission, the Department of Commerce and its bureaus operate hundreds of information systems. Among these are mission-critical systems designated as high value assets (HVAs), systems so critical their loss or corruption would seriously affect the Department's ability to meet its mission or do its work.

Additional security measures are required to protect HVAs from cyberattacks. The Cybersecurity and Infrastructure Security Agency (CISA) requires assessments and tests of HVAs and other IT systems. CISA also manages an online catalog of known exploited vulnerabilities, or KEVs (vulnerabilities that adversaries have already taken advantage of to conduct cyberattacks). Whenever the catalog is updated with new KEVs, agencies must scan their systems and remediate any KEVs they find within 2 weeks.

In addition to CISA's requirements, the Department requires annual penetration testing (simulated cyberattacks that test system security) of its mission-critical systems, including HVAs.

Why We Did This Review

We focused this audit on the Department's identification and remediation of vulnerabilities on HVAs. Our objective was to determine if the Department and its bureaus identify and remediate these vulnerabilities in accordance with federal requirements.

Specifically, we determined the extent the Department conducted HVA risk and vulnerability assessments within the last 3 years, resolved issues found in those assessments, and remediated KEVs by their due date.

OFFICE OF THE SECRETARY

Security Weaknesses in the Department's Mission-Critical High Value IT Assets Leave the Assets Vulnerable to Cyberattacks

OIG-23-030-A

WHAT WE FOUND

While the Department conducts HVA assessments in accordance with federal requirements, it did not always effectively identify and remediate vulnerabilities. It also did not follow CISA's best practice security guidance for HVAs. We found that

I. HVAs are operating with significant risk due to unresolved vulnerabilities. The Department conducts penetration tests as required, but does not remediate issues according to risk-based timelines. As a result, the Department's HVAs are operating with known exploited vulnerabilities for prolonged periods. The Department's lack of prioritization led to delays in remediating vulnerabilities.

II. OIG successfully exploited security weaknesses on multiple HVAs. All seven of the HVAs in our review had at least one exploitable vulnerability type, and the Department's vulnerability scanners do not always identify KEVs and other vulnerabilities in HVAs.

We also learned during our audit that the U.S. Patent and Trademark Office (USPTO) had asked the Department to downgrade all of its HVAs to non-HVAs. In September 2023, the Department's Chief Information Officer agreed to downgrade the majority of USPTO's HVAs.

WHAT WE RECOMMEND

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

1. Work with system owners to (a) determine why penetration tests and KEV findings are not resolved within established due dates, (b) prioritize resources to resolve the causes of the delayed remediations, (c) immediately remediate vulnerabilities, and (d) establish a real-time reporting mechanism to track closures.
2. Update departmental policies for HVAs to align control requirements more closely to HVA risk, such as implementing additional CISA-recommended controls.
3. Establish and implement a process to aggregate and share penetration testing results across bureau HVA system owners.
4. Work with bureaus to determine why KEVs were missed during vulnerability scanning and use that analysis to implement standard configurations for vulnerability scanners.

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