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

FINAL REPORT NO. OIG-23-030-A
September 28, 2023

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

September 28, 2023

MEMORANDUM FOR: Don Graves
Deputy Secretary of Commerce

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

SUBJECT: *Security Weaknesses in the Department's Mission-Critical High Value IT Assets Leave the Assets Vulnerable to Cyberattacks*
Final Report No. OIG-23-030-A

Attached is the final report on our audit of the U.S. Department of Commerce's identification and remediation of vulnerabilities on its high value assets (HVAs). The objective of this audit was to determine if the Department and its bureaus identify and remediate vulnerabilities on HVAs in accordance with federal requirements.

We found the following:

I. HVAs are operating with significant risk due to unresolved vulnerabilities.

II. OIG successfully exploited security weaknesses on multiple HVAs.

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

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 also provided bureau-specific technical and editorial comments. We accepted the technical comments, as appropriate, and included them in the final version of this report. The Department's response is included in appendix B.

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 OIG'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 Director for Cybersecurity Chuck Mitchell at (202) 809-9528.

Attachment

CC: André Mendes, Chief Information Officer, Office of the Chief Information Officer (OCIO)
Param Soni, Chief Information Officer, BEA
G. Nagesh Rao, Chief Information Officer, BIS
Luis Cano, Chief Information Officer, Census Bureau
Chandan Sastry, 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
MaryAnn Mausser, Audit Liaison, Office of the Secretary
Rehana Mwalimu, Risk Management Officer and Primary Alternate Department GAO/OIG Liaison, Office of the Secretary
Ryan Higgins, Chief Information Security Officer, OCIO
Joselyn Bingham, Audit Liaison, OCIO
Maria Hishikawa, Director, Office of Security Program Management Services, OCIO

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.

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 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 that their loss or corruption would have a serious impact on the Department's ability to meet its mission or do its work.[1] Because HVAs are so important, additional security measures are required to protect them from cyberattacks.

In recent years, the federal government has directed its agencies to better secure their HVAs and prioritize the timely remediation of vulnerabilities on organizational systems. The HVA program managed by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is a vital component of the United States' cybersecurity strategy that aims to secure the nation's most important systems and assets. By focusing on these assets, CISA's HVA program targets the limited resources available for cybersecurity to where they are needed most.

CISA has released directives to help identify and remediate vulnerabilities found on HVAs. First, federally operated HVAs must be assessed once every 3 years.[2] In addition, CISA manages an online catalog of known exploited vulnerabilities (KEVs), which are vulnerabilities adversaries have already exploited (that is, taken advantage of) to conduct cyberattacks. [3] For this reason, KEVs carry significant risk to information systems and their remediation is prioritized. The KEV catalog is updated regularly; after updates are published, agencies must scan all systems, including HVAs, for vulnerabilities and remediate any KEVs they discover within 2 weeks.

Beyond CISA's requirements, the Department requires annual penetration testing (simulated cyberattacks that test system security) of systems, including HVAs, that are so mission critical a breach could be expected to have a severe or catastrophic effect on operations, assets, individuals, other organizations, or national security.[4]

Effective management of HVA vulnerabilities is imperative to protect essential data. Mitigating security weaknesses identified through penetration tests and CISA's KEV catalog helps ensure the fulfillment of the Department's mission and its critical data are protected from attackers. For this reason, we focused this audit on the Department's identification and remediation of vulnerabilities on HVAs.

---

[1] Definition based on the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's *CISA Insights*, "Secure High Value Assets (HVAs)" (accessed June 7, 2023).
[2] CISA. Binding operational directive 18-02, available at https://www.cisa.gov/news-events/directives/bod-18-02-securing-high-value-assets (accessed July 25, 2023).
[3] CISA. Binding operational directive 22-01, available at https://www.cisa.gov/news-events/directives/binding-operational-directive-22-01 (accessed July 7, 2023). CISA's KEV catalog is available at www.cisa.gov/known-exploited-vulnerabilities-catalog (accessed July 7, 2023).
[4] Department of Commerce (DOC), June 2019. *Department of Commerce Information Technology Security Baseline Policy* (ITSBP), Version 1.0. Annex B-4: Security Assessment and Authorization (CA) ITSBP Requirements. Washington, DC: DOC.

Objective, Findings, and Recommendations

The objective of this audit was to determine if the Department and its bureaus identify and remediate vulnerabilities on HVAs in accordance with federal requirements. Specifically, we determined the extent that the Department conducted HVA risk and vulnerability assessments within the last 3 years, resolved issues identified during those assessments, and remediated the vulnerabilities published in CISA's KEV catalog by the due date. Appendix A details our audit scope and methodology.

We found that 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. As a result, the Department's HVAs are operating with significant risk due to unresolved vulnerabilities. In fact, as part of this audit OIG successfully exploited security weaknesses on multiple HVAs.

The Department currently operates 65 HVAs, each of which comprises multiple components (such as network devices, servers, and printers) that can add to its complexity. Without an effective process to identify and remediate vulnerabilities, HVAs may be compromised, hindering the Department's mission-essential functions. To prevent this outcome, the Department should not only follow federal best practice standards but also ensure HVAs are protected and vulnerability remediation is prioritized across its bureaus.

I. HVAs Are Operating with Significant Risk Due to Unresolved Vulnerabilities

CISA's HVA program requires penetration testing to identify vulnerabilities on systems. CISA also requires vulnerability scanning to identify KEVs. Although these techniques are similar in that they are both used to identify vulnerabilities in HVAs, each provides its own benefits. Penetration tests can be tightly or broadly scoped and typically involve multiple manual steps to verify their accuracy, while vulnerability scanning is an automated process that involves little human input.

After reviewing HVA penetration tests and KEV scan data, we confirmed that the Department had complied with its testing requirements. However, we found it does not always remediate vulnerabilities identified in those tests according to established timelines, nor does it remediate KEVs within the CISA-mandated 2-week due date.

A. The Department conducts penetration tests as required, but does not remediate issues according to risk-based timelines

CISA and the Department require penetration testing of systems at intervals that are based on the risk of vulnerabilities to those systems. CISA requires penetration testing of HVAs every 3 years, and the Department's baseline security policy requires annual testing of the HVAs for which a breach could have severe or catastrophic effects. CISA or CISA-trained departmental staff may lead the testing, depending on the potential severity of a breach's impact to the HVA.

To determine how well the Department's bureaus complied with CISA and departmental penetration testing requirements, we requested the latest penetration test reports for all 65 departmental HVAs. We found that the Department complied with all testing requirements in place at the time. Overall, 28 of the 65 HVAs had undergone testing.[5] The remaining 40 HVAs had not, either because they were scheduled for upcoming testing, had been categorized as HVAs only recently, or were excused from testing due to a temporary waiver from CISA.[6]

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 being the most potentially harmful and therefore necessitating priority remediation. CISA requires the remediation of critical or high vulnerabilities identified during CISA-led penetration tests within 30 days. The Department, however, requires remediation of vulnerabilities identified during its penetration tests between 14 and 90 days. Vulnerabilities in external systems, which the public can access through the Internet, must be remediated in 14 days, while those found in internal systems are remediated according to their impact level (see table 1).

Table 1. CISA and Departmental Remediation Requirements (in days)

Vulnerability Impact Level	CISA Requirements for All Systems	Departmental Requirements for External Systems	Departmental Requirements for Internal Systems
Critical	30	14	30
High	30	14	90
Medium	No requirement	14	90
Low	No requirement	No requirement	No requirement

Source: OIG analysis of the Department's internal cybersecurity policy and CISA's binding operational directive 18-02

To determine if the Department remediated vulnerabilities on HVAs in accordance with these requirements, we assessed the 28 applicable penetration tests. Seven of the tests were led by CISA and 21 by the Department. We limited our review to vulnerabilities designated in the penetration test as critical or high, as well as medium vulnerabilities that we determined to be of interest.

The vulnerabilities found in the 7 CISA-tested systems had been remediated within CISA's deadline, but 17 of the 21 Department-tested systems had one or more

[5] This number includes penetration tests from bureaus that were not required to conduct them; the bureaus conducted the tests of their own accord.

[6] CISA waived the penetration test requirement for some HVAs until the first quarter of FY 2023. As of the first quarter of FY 2023, these systems must now meet the requirement to test once every 3 years.

vulnerabilities that were not remediated by the Department's risk-based deadline. Across the 17 systems, a total of 88 vulnerabilities were overdue for remediation. We reviewed remediation evidence for the 88 vulnerabilities and noted that 58 were overdue by an average of 174 days (see table 2 for a breakdown).

Table 2. Number of Overdue Vulnerabilities Observed Across the 17 HVAs

Vulnerability Impact Level	Number of HVAs with Overdue Vulnerabilities[a]	Number of Overdue Vulnerabilities	Average Days Overdue
Critical	5	11	196
High	9	24	178
Medium	11	23	147

Source: OIG analysis
[a] Some HVAs had vulnerabilities across multiple impact levels.

Not only was remediation overdue, but we noted significant delays in documenting remediation efforts. Department policy[7] dictates that security personnel develop a vulnerability remediation plan of action and milestones (POA&M) if a vulnerability cannot be remediated within 30 days of its discovery. We found that POA&Ms had not been created for 32 of the vulnerabilities that had not been remediated within 30 days. In fact, some vulnerabilities went as long as 90 days without a POA&M, and some system personnel did not develop POA&Ms until we requested remediation evidence for the delays.

Overdue remediation and ineffective POA&M management represent a systemic problem in how the Department manages vulnerabilities on its HVAs. Risk-based timelines are used to prioritize remediation efforts because they are based on the impact an exploited vulnerability would have on the system; therefore, by allowing vulnerabilities to remain unresolved for months longer than their required deadline, the Department left its systems vulnerable to cyberattacks and exploitation. In addition, POA&Ms are one of the primary ways to inform leadership and stakeholders of system-related risk. Without POA&Ms, leadership could be making risk-based decisions based on incomplete or inaccurate information, putting the Department's data at risk.

B. The Department's HVAs are operating with known exploited vulnerabilities for prolonged periods

In addition to the penetration testing requirement, CISA requires the Department to identify and remediate KEVs. CISA guidance prioritizes the remediation of KEVs over any other security vulnerability because KEVs are actively exploited by attackers and thus pose a significant risk. The timeline for remediating a KEV is 2 weeks from the date

[7] DOC ITSBP, Annex B-4: Security Assessment and Authorization (CA) ITSBP Requirements.

it was added to the KEV catalog. This due date is based on the amount of risk posed to the system; it may be adjusted in the case of grave risk to the federal enterprise.[8]

We reviewed KEV-specific vulnerability reports for 63 of the Department's 65 HVAs[9] and found that 30 systems had at least one overdue KEV remediation. We found that as of February 2023, the Department had not remediated 103 of the 872 published KEVs within CISA-defined timelines; the average delay was 270 days. Overall, we found that six of the eight bureaus that operate HVAs had overdue KEVs, with one bureau responsible for approximately 92 percent of the overdue KEVs. We discuss the reasons below in subfinding C.

Many KEVs affected multiple components within HVAs, so if an attacker gained authorization to one affected component, they could use the same method to compromise multiple components. For example, we were able to successfully exploit one KEV that would allow an attacker to escalate their privileges and possibly gain administrative rights to 135 components in the same HVA.

C. The Department's lack of prioritization led to delays in remediating vulnerabilities

We contacted bureaus with overdue remediations to determine why the remediations were delayed. System security staff cited various reasons, including lack of time and resources or technological delays (such as dependencies between systems, decommissioning system components, and system migrations). These are common reasons that can be observed in all information system types. However, the HVA program is meant to identify and prioritize critical systems for better security.

Ultimately, we determined that lack of prioritization is at the center of most of the delays. For example, some bureaus delayed remediating vulnerabilities in an HVA because they were planning to migrate or decommission the HVA. The lack of available staff time and resources also indicated that HVAs were not prioritized.

Bureaus depend on the Department to set baseline HVA and vulnerability management requirements at the enterprise level. Given the lack of prioritization, we reviewed departmental policy to assess the Department's guidance for managing HVA vulnerabilities. We noted the policy did not tailor requirements to address the risk these vulnerabilities pose to the Department's HVAs:

- The Department has yet to implement additional CISA-recommended security controls for HVAs, such as requiring vulnerability scanning every 72 hours to help quickly identify and remediate KEVs.

- CISA requires 30 days at most to remediate high and critical vulnerabilities discovered during CISA penetration tests on HVAs, with a faster timeline for

[8] CISA. Binding operational directive 22-01, available at https://www.cisa.gov/news-events/directives/binding-operational-directive-22-01 (accessed July 7, 2023).
[9] Two HVAs are cloud based, so the Department is not responsible for vulnerability remediation.

KEVs; however, the Department allows up to 90 days for high vulnerabilities on internal systems.

- The Department did not require penetration testing of its HVAs until January 2023, even though CISA made penetration testing a requirement in 2018.

There are significant risks to not prioritizing remediation of these vulnerabilities on HVAs. HVAs are the most important systems in the Department, and the types of vulnerabilities we reviewed have been proven to be usable by adversaries. In fact, finding II of this report describes how we were able to successfully exploit several previously identified vulnerabilities, illustrating that an attacker could do the same.

Recommendations

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.

II. OIG Successfully Exploited Security Weaknesses on Multiple HVAs

Penetration testing allows system staff to identify exploitable vulnerabilities through simulated cyberattacks. As noted in finding I, 28 of the Department's 65 HVAs had undergone penetration testing. We reviewed the test results and identified recurring vulnerability types, such as default login credentials, unencrypted passwords, and outdated applications.

We then judgmentally selected 7 of the 65 HVAs and conducted manual penetration testing[10] on them to determine if they were vulnerable to those recurring vulnerability types. We also reviewed vulnerability scans and attempted to exploit a limited number of KEVs observed on each of the selected HVAs. In all tests, we used standard penetration testing tools from inside the network with general user privileges (not from outside the systems' network defenses).

We found that all seven of the HVAs we selected had at least one of five recurring vulnerability types. We also found that the vulnerability scanners the Department used did not always detect KEVs and other vulnerabilities as they should.

[10] See appendix A for more information on our manual penetration testing.

A. *All HVAs in our review had at least one exploitable vulnerability type*

Overall, we discovered 45 vulnerabilities—24 critical, 16 high, and 5 medium—affecting multiple components within the seven HVAs (see table 3).[11] These HVAs perform important functions, such as warning U.S. citizens of natural disasters, processing patents, and other mission-essential functions at the Department.

Table 3. Vulnerabilities Across HVAs in Our Sample by Recurring Vulnerability Type

	Identification & Authentication Failures	Sensitive Data Exposure	Security Mis-configurations	Vulnerable & Outdated Components	Improper Input Validation
HVA 1	-	1	-	1	-
HVA 2	-	-	-	2	-
HVA 3	1	1	-	4	1
HVA 4	3	1	-	4	-
HVA 5	2	1	-	2	-
HVA 6	2	2	1	5	-
HVA 7	8	1	-	1	1

Source: OIG analysis

We discuss each of these vulnerability types and their potential impact below.

- **Identification and Authentication Failures:** We found identification and authentication failures in all but two tested HVAs. The five HVAs had improperly configured login credentials (a username and password combination used to access a system), and some used default credentials or no credentials at all.

  When new software is installed, it can come without credentials or with preset default administrative credentials, which are available online or in the software's user manual. If the preset credentials are not changed, an attacker can use them to gain administrative or user access to the susceptible system. These types of attacks carry significant risk but are easily mitigated by changing credentials on new software and hardware.

- **Sensitive Data Exposure:** We identified sensitive data exposure on two HVAs at one bureau, three at another bureau, and one at a third bureau. In each instance, we found the HVAs were configured to send and receive sensitive data

[11] Once notified of vulnerabilities, most bureaus took corrective actions to resolve them; however, this was out of the scope of our audit, and we did not validate the sufficiency of their actions.

in HTTP, a protocol that transfers unencrypted data between two computers over a network.

Because HTTP is unencrypted, the transferred data is readable by anyone monitoring the communication, including an attacker. A simple way to protect data is to configure systems to communicate using HTTPS, an encrypted form of HTTP that has become standard across the Internet. Even if properly encrypted data is intercepted, it cannot be read by anyone other than a recipient with the correct decryption key.

Encrypted communication is especially important when transmitting passwords. On one system alone, we found 11 different login pages configured to use HTTP, not HTTPS. If an attacker intercepted unencrypted login credentials, they could log into the relevant application and make unauthorized changes or steal sensitive information.

- **Security Misconfigurations:** We identified an HVA at one bureau that had security misconfigurations, in which software or hardware configurations were not as secure as possible. Through our penetration testing, we exploited the HVA's misconfigured network management protocol by using publicly available hacking tools. This allowed us to extract information related to the HVA's software components, usernames, devices, open communication ports, and storage information.

  This form of information extraction, known as enumeration, gives attackers a roadmap of how and what to exploit when they gain entry to a system.

- **Vulnerable and Outdated Components:** We discovered vulnerable and outdated components in all tested HVAs. This makes these components easy targets, as they can be exploited by the same method. Many were also KEVs; our penetration testing found KEVs on all but two of our tested HVAs, and in some cases one KEV affected multiple components in the same HVA. In fact, 137 components in one bureau's HVA were vulnerable to a KEV that would allow an attacker to access the HVA and escalate privileges to perform unauthorized administrative changes.

  When software is outdated, it may not have the security updates a newer version has, making it susceptible to attacks. Vulnerabilities in outdated software range in severity, but in some cases they can be a gateway to access a system, send it commands, steal its data, or render it unusable. One common method for discovering outdated system components or software is to use a vulnerability scanner. Vulnerability scanners are periodically updated to check for various security issues, including outdated or unsupported software versions. Consequently, if the scanner itself is not updated, it may fail to identify vulnerabilities.

Notably, we identified one bureau using vulnerability scanning software that had been outdated for over a year. Through our penetration testing, we discovered a KEV the bureau was unaware of; we discuss this in detail in subfinding B.

- **Improper Input Validation:** We identified improper input validation configurations in two bureaus' HVAs. Improper input validation occurs when certain fields or forms are not configured to reject invalid user input. By exploiting this vulnerability, we carried out a cross-site scripting attack, a type of attack that allows an adversary to insert malicious code into an otherwise trusted webpage. When an unknowing user connects to the compromised webpage, the malicious code compromises the victim's browser. The attacker can use the malicious code to highjack the user's control and rewrite content or transmit sensitive information, such as passwords stored in the user's browser.

When vulnerabilities exist across multiple systems on the same network, attacks can be repeated more quickly and easily across the network. CISA recommends that entities in an organization share information about vulnerabilities with each other to help prioritize the remediation of vulnerabilities that affect HVAs across the organization. However, while the Department facilitates meetings among the bureaus' chief information officers, it does not require the chief information officers to share information about their bureaus' HVA vulnerabilities. Our testing revealed multiple systems with recurring types of vulnerabilities, which we were able to exploit. An adversary could carry out the same attacks we did.

B. Vulnerability scanners do not always identify KEVs and other vulnerabilities in HVAs

Automated vulnerability scans are the foundational step to identifying KEVs and other vulnerabilities. To ensure a scanner finds all weaknesses, it must be updated and configured to scan all components of an HVA. CISA recommends conducting discovery and system scans on HVAs every 72 hours to ensure the HVAs' inventories remain accurate and to quickly determine if any HVA has newly published KEVs.

As we briefly noted in subfinding A, we found KEVs on five of the seven tested HVAs. Some of these KEVs had not been identified during automated vulnerability scans because the scanners were misconfigured:

- After reviewing KEV reports for one bureau, we observed a KEV that would allow an attacker to read the configuration and source code files associated with an application on two HVA components. If the attacker uploaded malicious code, this KEV could be used to execute the code remotely. Through our penetration testing, we identified the same KEV on two other components within the HVA's boundary; however, the KEV report did not show the KEV affecting these components.

- At another bureau, we identified one KEV on seven HVA components. This KEV was also not in the HVA's KEV report. We informed system security staff and determined that the scanner did not pick up the KEV because of customized

configurations made during the system's installation. After we alerted security staff, they tested the system and identified the KEV on four other system components.

- We discovered a KEV on one component in one bureau's HVA. As with the other instances, this KEV was identified on some components within the HVA but not on the component we discovered it on, and it had not been caught by the HVA's vulnerability scanner. This KEV could allow an attacker to execute code remotely and gain full control of the HVA.

- The bureau responsible for maintaining current versions of all scanning software and tools used an outdated version of vulnerability scanning software for an entire year. Staff from the bureau asserted they were aware of the issue, and the bureau later updated the software. As we have noted, however, an outdated vulnerability scanner does not affect only the system operating it; it also may affect other systems that depend on the scanner. The outdated version of the scanning software the bureau was using could not produce customized KEV reports. After it was updated, we requested an updated KEV report, which flagged several KEVs. Our manual testing also found one KEV that was not in the KEV report the bureau provided. After following up with staff, we found the scanner was not configured to scan all components within the HVA's security boundary.

Although the Department has vulnerability scanning procedures for its bureaus to follow, its vulnerability management and scanning policy does not include a process or mechanism to ensure all bureaus update and correctly configure their vulnerability scanners. When scanners are not configured properly, KEVs or other critical vulnerabilities may go undiscovered.

Department officials stated they are updating the policy. However, at the time of our review, an updated policy had not yet been officially implemented.

Recommendations

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

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.

Other Matter: USPTO Asked the Department to Downgrade Its HVAs

In February 2023, we were notified that the United States Patent and Trademark Office (USPTO) was asking to downgrade all its HVAs to non-HVAs. At the time of our audit, USPTO was the Department's second-largest HVA operator. USPTO's rationale for the request was that its systems did not perform any of the Department's primary mission-essential functions.[12] The bureau also did not believe the loss, misuse, disclosure, or unauthorized access to or modification of any of its current HVAs would have a debilitating impact on its mission.

However, USPTO's own description of itself and its mission asserts its significance and indicates that USPTO is fulfilling a vital function for the nation. USPTO describes itself on its website as the federal agency that grants U.S. patents and registers trademarks, a function that includes processing and storing patents, intellectual property, and businesses' intellectual information as well as fulfilling the mandate of a constitutional clause. The bureau takes responsibility for protecting new ideas and investments that help American industry flourish.[13]

By the end of our fieldwork in May 2023, the Department had not decided whether to grant USPTO's request. Instead, the Department returned the request to USPTO, saying that it would decide after USPTO followed the correct HVA downgrade process.

Given USPTO's position as a central authority for collecting and processing patents and other intellectual property, we believe a wholesale downgrade of all HVAs in USPTO appears to conflict with the Department's HVA program's goal of prioritizing its most valuable assets and information. However, in September 2023, the Department's Chief Information Officer agreed to downgrade the majority of USPTO's HVAs. Therefore, the Department should reevaluate how it identifies all of its HVAs to ensure that it is consistently protecting and prioritizing its mission-critical systems.

[12] Primary mission-essential functions directly support the government functions needed to lead and sustain operations during a national emergency.
[13] USPTO. "About Us." Available online at https://www.uspto.gov/about-us (accessed June 23, 2023).

Summary of Agency Response and OIG Comments

On September 12, 2023, 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. We accepted the technical comments, as appropriate, and included them in the final version of this report.

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

Appendix A: Objective, Scope, and Methodology

Our audit objective was to determine if the Department and its bureaus identify and remediate vulnerabilities on HVAs in accordance with federal requirements. To do so, we

- analyzed HVA-related artifacts such as system security plans, POA&Ms, penetration test reports, vulnerability scan results, and other necessary documentation for all 65 of the Department's HVAs;
- reviewed bureaus' compliance with the following applicable internal controls, provisions of law, and mandatory guidance:
    - Department of Commerce enterprise cybersecurity policy, version 1,
    - the Department's information technology security baseline policy,
    - bureau vulnerability management policies,
    - CISA binding operational directive 18-02,
    - CISA binding operational directive 22-01,
    - National Institute of Standards and Technology special publication 800-53, revision 5, *Security and Privacy Controls for Information Systems and Organizations;* and
- interviewed the Department's Office of the Chief Information Officer staff responsible for developing IT policies, procedures, and operational guidelines and monitoring the Department's overall HVA security posture.

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.[14]

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 HVA vulnerability management process. Our work was broken down into the following sub-objectives:

[14] 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).

- **Sub-objective A:** To determine whether the Department conducted HVA risk and vulnerability assessments within the last 3 years, we requested and assessed penetration tests for the Department's 65 HVAs.

- **Sub-objective B:** To determine whether the Department resolved issues identified during those assessments, we assessed bureaus' penetration tests, POA&M data, and other resolution-supporting evidence.

    - Using the vulnerability identification date in the penetration test report publication date or the dates in the report, we determined the appropriate risk-based due date. We then compared those due dates against the actual completion dates documented in POA&Ms provided by the bureau in other remediation evidence.

- **Sub-objective C:** To determine if the Department identified and remediated KEVs within CISA-defined timelines, we collected KEV data from each HVA and assessed how much each exceeded CISA's remediation requirements.

- **Additional Assessment:** To validate the exploitability of KEVs and recurring vulnerability types identified in sub-objectives A and B, we judgmentally[15] selected seven HVAs and conducted our own penetration testing:

    - First, to test for false positives, we reviewed each HVA's KEV data and selected a limited number of KEVs known to exist on the selected HVAs. We then reviewed the results of the 21 available penetration tests and identified recurring vulnerability types such as default credentials, unencrypted passwords, and outdated applications.

    - Next, we developed predetermined testing steps and methodologies to attempt to exploit previously identified KEVs and recurring vulnerability types.

    - Lastly, we provided each target system's security staff with rules of engagement. After agreeing on a course of action, we worked with the staff to connect to the target HVAs. To do so, staff provided us with each system's IP ranges within scope, VPNs, government-furnished equipment (if necessary), and sometimes low-level account credentials. We then used virtual machines with Kali Linux instances to perform our testing.

We conducted our review from August 2022 through May 2023 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. § 401 et seq.), and Department organization order 10-13, dated October 21, 2020. We performed our fieldwork remotely.

[15] The seven systems were selected based on various criteria, including but not limited to the number of present KEVs, the system's Federal Information Processing Standards Publication 199 categorizations (low, moderate, or high), the system's CISA-designated HVA breach impact level, and whether the system had been penetration tested before.

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 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.

Appendix B: Agency Response

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

September 11, 2023

MEMORANDUM FOR: Peggy E. Gustafson
Inspector General

FROM: André V. Mendes ANDRE MENDES Digitally signed by ANDRE MENDES Date: 2023.09.11 16:58:53 -05'00'

SUBJECT: Department of Commerce's Concurrence to the Office of Inspector General's Draft Report, *Security Weaknesses in the Department's Mission-Critical High Value IT Assets Leave the Assets Vulnerable to Cyberattacks* (August 8, 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, *Security Weaknesses in the Department's Mission-Critical High Value IT Assets Leave the Assets Vulnerable to Cyberattacks (August 8, 2023).*

The DOC Office of Chief Information Officer (OCIO) reviewed the draft report and generally concurs with the findings and recommendations. OCIO recognizes the need to increase visibility and insight, address gaps in people, processes, and technology, and reduce overall risk. The Department has made significant strides in updating policies, standards, and handbooks that address various cybersecurity functions and disciplines. Specifically, to address the gaps identified in the draft report, we are in final stages of review and approval for policy documents that address vulnerability management, information security continuous monitoring, and High Value Asset (HVA) management. The findings and recommendations contained in the report will support us in ensuring the Department's high value IT assets are appropriately protected and remain resilient.

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.

Attachments

cc: MaryAnn Mausser
Joselyn Bingham
Ryan A. Higgins
Maria Hishikawa

Department of Commerce Technical and Editorial Comments
on the OIG Draft Report: *Security Weaknesses in the Department's Mission-Critical High Value IT Assets Leave the Assets Vulnerable to Cyberattacks*
(OIG-22-432, August 8, 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.

National Oceanic and Atmospheric Administration (NOAA)

General Comments

None

Recommended Changes for Factual/Technical Information

Page 4, second paragraph, last sentence. The National Oceanic and Atmospheric Administration (NOAA) provided information demonstrating that there was a Plan of Action and Milestones (POA&M) in place for the outstanding Known Exploited Vulnerabilities (KEVs) and vulnerabilities found in the assessed High Value Assets (HVAs). We are requesting that this be changed in the report to reflect NOAA's effort to manage all vulnerabilities within all NOAA systems.

Page 5, Bullet number 1. While the department does not have a policy to require vulnerability scanning every 72 hours, NOAA has implemented this requirement as part of our internal Continuous Diagnostics and Mitigation (CDM) Program to ensure accurate vulnerability identification and remediation. We are requesting that this is added to the report.

Page 6, Bullet number 1. NOAA since 2015 has required penetration testing for all HIGH impact systems which includes the majority of our HVAs. We are requesting that this is added to the report.

U.S. Patent and Trademark Office (USPTO)

General Comments
The USPTO is proud of the work we do and take seriously our responsibility to protect the new ideas and investments that help American industry flourish. While we appreciate the OIG's feedback about effective management of High Value Asset (HVA) vulnerabilities in this audit, we are concerned that the OIG's discussion in the "Other Matter" section is misleading and does not reflect all of the facts related to how agencies, including the USPTO, determine which assets are considered high value under Office of Management and Budget (OMB) M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program* (December 10, 2018). For clarity, we offer the following additional context.

The USPTO initially designated 26 of its systems as HVAs in 2019, based on our understanding at the time of what constituted mission essential functions and in light of

Department of Commerce (DOC) guidance. In 2023, the USPTO determined it had incorrectly applied the M-19-03 guidance when designating these systems. Specifically, in January 2023, the USPTO reviewed its designations of systems as HVAs and determined that it does not serve National Security and Primary Mission Essential Functions (PMEF), as defined in the criteria for the "Mission Essential" category of HVAs under M-19-03. Therefore, the USPTO determined it is not required to report any "Mission Essential" HVAs in accordance with M-19-03. This analysis resulted in the decision to de-list all of the USPTO's HVAs, described by the OIG in the "Other Matter" section. Subsequently, in May 2023, the USPTO reassessed its HVAs under the "Informational Value" category described in M-19-03 and determined that a small sub-set of the previously identified HVAs should retain the HVA designation.

The USPTO agrees with the OIG that its decision to downgrade many of its HVAs may be a catalyst for the entire Department to reevaluate how HVAs are identified to ensure that DOC and its bureaus and agencies are consistently protecting and prioritizing mission-critical systems.

01 12000 00 432