AUDIT REPORT

Audit of the Department's Vulnerability Reporting and Resolution Program

REPORT NO. OIG-26-002-A

NOVEMBER 20, 2025

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

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Office of Audit and Evaluation
Washington, DC 20230

November 20, 2025

MEMORANDUM FOR: Paul M. Dabbar
Deputy Secretary of Commerce

FROM: Arthur L. Scott Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *Audit of the Department's Vulnerability Reporting and Resolution Program*
Report No. OIG-26-002-A

Attached is the final report on our audit of the Department's vulnerability reporting and resolution program's effectiveness in accepting, analyzing, and resolving vulnerabilities identified on the Department's internet-accessible systems. We will post the report on our website per the Inspector General Act of 1978, as amended (5 U.S.C. §§ 404, 420).

Within 60 calendar days, please provide an action plan addressing the report's recommendations, as required by Department Administrative Order 213-5.

We appreciate your staff's cooperation and professionalism during this audit. If you have any questions or concerns about the report, please contact me at 202-792-4192 or Director for Cybersecurity Chuck Mitchell at 202-809-9528.

Attachment

Audit of the Department's Vulnerability Reporting and Resolution Program

Audit Report OIG-26-002-A
November 20, 2025

What We Audited | Our objective was to assess the effectiveness of the Department's program for managing public-reported vulnerabilities in its public-facing information technology systems.

Why This Matters | To foster economic growth and opportunities, the Department relies on internet-accessible systems such as government websites, web and mobile applications, third-party services, and databases, which allow the Department to interact with the public by providing services like weather prediction, processing patent applications, and supplying international trade information. With this public accessibility comes an inherent risk of cyberattacks as internet-accessible systems are exposed to global threats and do not have the full protection of internal network defenses.

Recognizing this inherent risk, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued *Develop and Publish a Vulnerability Disclosure Policy*, which states, "[c]ybersecurity is a public good that is strongest when the public is given the ability to contribute." This directive requires that each federal agency establish a vulnerability disclosure policy (VDP) that authorizes members of the public (security researchers) to identify and report vulnerabilities on internet-accessible government systems.

What We Found | The Department established a vulnerability disclosure program; however, it was not fully effective. Specifically, the Department's VDP did not include all internet-accessible systems, the VDP's testing guidelines restricted the tools public security researchers could use to identify system vulnerabilities, the Department did not always fully remediate reported vulnerabilities, and the Department did not always remediate vulnerabilities within established deadlines.

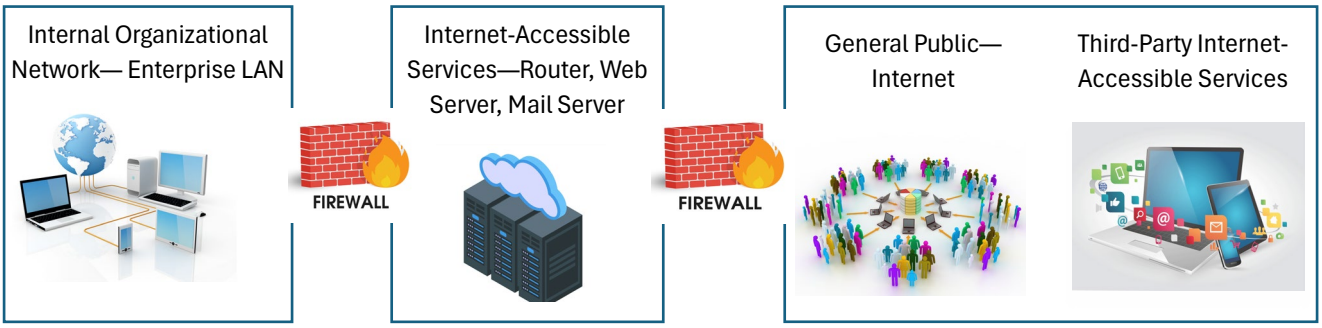
What We Recommend | We made three recommendations to the Department to revise the testing scope to align with CISA's VDP policy, update and implement VDP procedures, and work with bureaus to implement an automated solution to prompt action on delayed vulnerability remediation. The Department concurred with our recommendations and is working to implement them.

Contents

Introduction

To foster economic growth and opportunities for all communities, the U.S. Department of Commerce relies on internet-accessible (that is, public-facing) systems[1] such as government websites, web and mobile applications, third-party services,[2] and databases. These internet-accessible systems allow the Department to interact with the public by providing services like weather prediction, processing patent applications, and supplying international trade information. Along with this public accessibility comes an inherent risk of cyberattacks as internet-accessible systems are exposed to global threats and do not have the full protection of internal network defenses (see figure 1).

Figure 1. The Department's Internet-Accessible System Architecture



Source: OIG, derived from an analysis of the Department's system architecture

Recognizing this inherent risk, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued *Develop and Publish a Vulnerability Disclosure Policy*,[3] which states that "[c]ybersecurity is a public good that is strongest when the public is given the ability to contribute." This directive requires that each federal agency establish a vulnerability disclosure policy (VDP) that authorizes members of the public (security researchers) to identify and report vulnerabilities[4] on internet-accessible government systems.

---

[1] The Cybersecurity and Infrastructure Security Agency broadly defines internet accessible as any system or service that is accessible by the internet; each agency defines its boundary for applications differently. CISA. September 2, 2020. *Develop and Publish a Vulnerability Disclosure Policy.* Binding Operational Directive (BOD) 20-01,18.

[2] A third-party service is a system or service not directly managed or owned by an agency but providing resources or services to an agency.

[3] CISA, *Develop and Publish a Vulnerability Disclosure Policy,* 1.

[4] CISA defines a vulnerability as a "[w]eakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." CISA, *Develop and Publish a Vulnerability Disclosure Policy*, 2.

At a minimum, CISA requires that agency VDPs include (1) what systems public security researchers can test, (2) types of testing public security researchers can perform, (3) a general description of how to submit vulnerability disclosures, (4) a commitment not to pursue legal action against the public security researcher, (5) what communication the public security researcher can expect to receive from the agency, and (6) a descriptive summarization of change history as the policy is updated. Agencies must meet these minimum requirements, but CISA allows agencies to tailor requirements to specific security needs.

VDPs grant public security researchers the legal authorization to test internet-accessible systems for vulnerabilities and submit a vulnerability disclosure, which allows the agency time to assess and remediate[5] vulnerabilities before public disclosure. VDPs also encourage public security researchers to test systems for vulnerabilities using tools and methods that otherwise could be abused by an adversary. VDP reporting is an immense benefit as it allows the agency to remediate vulnerabilities, thus mitigating the risk of compromising the system before the vulnerabilities are exploited by malicious actors.

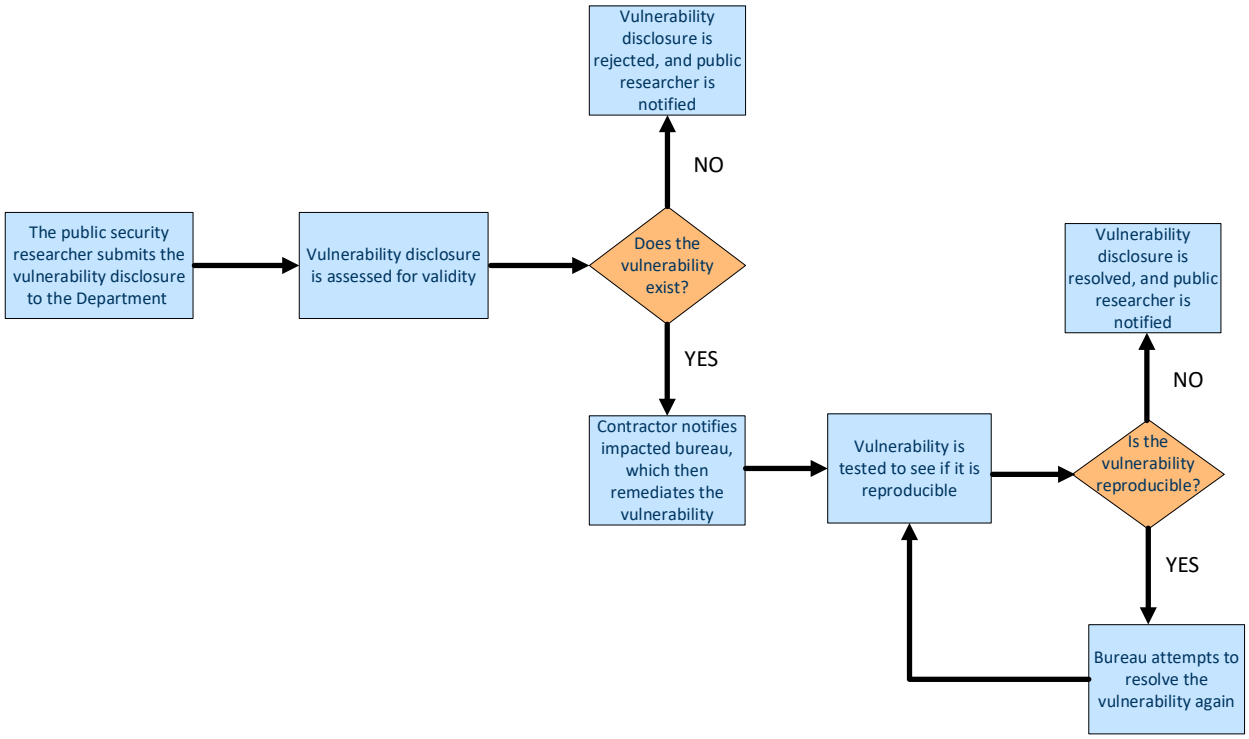
In March 2021, the Department published its VDP[6] and developed a program to support the policy. Initially, the Department managed the program; however, since 2022, a third-party contractor has managed the policy's implementation. Figure 2 shows the Department's process for disclosing and resolving vulnerability disclosures. [7]

[5] Remediation is the process of correcting known defects, vulnerabilities, or weaknesses to remove or eliminate the related risks. U.S. Department of Commerce. April 2025. *Vulnerability Management Standard Office of Cybersecurity and IT Risk Management (OCRM),* Version 1.1, 22.

[6] U.S. Department of Commerce. January 2023. *Vulnerability Disclosure Policy*.

[7] In this report, we use "remediation" to describe fixing the vulnerability itself. We use "resolution" when describing the vulnerability disclosure process in its entirety.

Figure 2. The Department's Vulnerability Disclosure and Resolution Process



Source: OIG analysis of the contractor's documentation and interviews with VDP managing staff

Objective

Our objective was to assess the effectiveness of the Department's program for managing public-reported vulnerabilities in its public-facing information technology systems. Appendix 1 details our scope and methodology.

Findings and Recommendations

Summary: We found that the Department established a vulnerability disclosure program; however, the program was not fully effective. Specifically:

- The VDP did not include all internet-accessible systems.
- The VDP's testing guidelines restricted the tools that public security researchers could use to identify system vulnerabilities.
- The Department did not always fully remediate reported vulnerabilities.
- The Department did not always remediate vulnerabilities within established deadlines.

Without an effective vulnerability disclosure program, the Department cannot safeguard its internet-accessible systems, leaving them susceptible to potential compromise and exploitation.

The Department's VDP Has Gaps in Key Areas That Reduce the Program's Effectiveness

Although the Department's VDP supports the acceptance and resolution of vulnerability disclosures, we found shortcomings in key areas that reduce the program's overall effectiveness. At its core, an agency's VDP should define the scope of testable systems and acceptable testing methods. We identified issues in both areas. Specifically, the Department's VDP did not include all internet-accessible assets, and testing guidelines restricted public researchers from using common testing tools.

The VDP Did Not Include All Internet-Accessible Systems

Rather than broadly defining its VDP scope as all internet-accessible systems, the Department limited its VDP scope to a list of 64 internet-accessible websites (for example, www.doc.gov).[8] To determine whether the VDP scope accurately reflected the Department's internet-accessible systems, we compared it against our independently

[8] The Department used a CISA template and BOD 20-01 guidance to specify the initial scope of its VDP. However, that same guidance noted that "[a]t 2 years after the issuance of this directive, all internet-accessible systems or services must be in scope of your policy."

verified internet-accessible inventory. We found that 22 Department-owned or -operated websites were excluded from the VDP. Of those 22 websites, the Department disputed ownership of 6. Department personnel told us that the six disputed websites were owned and operated by a third-party service and therefore the Department was not required to list them in its VDP.[9]

However, the Department owns the accounts and data hosted on the third-party services; therefore, any compromise could negatively impact the Department. For example, we found a password to a bureau system on a public third-party website. If that password had been discovered by a malicious actor, it could have been used to attack that system. Because the Department's VDP does not include third-party services, a public security researcher might not report this vulnerability or could face legal ramifications by doing so.[10]

Additionally, we found the policy's focus on websites inherently excluded systems or services that are internet-accessible but not accessible through a website (for example, a file transfer system or a mobile application). In fact, our review of the Department's network[11] identified more than 500 internet protocol (IP) addresses that were internet accessible but not associated with a website. Although not directly associated with a website, these systems store data and provide important services, such as network management. If compromised, these systems could be used to gain unauthorized entry into the Department's protected network.

In addition, our analysis found that the Department failed to establish a process to continuously update the VDP scope. Instead, the Department relied on an ad hoc manual process to update its list of internet-accessible websites, which had not been updated since 2022. When asked why the VDP scope was limited to specific websites instead of all internet-accessible websites, Department leadership stated that the program's intent was to include all internet-accessible assets and reasoned that limited VDP coverage would allow them to focus on prioritizing critical systems first and address bureau concerns.

The VDP's Testing Guidelines Restricted the Tools That Public Security Researchers Could Use to Identify System Vulnerabilities

In addition to limiting what systems could be tested, the Department contractor's reporting portal also limited what tools could be used for testing. We found that the VDP contractor's

[9] BOD 20-01 encourages the VDP to be applied as widely as possible and account for nuances such as when the agency does not have the authority to authorize testing on software as a service. In such a case, one BOD recommendation is to work with the service provider to establish how a third-party asset can be added to a VDP.

[10] Only websites published in the VDP are legally testable.

[11] For more details on our testing, see appendix 1.

reporting portal prohibited the use of automated scanners commonly used by public security researchers to identify vulnerabilities.[12] To determine whether this prohibition was widespread, we assessed all 24 Chief Financial Officers Act of 1990[13] agencies and found that only 3 agencies (13 percent), including the Department, banned the use of these automated testing tools. When we brought this to the attention of Department officials, they stated that they were unaware that automated tools were banned and promptly removed the language prohibiting the use of automated tools from the contractor's reporting portal.

Taken together, restricting what Department internet-accessible systems the public security researchers test and how they test the systems increases the risk that they will not identify vulnerabilities. In fact, we employed automated tools to test Department systems excluded from the VDP.[14] Our testing confirmed two concerns: potential vulnerabilities (issues that might pose a risk) existed on 18 of the 22 unlisted websites, and exploitable vulnerabilities (those that could be actively used) existed on 6 unlisted IP addresses or websites. While including systems in the VDP does not guarantee vulnerabilities will be found, it does provide public security researchers with a legal way to test systems and report vulnerabilities.

Recommendation

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

1. Revise the Department's VDP testing scope to align with CISA's BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, which would include testing all internet-accessible systems.

---

[12] National Institute of Standards and Technology (NIST). September 2011. *Information Security* states that "automated tools are often able to recognize patterns and relationships that may escape the notice of a human analyst, especially when the analysis is performed on large volumes of data." NIST Special Publication 800-137,12.

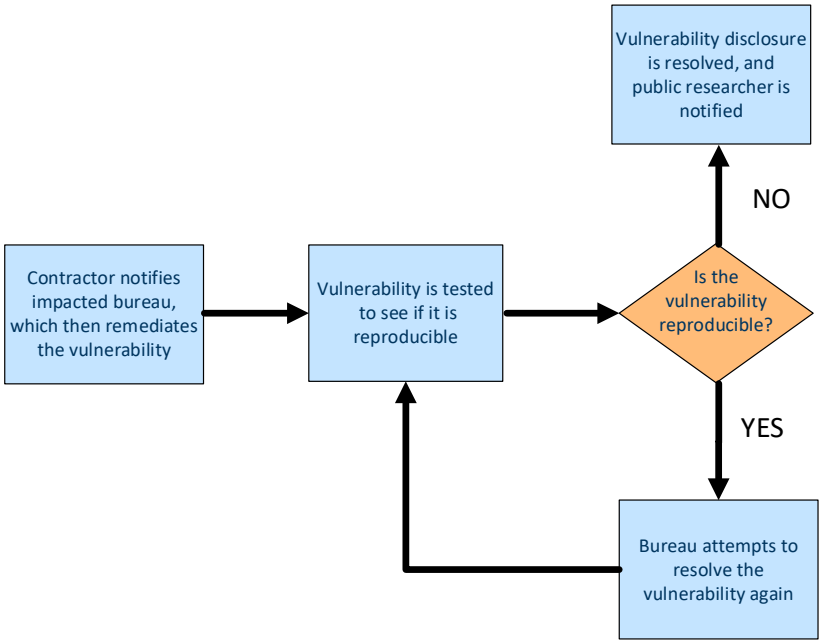
[13] Pub. L. No. 101-567. The act gave the Office of Management and Budget authority and responsibility for directing federal financial management, modernizing the government's financial management systems, and strengthening financial reporting. The act covers 24 agencies, including the Department.

[14] We performed manual testing from outside of the Department's security perimeter, using publicly accessible security tools to mimic the methods and environment of a public security researcher or malicious actor.

The Department Did Not Always Fully Remediate Reported Vulnerabilities

Once the Department confirms that a reported vulnerability exists, it is crucial that the Department remediate the vulnerability. Resolving vulnerability disclosures is a two-step process: (1) the bureau remediates the identified vulnerability and (2) the Department's contractor tests the vulnerability to verify that it is fully remediated, that is, not reproducible (see figure 3). When a public security researcher submits a vulnerability disclosure, they provide the location where they found the vulnerability and steps to reproduce their results. While the public security researcher may identify a specific instance of a vulnerability, they may not identify everywhere that the vulnerability exists on the website. This highlights why a system-wide approach to remediation is crucial.

Figure 3. Vulnerability Resolution Process



Source: Analysis of the contractor's documentation and interviews with VDP managing staff

To determine whether the Department fully remediated vulnerabilities, we assessed 71 resolved vulnerability disclosures.[15] We attempted to reproduce vulnerabilities on both the location identified in the original submission and locations elsewhere on the website. Our testing found that 57 reported vulnerabilities (80 percent) were fully remediated but 14 (20 percent) were not. Of those 14 vulnerabilities, we were able to replicate 5 in their

[15] At the time of our data collection, the Department had closed 73 vulnerability disclosures. Prior to our assessment, we removed two disclosures from our testing sample as they were pending review.

reported location and 9 in different locations on the same website. In all cases, the Department had indicated that the vulnerability was remediated, and the contractor had verified the fix.

We followed up with the Department bureaus and the VDP contractor to determine why the 14 vulnerabilities persisted. For the five vulnerabilities reproduced in the location specified by the public security researcher, the contractor had incorrectly validated that they had been remediated. When we met with the contractor and the most-impacted bureau's personnel to discuss vulnerabilities reproduced in locations outside of the location specified in the original vulnerability disclosure, both stated that remediation efforts were intentionally limited to locations identified by the public security researcher and were not focused on system-wide mitigation. We confirmed that system-wide mitigation is outside the scope of the VDP contractor's responsibilities; consequently, the responsibility to expand remediation efforts falls to the Department and its bureaus. CISA states that "[a]gencies must assume that any vulnerability discovered by a good-faith researcher may have easily been discovered already by a bad actor."[16] Incomplete vulnerability remediation leaves systems exposed to known threats, so it is imperative that the Department's mitigation efforts fully resolve reported vulnerabilities.

Recommendation

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

2. Update and implement VDP reporting and resolution standard operating procedures to ensure that vulnerability remediation is comprehensive across impacted systems.

[16]CISA, *Develop and Publish a Vulnerability Disclosure Policy,* Frequently Asked Questions, "Does the directive require a deadline to fix reported vulnerabilities?", 22.

The Department Did Not Always Remediate Vulnerabilities Within Established Deadlines

Bureaus are responsible for remediating vulnerabilities within established timelines that are based on the severity of the vulnerability; higher-impact issues have shorter deadlines (see figure 4).[17]

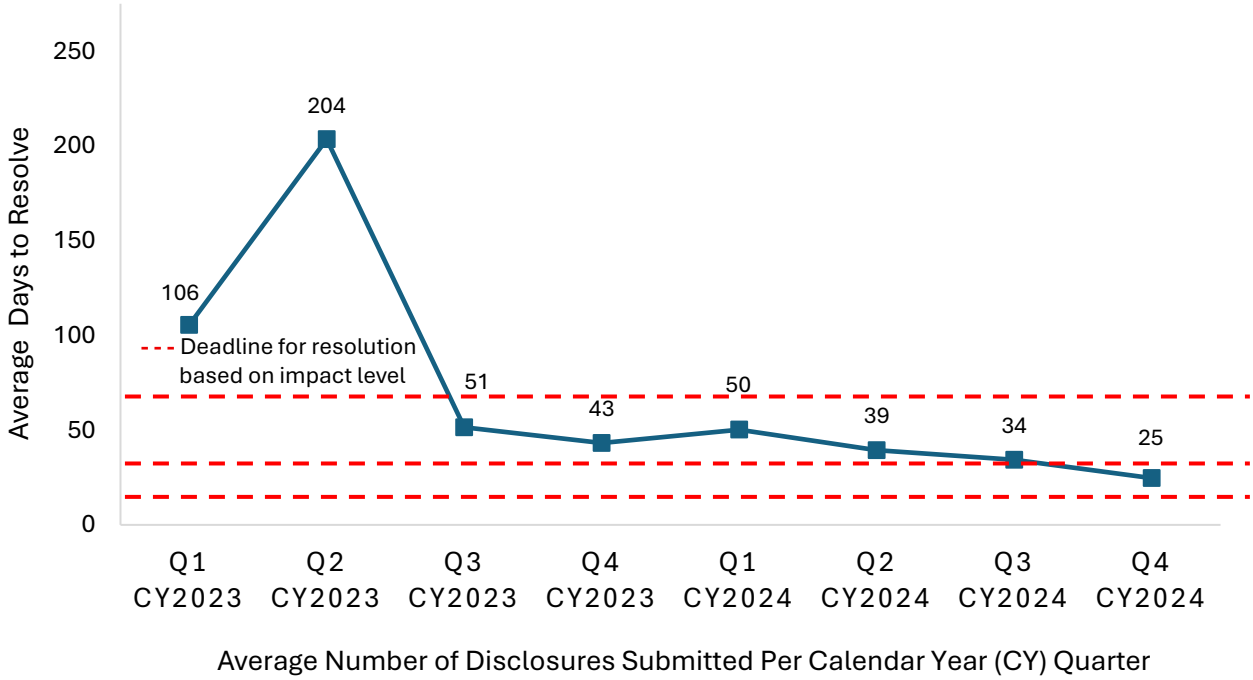
Figure 4. The Department's VDP Requirements for Remediation of Vulnerabilities

15 calendar days	30 calendar days	60 calendar days
For critical-impact vulnerabilities	For high-impact vulnerabilities	For medium-impact vulnerabilities

We found that since 2023, the Department did not remediate vulnerabilities within established deadlines about 35 percent of the time. Additionally, we observed that remediation times are improving (see figure 5), but bureaus were still not consistently meeting deadlines.

[17] There are four vulnerability impact levels: critical-, high-, medium-, and low-impact. Critical-impact vulnerabilities are those that pose the highest risk, such as complete system compromise. High-impact vulnerabilities pose a significant risk, such as unauthorized access to an application or data. Medium-impact vulnerabilities pose less of a risk and may not compromise a system, such as misconfigurations. Low-impact vulnerabilities are the least severe and rarely compromise the system, such as information disclosure. As there were no low-impact vulnerabilities available during our testing, we excluded them from our criteria and testing.

Figure 5. The Department's Remediation Times for Reported Vulnerabilities Have Improved

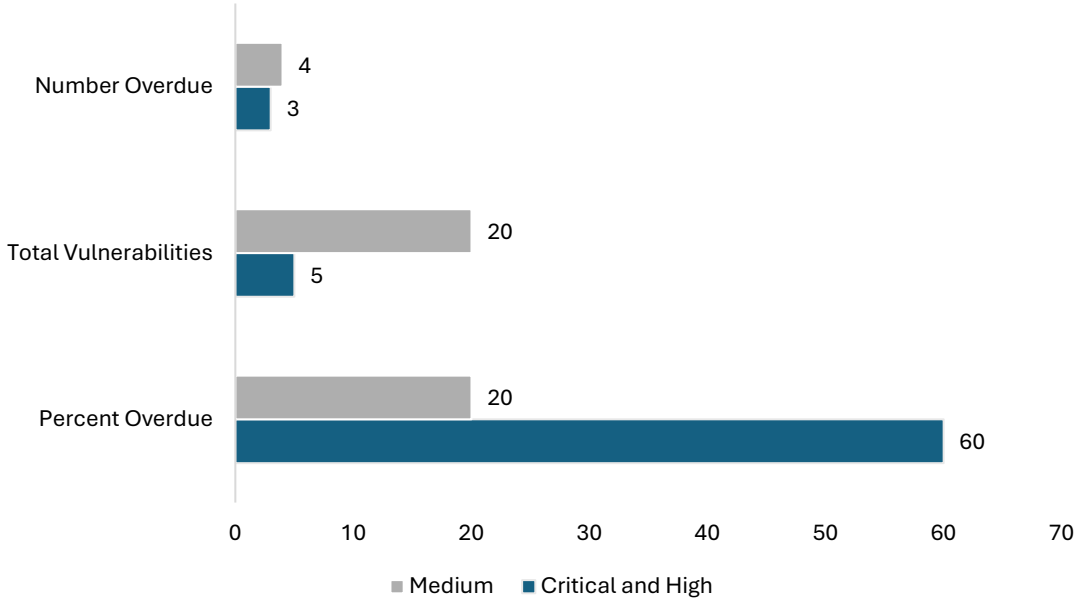


Source: OIG analysis of Department data

In 2024, the Department missed risk-based deadlines for 7 of 25 (28 percent) vulnerability disclosures. Some of these delays were substantial—one critical-impact vulnerability remained unaddressed for 62 days, while a medium-impact vulnerability went unresolved for 116 days.

Beyond these examples, we also found that the Department did not consistently prioritize the remediation of vulnerabilities that posed the greatest risk. The Department did not meet deadlines more often for critical- and high-impact vulnerabilities. Specifically, the Department's remediation of critical- and high-impact vulnerabilities was overdue 60 percent (3 of 5) of the time. This contrasts with medium-impact vulnerabilities, the remediation of which was only overdue 20 percent (4 of 20) of the time (see figure 6 for details).

Figure 6. The Department Did Not Prioritize the Remediation of Critical- and High-Impact Vulnerabilities



Source: OIG analysis of 25 vulnerability disclosures submitted in 2024

The delays in vulnerability remediation were driven by several interconnected issues within the vulnerability disclosure program's process. Primarily, challenges in coordination and communication across the multiple involved parties—public researchers, the VDP contractor, and the bureaus—often led to significant delays.

In addition, the VDP contractor indicated that initial program inefficiencies, such as a manual notification process and restricted bureau access to vulnerability disclosures, contributed to earlier delays. Impacted bureaus attributed more recent delays to the use of disparate internal tracking processes, the inherent complexity of remediating certain vulnerabilities, and prevailing resource or time constraints. Collectively, these coordination problems, process gaps, and resource limitations directly hindered the Department's ability to address vulnerabilities in a timely manner, leaving its public systems at risk.

Recommendation

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

3. Work with bureaus to establish and implement an automated solution to coordinate communication between the contractor and bureaus and to prompt action on delayed vulnerability remediation based on impact level.

Conclusion

The Department established a vulnerability disclosure program in 2021 to comply with a federal directive.[18] Since the Department established its current disclosure process in 2023, the program has accepted 77 vulnerability disclosures from public security researchers. However, the program's effectiveness in reducing risk is hampered by the VDP's restrictions in scope and the tools the public security researchers are allowed to use, as well as stakeholder coordination challenges. In addition, our review identified failures in the remediation of known vulnerabilities within established, risk-based timelines. This problem is compounded by inadequate prioritization of the most critical threats and by the Department's issues in fully remediating vulnerabilities so that they are no longer reproducible. Implementing the recommendations in this report will improve the vulnerability disclosure program and strengthen the Department's cybersecurity posture.

[18] CISA's *Develop and Publish a Vulnerability Disclosure Policy.*

Summary of Agency Response and OIG Comments

On September 10, 2025, we received the Department's response to our draft report. In its response to our draft report, the Department generally concurred with all our findings and recommendations and described actions it has taken, or will take, to address them. The Department's complete response is included in this report as appendix 2.

The Department also provided technical comments on the draft report. We considered those comments and revised the report where appropriate.

We are pleased that the Department concurs with our recommendations and look forward to reviewing its corrective action plan.

Appendix 1. Scope and Methodology

Our objective was to assess the effectiveness of the Department's program for managing public-reported vulnerabilities in its public-facing information technology systems. To assess the vulnerability disclosure program, we:

- Analyzed VDP-related artifacts such as vulnerability disclosures, vulnerability remediation data, VDP dashboard statistics, and other necessary documentation for all applicable vulnerability disclosures
- Reviewed the following documents:
    - Chief Financial Officers Act of 1990
    - CISA's *Develop and Publish a Vulnerability Disclosure Policy*, September 2, 2020
    - The Department's
        - *Enterprise Cybersecurity Policy (ECP)*, Version 1.1, September 2022
        - *Vulnerability Management Standard Office of Cybersecurity and IT Risk Management (OCRM)*, Version 1.1, February 2025
        - *Vulnerability Disclosure Policy*, Version 6.14, January 2023
    - Bureau VDP policies
    - The National Institute of Standards and Technology's *Information Security*, September 2011
- Interviewed:
    - The Department's Office of the Chief Information Officer staff responsible for developing and maintaining VDP policies, procedures, and operational guidelines, and monitoring the Department's overall vulnerability disclosure program
    - VDP contracting staff responsible for hosting and monitoring the Department's overall vulnerability disclosure program

We assessed internal controls significant to the audit objective. This included an assessment of four internal components—Control Environment, Risk Assessment, Control Activities, and Monitoring—defined in the U.S. Government Accountability Office's

Standards for Internal Control in the Federal Government.[19] We also assessed the underlying principles of internal controls. The team identified internal control weaknesses during this audit and proposed recommendations to address them.

We employed a comprehensive methodology to review internal and external information technology (IT) security requirements within the context of our audit objective to determine the effectiveness of the Department's vulnerability disclosure program.

To determine whether all internet-accessible information systems have been included in the program, we:

- Collected internet-accessible IT system inventory from the bureaus and public sources and compared it against the Department's VDP domains
- Scanned IP address ranges provided by the Department's bureaus and identified which IT system could be reached from the internet; after filtering to remove any IP address that had a secure website certificate, we identified over 500 internet-accessible IPs not covered by the VDP

To determine whether the Department accepted, analyzed, and tracked vulnerabilities for its public-facing information systems, we reviewed a random sample of 50 accepted and rejected vulnerability disclosures and assessed whether the VDP contractor handled submission appropriately.

We reviewed all (71) closed vulnerability disclosures available at the time of our testing and attempted to reproduce identified vulnerabilities on either the same location as originally reported or a different endpoint on the same website.

To determine whether the Department effectively remediated reported vulnerabilities in a timely manner, we assessed the 72 closed vulnerability disclosures[20] available at the time of our testing and determined whether they were closed within Department-defined timelines.

We relied on computer-processed data to support our findings, conclusions, and recommendations. We assessed the reliability of data up to January 28, 2025. We found the data to be sufficiently reliable to support our findings and conclusions.

[19] U.S. Government Accountability Office. September 2014. *Standards for Internal Control in the Federal Government*, GAO-14-704G, 7–8.

[20] We conducted our testing over a period of several months; therefore, the number of available reports differed depending on the analysis phase.

We conducted our audit from October 2024 through August 2025 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401–424), and Department Organization Order 10-13, as amended October 21, 2020.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those 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 2. Department's Response

The Department's response to our draft report begins on the next page.

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

MEMORANDUM FOR: Duane Townsend
Acting Inspector General

FROM: Brian Epley BRIAN EPLEY Digitally signed by BRIAN EPLEY Date: 2025.09.10 09:16:58 -04'00'

SUBJECT: The Department of Commerce Concurrence on the Office of Inspector General Draft Report, *Audit of the Department's Vulnerability Reporting and Resolution Program (August 6, 2025)*

We appreciate that the Office of the Inspector General (OIG) presented the Department of Commerce (DOC) with an opportunity to review the Draft Report, *Audit of the Department's Vulnerability Reporting and Resolution Program (August 6, 2025).*

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 manage and remediate public-reported vulnerabilities in its public-facing information technology systems.

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

Attachment

cc: MaryAnn Mausser
Joselyn Bingham
Aditi Palli
Ryan Higgins
Nathan Thweatt
Maria Hishikawa
Shavon Moore

Department of Commerce Technical and Editorial Comments on the OIG Draft Report:
Audit of the Department's Vulnerability Reporting and Resolution Program
(OIG-25-500, August 6, 2025)

The Department of Commerce (DOC) has reviewed the draft report, and we offer the following comments for the Office of the Inspector General's consideration. Page numbers refer to page numbers in the draft report unless otherwise stated.

General Comments

Recommended Changes for Factual/Technical Information

Page 4, Paragraph 1, "Specifically, the Department's Vulnerability Disclosure Policy (VDP) did not include all internet-accessible assets, and testing guidelines restricted public researchers from using common testing tools."

DOC is requesting this statement be modified to acknowledge this was a temporary condition that was remediated upon notification.

Page 4, Paragraph 2, "Rather than adhering to the Cybersecurity & Infrastructure Security Agency's (CISA) requirements and broadly defining its VDP scope as all internet-accessible systems, the Department limited its VDP scope to a list of 64 internet-accessible websites (e.g., www.doc.gov)."

CISA provided agencies the VDP template to assist with complying with Binding Operational Directive (BOD) 20-01. DOC used this template which remains as a resource on CISA's BOD 20-01 page as of August 2025. The scope format is also widely used by other Chief Financial Officers Act agencies.[1] Furthermore, the CISA VDP template and BOD 20-01 frequently asked questions also recommends agencies include the following language with the scope of their VDP following the list of agency domains: "*Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at security@agency.gov before starting your research."*

[1] See Department of Transportation VDP, Health and Human Services VDP, United States Department of Agriculture VDP and Department of Labor VDP.

DOC is requesting the removal of statements that imply lack of compliance with CISA directive and context added to acknowledge the formatting of the scope was provided by CISA and is widely utilized by Federal agencies.

Page 5, Paragraph 1, "Because the Department's VDP does not include third-party services, a public security researcher might not report this vulnerability or could face legal ramifications by doing so."

This statement implies the scope of the DOC VDP should include vendor and third-party owned services and sites. However, language in the BOD 20-01 VDP template and frequently asked questions contradicts this: *"Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at security@agency.gov before starting your research."*

DOC is requesting context be added to acknowledge DOC follows the approach recommended by CISA.

Page 8, Paragraph 3: "Bureaus are responsible for remediating vulnerabilities within established timelines that are based on the severity of the vulnerability; more critical issues have shorter deadlines (see figure 4)."

Vulnerabilities are assigned impact levels, critical, high, medium, or low as noted in footnote 15. As such, vulnerabilities are not 'more or less critical,' rather they are critical or other than critical. Recommend removing the phase 'more critical issues have shorter deadlines' or rephrasing as 'deadlines are shorter for higher severity impact level vulnerabilities.'

Page 11, Recommendation 3.a: "Determine why vulnerabilities were not remediated within established deadlines and why more critical vulnerabilities were not prioritized."

As noted in the comment for **page 8, paragraph 3 above,** vulnerabilities are assigned impact levels which determine deadlines, not categorized as more or less critical. Additionally, the recommendation asks two 'why' questions then directs action in Recommendation 3.b to improve coordination and communication based on the findings from the audit. Since the standard operating procedures for VDP resolution is suggested in Recommendation 2 and Recommendation 3.b directs improvements in communications, Recommendation 3.a is superfluous and should be removed.

REPORT

FRAUD & WASTE & ABUSE

HOTLINE

Department of Commerce

Office of Inspector General Hotline

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