OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

Inspection

The U.S. Department of the Interior Information Systems at Increased Risk Due to Unmitigated Known Vulnerabilities

Report No. 2023-ITA-007

September 2025

This is a revised version of the report prepared for public release.

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

SEP 17 2025

Memorandum

To: Paul A. McInerny
Chief Information Officer

From: Nicki Miller
Assistant Inspector General for Audits, Inspections, and Evaluations

Subject: Final Inspection Report – *The U.S. Department of the Interior Information Systems at Increased Risk Due to Unmitigated Known Vulnerabilities*
Report No. 2023-ITA-007

This memorandum transmits our final inspection report on the Department of the Interior's (DOI) software vulnerability identification and remediation practices. Specifically, we determined that, notwithstanding DOI and other Federal policies, DOI is not consistently reducing cybersecurity risks by remediating software vulnerabilities that have been rated as the most severe.

We will track open recommendations for resolution and implementation. We will notify Congress about our findings, and we will report semiannually, as required by law, on actions you have taken to implement the recommendations and on recommendations that have not been implemented. We will also post a public version of this report on our website.

If you have any questions about this report, please contact me at aie_reports@doioig.gov.

Contents

Cover photo source: teusrenes/stock.adobe.com

Results in Brief

Objective

To determine whether the U.S. Department of the Interior (DOI) is reducing cybersecurity risks by remediating software vulnerabilities in accordance with Federal and DOI policies.

Finding

We determined that, notwithstanding DOI and other Federal policies, DOI is not consistently reducing cybersecurity risks by remediating software vulnerabilities[1] that have been rated as the most severe. [2] Specifically, we found 9,384 vulnerabilities on DOI systems identified by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) as "known exploited vulnerabilities" (KEVs) that had not been remediated within the mandated timeframe. KEVs are the highest priority for remediation, as they have been identified by CISA as being actively exploited by malicious cyber actors. We also found a total of 153,665 critical and high impact vulnerabilities on DOI systems that were not remediated within required timeframes. We immediately notified DOI and the affected bureaus and offices of these findings so they could validate and remediate these issues. DOI's high number of unresolved critical and high impact vulnerabilities also significantly increased DOI's risk of compromise.

These deficiencies occurred because the DOI Office of the Chief Information Officer did not provide sufficient vulnerability remediation guidance and oversight to bureaus and offices. We found this lack of guidance caused the vulnerability management standard operating procedures to vary between bureaus and offices, resulting in inconsistent remediation of vulnerabilities across DOI. This issue was exacerbated because, while the historical data required for calculating the age of a vulnerability existed within DOI, it was not readily available on the dashboard, and not all bureaus knew how to access that data outside the dashboard. Without this data, DOI could not determine how long a vulnerability went unremediated on its network.

Impact

Vulnerabilities in Federal computer systems are frequent attack vectors[3] for malicious cyber actors and pose significant risk to critical Federal systems and data. If exploited, these vulnerabilities could have serious or severe adverse effects on DOI operations, including, but not limited to, system takeover by malicious third parties, ransomware, or exposure of sensitive data. DOI relies on complex, interconnected information systems to carry out its daily operations and maintain an accurate view of the security posture of every bureau and office. Without sufficient oversight of information systems, DOI will remain unaware of potential threats posed by vulnerabilities that could permeate the networks connecting bureaus and offices. To reduce risk, DOI must remediate vulnerabilities in a timely manner to reduce the window of opportunity for attackers. If DOI is not aware of, or does not accurately report its security posture, DOI's risk-based decision making could be impeded and result in increased risk of compromise to its information systems, loss of sensitive data, and disruption of mission operations.

[1] The National Institute of Standards and Technology (NIST) defines vulnerability as "[w]eakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." https://csrc.nist.gov/glossary/term/vulnerability.

[2] Vulnerabilities are ranked according to their potential harm to systems, with risk ratings of critical, high, medium, or low. These vulnerability ratings allow organizations to prioritize remediation by addressing the highest rated vulnerabilities first. CISA further designates vulnerabilities it identifies as currently being exploited as KEVs and requires the vulnerabilities to be the most aggressively remediated, regardless of their initial vulnerability rating.

[3] According to NIST Special Publication 800-53 RA-5(10), an attack vector is a path or means by which an adversary can gain access to a system to deliver malicious code or exfiltrate information.

Recommendations

We make nine recommendations to help DOI strengthen its IT governance practices pertaining to vulnerability management and reduce the risk that unmitigated vulnerabilities pose to DOI IT assets.

Introduction

Objective

The objective of our inspection was to determine whether the U.S. Department of the Interior (DOI) is reducing cybersecurity risks by remediating software vulnerabilities in accordance with Federal and DOI policies.

See Appendix 1 for the scope and methodology of our review and Appendix 2 for a list of the abbreviations and terms used throughout the report.

Background

In fiscal year (FY) 2023, DOI spent approximately $1.7 billion on its IT asset portfolio[4] of systems across a range of programs at its 11 bureaus and multiple offices. These programs include those that support DOI's mission to "protect and manage the Nation's natural resources and cultural heritage; provide scientific and other information about those resources; and honor its trust responsibilities or special commitments to American Indians, Alaska Natives, Native Hawaiians, and affiliated Island Communities."[5]

Protecting Federal IT networks, like the ones used by DOI, remains one of the government's highest risk areas that could lead to fraud, waste, abuse, and mismanagement.[6] Vulnerabilities in Federal computer systems are frequent attack vectors for malicious cyber actors and pose significant risk to critical Federal systems and data. According to the U.S. Department of Homeland Security's (DHS's) Cybersecurity and Infrastructure Security Agency (CISA), "Recent reports from government and industry partners indicate that the average time between discovery and exploitation of a vulnerability is decreasing as today's adversaries are more skilled, persistent, and able to exploit known vulnerabilities."[7]

Ongoing monitoring for vulnerabilities and timely remediation are essential for maintaining the security of DOI IT assets. Vulnerabilities are commonly remediated by applying software patches,[8] updating system configurations, or applying compensating controls that mitigate their impact. For example, computer operating systems that do not have the latest software patches are susceptible to compromise. Attackers actively search for unpatched vulnerabilities to gain unauthorized access to DOI's computer network. An attacker who gains access could use the compromised computer to exploit other weaknesses, which could result in the loss or impairment of DOI IT resources, including its high-value assets.[9] While there are no solutions that protect against all potential attacks, Federal agencies may reduce risk by implementing processes to identify and promptly remediate vulnerabilities on their computer systems and networks.

Mainstays of an effective vulnerability management program include accurate hardware and software inventories, detailed vulnerability identification and reporting, and timely remediation. In addition, information on long-term trends that can be used to monitor and improve processes is key to ensuring the efficacy of the program.

---

[4] IT spending information was obtained from https://www.itdashboard.gov.

[5] DOI website, "*About Interior*," https://www.doi.gov/about.

[6] United States Government Accountability Office, GAO-25-107743, *Report to Congressional Committees, High-Risk Series Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness,* February 2025, https://www.gao.gov/assets/gao-25-107743.pdf.

[7] CISA, Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems,* April 29, 2019, https://www.cisa.gov/news-events/directives/bod-19-02-vulnerability-remediation-requirements-internet-accessible-systems.

[8] Software patches are a set of changes to a computer program or operating system designed to install updates, bug fixes, or vulnerability fixes.

[9] According to CISA, a high-value asset "is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business." https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf.

Vulnerability scanners automate the discovery and reporting of vulnerability information. With the proper configuration, scanners are capable of multiple detection methods, such as analyzing and identifying software versions for missing patches, testing a system's services for misconfigurations, and looking for signatures that would indicate a known vulnerability.[10] The scanners rank vulnerabilities according to their potential to harm a system using the Common Vulnerability Scoring System,[11] which allows an organization to prioritize remediation by rating vulnerability impact as critical, high, medium, or low.

CISA's Vulnerability Remediation Requirements for Federal Agencies

Federal agencies are required to comply with DHS-developed information system directives.[12] Accordingly, CISA BOD 22-01 requires agencies to remediate known exploited vulnerabilities (KEVs) on an accelerated timeline because of their severity and high risk of exploitation.[13] A KEV is a vulnerability that has (1) an assigned Common Vulnerabilities and Exposures (CVE) identifier, (2) reliable evidence that the vulnerability is actively being exploited by a threat actor to compromise computer systems "in the wild,"[14] and (3) a clear remediation action for the vulnerability, such as a vendor-provided update. Unmitigated KEVs pose an increased risk to Federal computer systems.

CISA publishes a catalog of KEVs,[15] which provides the required timelines for remediation, typically within two weeks from its inclusion in the catalog. CISA may adjust default timelines in the case of grave risk to the Federal Government. In addition, CISA requires agencies to establish a process for ongoing remediation of KEVs.[16] If agencies cannot update IT assets with KEVs as recommended, CISA requires that the agency remove the affected IT asset from the network. Depending on the environment, CISA suggests isolation techniques such as decommissioning; removing the vulnerable software product; or implementing network segmentation, software-defined perimeters, and proxies. For example, in January 2024, CISA Emergency Directive 24-01 identified a critical vulnerability in remote access software that posed such a grave risk to the Federal Government that it required all agencies to fully disconnect all vulnerable systems within three days of the notice.

> The *Verizon 2024 Data Breach Investigations Report* identifies a "180% increase in the exploitation of vulnerabilities as the critical path action to initiate a breach."

An analysis of the time between public disclosure of a vulnerability to the first witnessed malicious scans by cyber actors looking for vulnerable systems is documented in the *Verizon 2024 Data Breach Investigations Report.*[17] This report is an annual investigation and analysis of breaches occurring globally. Private- and public-sector organizations, such as CISA, the Defense Counterintelligence and Security Agency, and the Federal Bureau of Investigation – Internet Crime Complaint Center, contributed to this report. The Verizon report noted the time between public disclosure and the first malicious scans "for a Common Vulnerabilities and Exposures (CVE) registered vulnerability in the CISA KEV is five days. On the other hand, the median time for non-CISA KEV vulnerabilities sits at 68 days." Vulnerabilities in the KEV catalog

[10] NIST's searchable Common Vulnerabilities and Exposures (CVE) database is available at https://nvd.nist.gov/vuln/search.

[11] Additional scoring system information is available at https://nvd.nist.gov/vuln-metrics/cvss.

[12] A Binding Operational Directive (BOD) is a compulsory direction to Federal, executive branch, departments, and agencies for the purpose of safeguarding Federal information and information systems. Section 3553(b)(2) of title 44, U.S. Code, authorizes the DHS Secretary to develop and oversee the implementation BODs and specifies that these directives do not apply to statutorily defined "national security systems" nor to certain systems operated by the Department of Defense or the Intelligence Community.

[13] CISA BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities,* November 3, 2021, requires vulnerabilities with a CVE ID assigned prior to 2021 to be remediated within six months and all other vulnerabilities to be remediated within two weeks. https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities.

[14] Exploited "in the wild" refers to when threat actors are currently using a vulnerability in a malicious attack or other real-world scenario that could compromise system security.

[15] CISA's KEV catalog is available at https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

[16] CISA BOD 22-01.

[17] *Verizon 2024 Data Breach Investigations Report*, https://www.verizon.com/dbir.

are attacked more than 13 times faster than those that are not. This metric shows that the severity of a KEV requires a higher priority for remediation. While the Verizon report states that "when exploitation starts running rampant, vulnerabilities are added to the KEV" catalog, it also acknowledged, "There are few hindsight metrics as powerful as this one to guide what you should be patching first."[18] The report advises that "if it goes into the KEV, go fix it ASAP."[19] Malicious actors are already actively exploiting vulnerabilities added to the KEV catalog; therefore, Federal agencies should consider remediation of KEVs as their top priority.

In addition, CISA BOD 19-02, which applies only to internet-accessible devices, requires the following minimum vulnerability remediation timelines:

- Critical impact vulnerabilities must be remediated within 15 calendar days of initial detection.
- High impact vulnerabilities must be remediated within 30 calendar days of initial detection.

DOI's Vulnerability Identification and Remediation Practices

DOI's Office of the Chief Information Officer (OCIO) is responsible for developing and overseeing a Departmentwide, risk-based, cost-effective IT security program.[20] DHS established the Continuous Diagnostics and Mitigation (CDM) Program to assist Federal agencies in better understanding, prioritizing, and mitigating cyber risk. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating Federal agencies with the goal of helping them improve their security posture.[21] The OCIO has centralized CDM implementation across DOI for service procurement, deployment, management, and communication. As part of DOI's centralized CDM initiative, enterprise CDM tools (for example, [redacted], [redacted], and [redacted]) regularly scan all bureau and office systems for vulnerabilities and build DOI-wide inventories of hardware and software assets. The data derived from the CDM tools are aggregated in DOI's enterprise data collection tool ([redacted]).

Each bureau and office is responsible for its respective IT systems; however, the CDM tool's reporting structure does not directly align with DOI's overall organizational structure.[22] Instead, the vulnerability management tool ([redacted]) categorizes bureau and office vulnerability management responsibilities as follows:

- Bureau of Indian Affairs (BIA)
- Bureau of Indian Education (BIE)
- Bureau of Land Management (BLM)
- Bureau of Reclamation (BOR)

[18] *Id*.

[19] *Id*.

[20] DOI OCIO is responsible for all IT management per Secretarial Order No. 3340, *Strengthening and Securing Information Management and Technology at the Department of the Interior*, August 15, 2016. The order brought DOI in line with the Federal Information Technology Acquisition Reform Act and established that DOI's Chief Information Officer is responsible for overseeing and managing all DOI information management and technology.

[21] On November 18, 2013, the Office of Management and Budget (OMB) issued Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, which identifies cybersecurity as a cross-agency priority and requires the management of information security risks on a continuous basis. In response, DHS established the CDM Program to carry out these OMB requirements. Additional details regarding CDM Program capabilities are available at https://www.cisa.gov/sites/default/files/publications/2020%252009%252003_CDM%2520Program%2520Overview_Fact%2520Sheet.pdf.

[22] See http://www.doi.gov/bureaus for a full list of the DOI's bureaus and a link to a full list of all departmental offices. For this report, we use the bureau and office labels as they are defined in DOI's primary CDM vulnerability management tool. Some repositories contain multiple offices; in these cases, we use the combined label instead of attempting to separate the data to reflect DOI's organizational structure.

- Bureau of Safety and Environmental Enforcement (BSEE)[23]
- Bureau of Trust Funds Administration (BTFA)
- Departmental Offices, referred to as the Office of the Secretary (OS)
- National Park Service (NPS)
- Office of Inspector General (OIG)
- Office of Surface Mining Reclamation and Enforcement (OSMRE)
- U.S. Fish and Wildlife Service (FWS)
- U.S. Geological Survey (USGS)

While the OCIO is responsible for oversight of the vulnerability management program, it stated that bureaus and offices are responsible for prioritizing and remediating their identified system vulnerabilities in accordance with their own vulnerability remediation procedures. Bureaus and offices must also comply with DOI's vulnerability management policies that align with CISA BOD 19-02 for internet-accessible systems and CISA BOD 22-01 for KEVs.[24] Specifically, bureaus and offices are required to remediate vulnerabilities according to the following timelines:

- By the due date set forth in CISA's catalog for KEVs.
- Within 15 days of detection for critical vulnerabilities on internet-accessible[25] systems.
- Within 30 days of detection for critical vulnerabilities on non-internet-accessible systems.
- Within 30 days of detection for high vulnerabilities on all systems (internet-accessible and non-internet-accessible).

According to the OCIO, it is responsible for ensuring bureaus and offices remediate all vulnerabilities in accordance with these timelines and accurately report remediation in accordance with CISA BODs.

DOI OIG has conducted four prior reviews of DOI's cybersecurity program that identified findings and provided recommendations relevant to effective vulnerability management. See Appendix 3 for a summary of these reviews.

[23] In the CDM vulnerability management tool, BSEE's repositories include the Bureau of Ocean Energy Management (BOEM) and the Office of Natural Resources Revenue (ONRR).

[24] DOI OCIO, *Security and Privacy Control Standard: Risk Assessment* (Version 1.0), "RA-5 Vulnerability Monitoring and Scanning," December 2022.

[25] Under BOD 19-02, CISA defines internet-accessible as "any system that is reachable over the public internet that has a publicly routed IP [Internet Protocol] address or a hostname that resolves publicly in DNS [Domain Name System] to such an address."

Results of Inspection

We determined that DOI is not consistently reducing cybersecurity risks by remediating software vulnerabilities in accordance with Federal and DOI policies. We found vulnerabilities on DOI systems identified by DHS' CISA as KEVs that had not been remediated within the mandated timeframes. Specifically, we reviewed DOI's vulnerability data as of July 2023 and identified 9,384 KEVs that were 30 days or more past CISA's remediation deadlines and 4,634 KEVs that were one year or more past due. In addition, we identified a total of 153,665 critical and high impact vulnerabilities on DOI systems that were not remediated within required timeframes. While KEVs are of highest importance because these vulnerabilities have been identified by CISA as being actively exploited, critical and high impact vulnerabilities must also be remediated. Large numbers of unmitigated vulnerabilities increase a malicious actor's opportunities to target and exploit DOI's information systems.

9,384 KEVs
30 days or more past due

4,634 KEVs
one year or more past due

Vulnerabilities went unremediated in part because, while the OCIO scanned its systems for vulnerabilities, it could not distinguish between internet-accessible and internal systems, hindering its ability to comply with remediation timelines. Additionally, DOI's OCIO did not provide sufficient vulnerability remediation guidance to bureaus and offices, nor did it provide oversight to ensure timely remediation. We found this lack of guidance caused the vulnerability management standard operating procedures to vary by bureau and office, resulting in inconsistent remediation of vulnerabilities across the DOI. While the historical data required for calculating the age of a vulnerability existed within the DOI, it was not readily available on the dashboard, and not all bureaus knew how to access that data outside the dashboard. Understanding the age of a vulnerability is necessary to identify the timeframe in which vulnerabilities must be remediated. Without this information, the bureaus and offices responsible for vulnerability remediation did not take the age of the vulnerabilities into account when prioritizing them for remediation.

DOI's interconnected information system architecture relies on a level of trust that is dependent on an accurate view of the security posture of every bureau and office. Without sufficient oversight by the OCIO, DOI will remain unaware of potential threats posed by vulnerabilities that could permeate the networks between bureaus and offices.

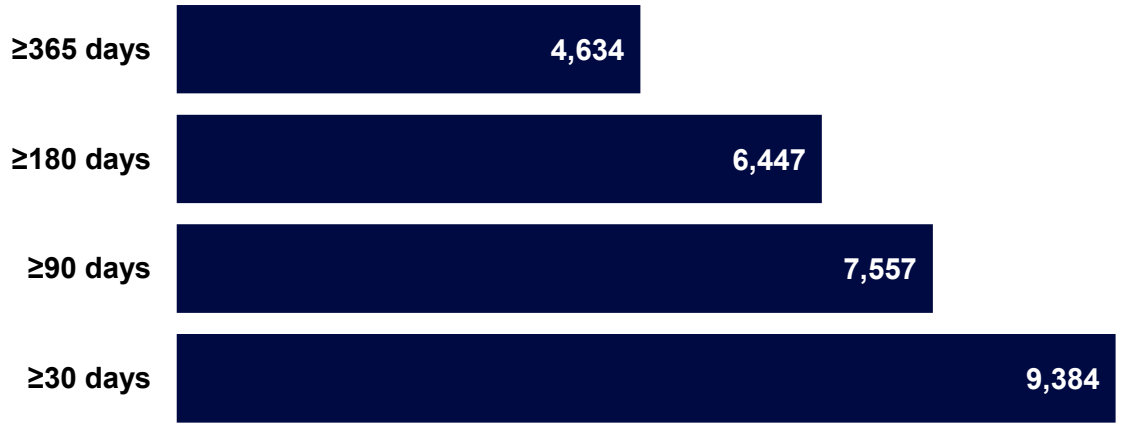
DOI Failed To Remediate Significant Vulnerabilities in a Timely Manner, Increasing Risk of Compromise

CISA BOD-22-01 requires agencies to establish a process for ongoing remediation of KEVs and assigns due dates for each KEV, typically within two weeks from its inclusion in the catalog. We analyzed vulnerabilities reported by DOI's mandated vulnerability management tool ([redacted]) for the timeframe of July 2022 to July 2023 and found that DOI did not remediate software vulnerabilities in a timely manner.[26] As of July 2023, we identified 9,384 KEVs across the DOI network that were at least 30 days past CISA's prescribed due date for remediation. Nearly half of those vulnerabilities were one year or more overdue. We communicated these findings to the DOI Chief Information Security Officer in May 2024 to ensure the OCIO resolved the outstanding KEVs. In response to our notifications, OCIO implemented a dashboard in the enterprise data collection tool to validate our findings and help bureaus and offices easily identify and remediate the overdue vulnerabilities we identified.

[26] See Appendix 1, Scope and Methodology, for further details on our data analysis.

Figure 1 shows the total number of overdue KEVs that existed on the DOI network for at least two weeks. These KEVs are organized by the amount of time that had passed since CISA's prescribed due date.

Figure 1: KEVs Overdue as of July 2023

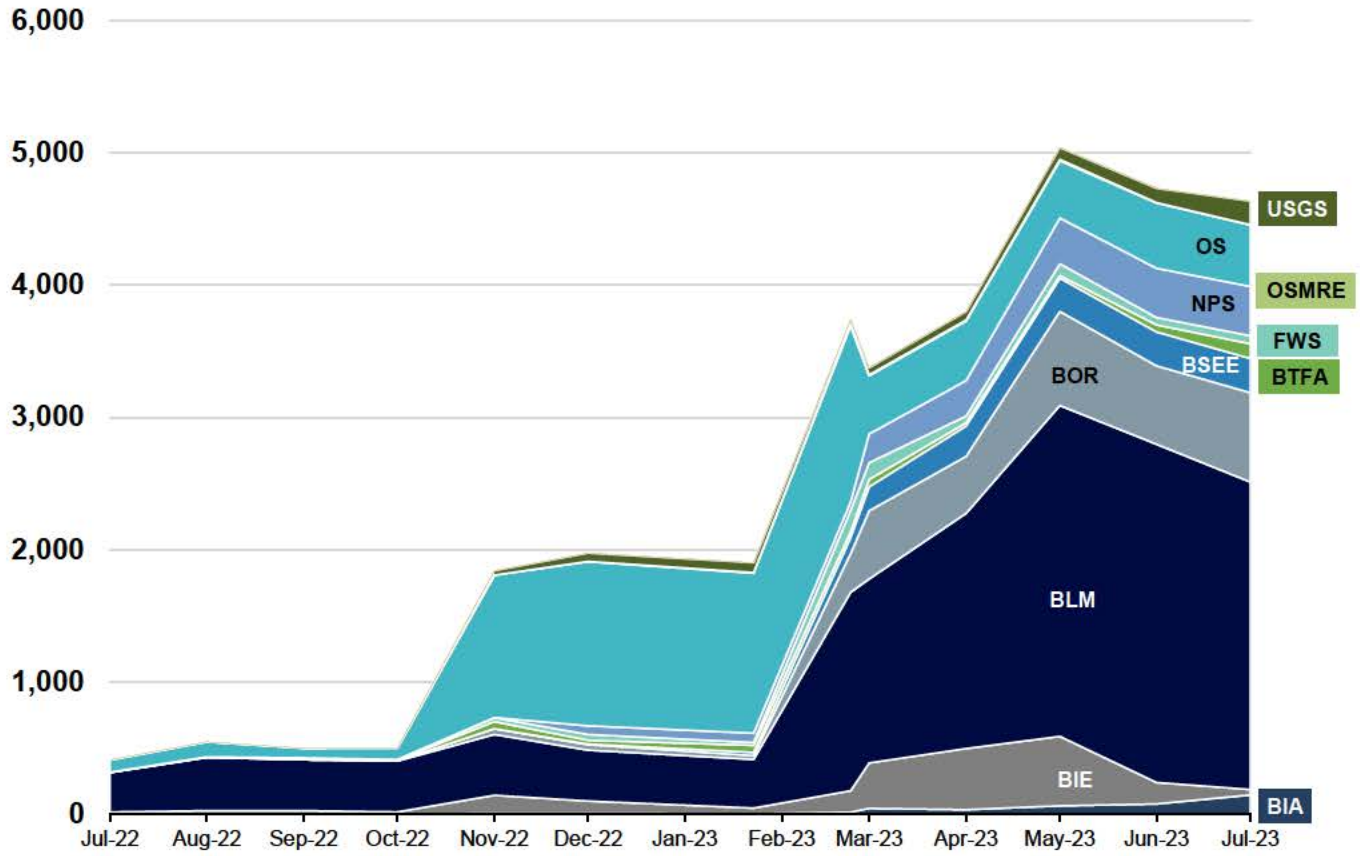


Source: DOI OIG.

Note: The total number of KEVs are inclusive of the next lower age. For example, all vulnerabilities overdue as of 365 days are also overdue for 180, 90, and 30 days and are represented as such in the above chart. Figure due dates do not represent how long a vulnerability existed on the network because DOI policy dictates that the KEV must be remediated within 15 days of discovery. For example, a new computer that connects to the network for the first time may have a KEV that is a year or more past its due date until it is fully patched. Accordingly, we accounted for the two-week patching grace period and did not include overdue KEVs that had existed for 15 days or less on the network.

Figure 2 shows the total number of KEVs that were more than 365 days past their due date, totaled monthly, and split by bureau and office. The data shows a significant compounding of KEVs that are well past required remediation dates across most bureaus and offices as the year progressed. Finding historical information required bureaus and offices to look deeper into the vulnerability management ([redacted]) and enterprise collection ([redacted]) tools because it was not made available in the dashboards provided by the OCIO. Over the period of our evaluation, the number of unremediated KEVs that were 365 days or more past due grew more than 11-fold (1,127 percent), from 411 in July 2022 to 4,634 in July 2023, indicating that historical data in the dashboards is necessary for identifying these trends on a regular basis.

Figure 2: Bureau and Office Monthly Distribution of KEVs Overdue 365 Days or More



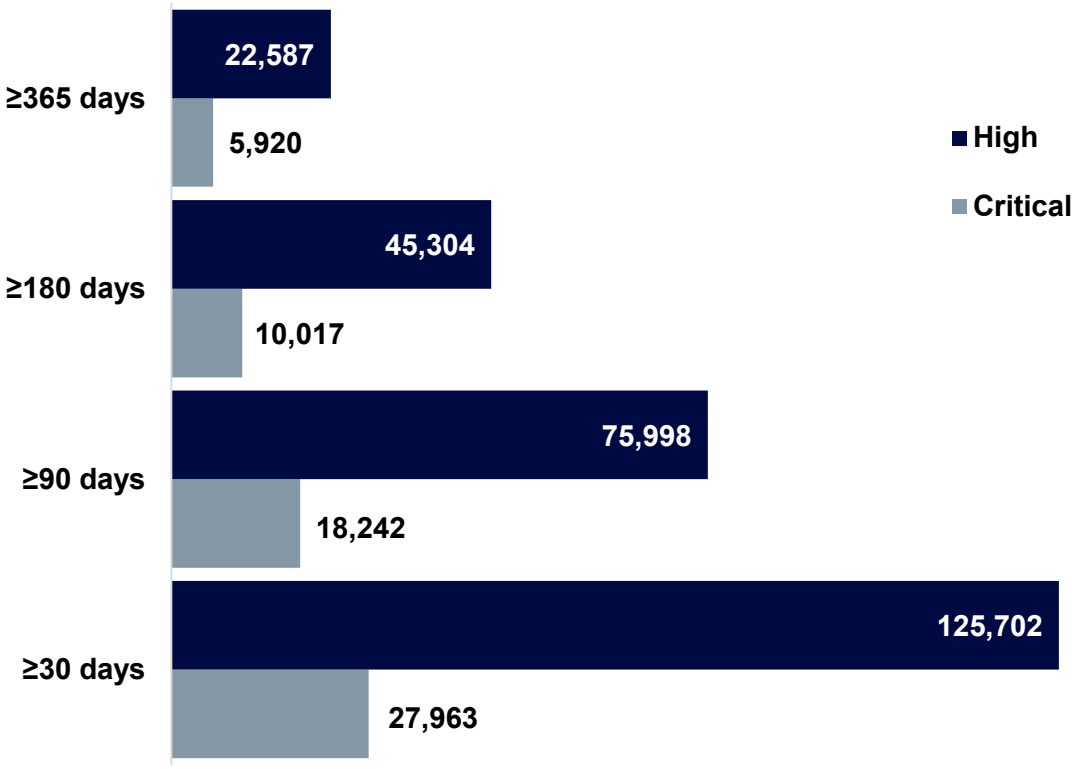
Source: DOI OIG.

Although KEVs pose the most dangerous threat to DOI because malicious actors have been observed exploiting them, all vulnerabilities with a critical and high rating can have serious or severe adverse effects on Department operations and result in the loss of sensitive data. The DOI *Security and Privacy Control Standard: Risk Assessment* requires all critical and high vulnerabilities to be remediated within 30 days of discovery. Vulnerabilities with a critical rating have the highest potential for exploitation or severe impact if exploited, while vulnerabilities with a high rating have a substantial potential impact if exploited. These vulnerabilities must not be ignored simply because they are not known to be exploited at the time of discovery.

During our analysis, we reviewed all critical and high vulnerabilities that existed on the network past DOI's remediation deadline of 30 days post identification. We found 153,665 critical and high vulnerabilities that went unmitigated for 30 days or more, demonstrating that these vulnerabilities are also not being prioritized and remediated in accordance with DOI's policy.

Because of the high number of vulnerabilities that were overdue 30 days or more, we also examined vulnerabilities that were open for additional timeframes (see Figure 3).

Figure 3: Critical and High Vulnerabilities by Age as of July 2023



Source: DOI OIG.

These large numbers of unmitigated vulnerabilities demonstrate that untimely remediation is systemic across vulnerability and patch management processes within DOI and is not solely limited to KEVs. DOI must take action to remediate these vulnerabilities before they are exploited.

Four prior OIG reports found weaknesses in DOI's vulnerability management program leading to increased risk of compromise, with three of these reports specifically identifying critical and high vulnerabilities that were not mitigated. These recommendations were resolved or implemented by the respective bureaus. Appendix 3 summarizes these prior findings and recommendations.

The OCIO Did Not Maintain an Inventory of Internet-Accessible Systems

Both NIST Special Publication (SP) 800-53[27] and DOI's *Security and Privacy Control Standard: Configuration Management*[28] specify that the bureaus and offices must maintain and update regularly a complete and accurate inventory of all information system components that is at the level of granularity deemed necessary for tracking and reporting. Additionally, because of the increased access to publicly facing systems, known as internet-accessible systems, CISA BOD 19-02 requires critical vulnerabilities detected on these to be remediated within 15 days. The OCIO relies on CISA's Cyber Hygiene scanning programs[29] to determine its inventory of internet-accessible systems, but the OCIO did not apply these required stricter remediation

[27] NIST SP 800–53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

[28] DOI OCIO, *Security and Privacy Control Standard: Configuration Management*, Version: 1.0, "CM-8 System Component Inventory," December 2022.

[29] As part of this program, CISA provides vulnerability scanning services to evaluate Federal agencies' external network presence by performing scans for internet-accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad hoc alerts.

timelines. Further, we were unable to validate that an organization-wide inventory of internet-accessible systems existed, hindering our ability to determine if DOI was able to meet the timelines.
Inventory management has been a persistent issue at DOI. In our 2018 inspection of DOI's email and web security mandates,[30] we included a similar finding that DOI relied on outside agencies to discover and report its internet-accessible websites. We found that DOI's reliance on outside agencies to maintain its inventory resulted in its failure to secure a significant portion of its internet-accessible systems. DOI closed the related recommendation[31] in March 2021, stating that the OCIO maintains an inventory of internet-accessible websites through DOI's annual assurance statement process.[32] Although OCIO stated the recommendation was implemented in March 2021, we again confirmed during this inspection that this process did not, in fact, exist. See Appendix 3 for more information about our previous inventory-related finding from the 2018 inspection.

Without its own inventory, the OCIO is unable to validate whether the Cyber Hygiene scans successfully identified all of DOI's internet-accessible systems and scanned the systems for vulnerabilities. Accordingly, the OCIO is unaware of the population of its internet-accessible systems or whether it is successfully patching critical vulnerabilities on the systems within 15 days. Given DOI's size and high number of internet-accessible systems, the OCIO must maintain its own inventory to ensure it is protecting all its internet-accessible systems.

The OCIO Provided Insufficient Oversight and Historical Data

The large number of the most severe vulnerabilities persisted because the OCIO had not established a set of clear roles and responsibilities for its own office or for DOI's bureaus and offices. The OCIO stated that its vulnerability policies and procedures are limited to guidance on maintaining and administering vulnerability management tools and mandating that the bureaus and offices use those tools; however, the OCIO does not describe how system administrators should use the tools to respond to vulnerabilities. This gap in guidance leaves bureaus and offices to interpret and implement significant vulnerability remediation activities on their own, which leads to differing practices among bureaus and offices because a standardized approach is not available.

Additionally, we found that the OCIO focused on presenting only the current security posture at DOI and did not provide the detailed historical or age information of an identified vulnerability in its vulnerability dashboards. The OCIO created dashboards in the enterprise data collection tool ( ) to make it easier for bureaus and offices to identify vulnerabilities; however, while the data required for calculating the age of a vulnerability existed in the enterprise collection tool ( ), it was not readily available on the dashboard, and not all bureaus knew how to access that data outside the dashboard. As a result, bureaus and offices relied on DOI's direction for prioritizing the most dangerous vulnerabilities. Further, they did not consider the age of the vulnerability when prioritizing bureau and office vulnerability management efforts.

The age of KEV data was available to bureaus and offices in via custom queries and reports, but the OCIO did not review or provide the information in the dashboards for incorporation into the decision making processes of those responsible for remediation. Instead, OCIO officials stated in interviews that it performed ad hoc queries and informally notified bureaus and offices of the "top 5" unmitigated KEVs on their networks to help entities focus on remediating vulnerabilities with the highest potential risk and impact. However, the OCIO did not have a formal process for identifying and reporting vulnerabilities that existed on their networks beyond required due dates to bureaus and offices. In response to our inquiries on these outstanding vulnerabilities, the OCIO created a new custom dashboard that showed all vulnerabilities that were one year or greater in age. Although this is a positive step to address these concerns, a more detailed solution that can identify overdue vulnerabilities before they reach one year of age is warranted.

[30] *The Department of the Interior Generally Complied with Email and Web Security Requirements* (Report No. 2018-ITA-019), issued July 2018, https://www.doioig.gov/reports/inspection-evaluation/department-interior-generally-complied-email-and-web-security.

[31] Recommendation 1 of Report No. 2018-ITA-019 was, "We recommend that the OCIO develop a comprehensive inventory management program that includes periodic discovery scanning for all publicly accessible websites and IP ranges, including those with non-.gov domains."

[32] DOI's annual assurance statement process allows bureaus and offices to self-certify and report their respective security postures to the Chief Information Officer in support of annual Federal Information Security Modernization Act requirements.

Furthermore, the OCIO does not have an effective process in place to provide bureaus and offices with feedback and effective oversight of their vulnerability management programs. In turn, this minimizes the OCIO's ability to improve its guidance and recommendations to bureaus and offices based on an informed understanding of the effectiveness of their vulnerability management programs. Although the OCIO provided bureaus and offices with centrally managed vulnerability tools, the OCIO did not effectively use these same tools to identify vulnerabilities that were open well beyond the required timeframes for remediation and communicate the problem to the bureaus and offices or system owners directly.

Bureaus and Offices Had Inconsistent Vulnerability Management Practices

The vulnerability management practices varied at bureaus and offices as a result of the lack of guidance from the OCIO. Some bureaus and offices primarily used only the software management tool for vulnerability management, while others combined both the software management tool and vulnerability management tool data. Some stood up their own vulnerability detection platforms. Ultimately, certain bureaus had larger percentages of KEVs that were overdue when compared to their total number of hardware assets.

For example, when we compared the number of KEVS overdue by 365 days or more to the number of hardware assets belonging to each bureau or office as of July 2023, some bureaus and offices have a disproportionate number of overdue KEVs.[33]

We found BLM, BOR, and OS had a disproportionate number of overdue KEVs when compared to the number of hardware assets. Specifically, we noted the following:

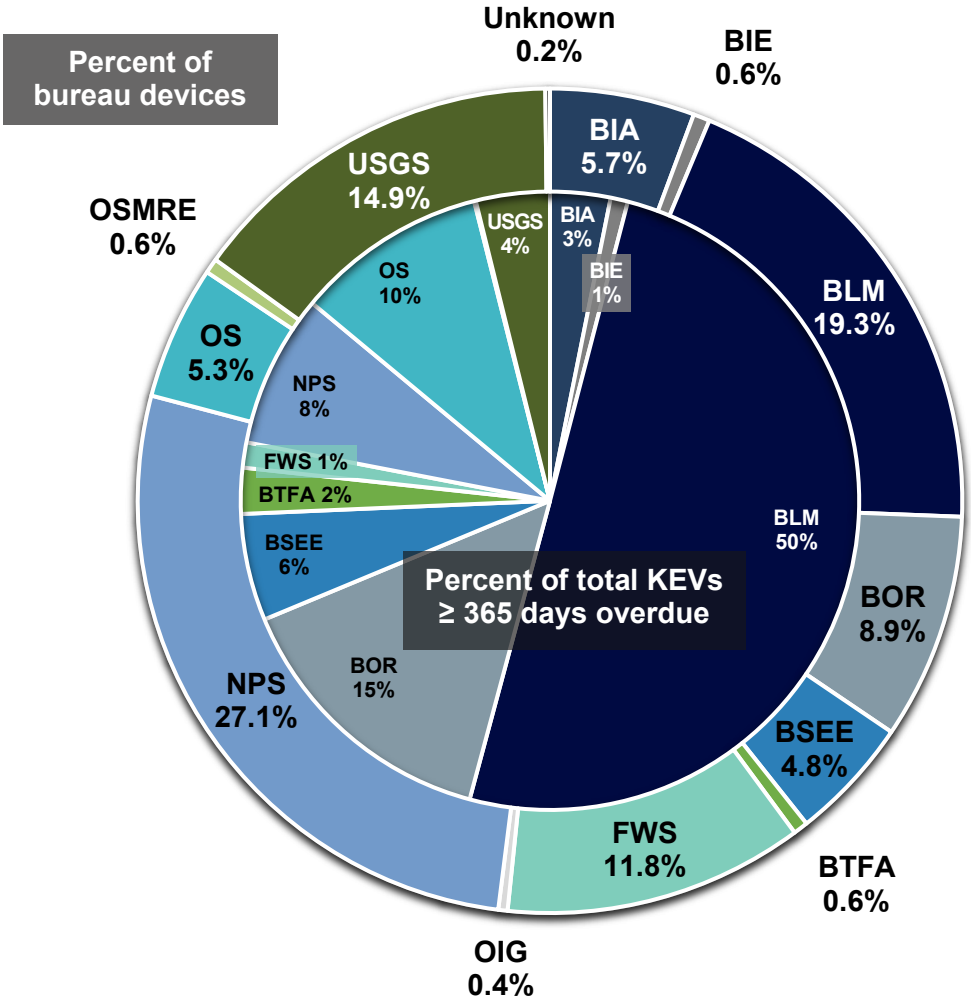
- BLM was accountable for 50 percent of the total number of KEVs overdue by at least 365 days as of the end of July 2023, despite only owning roughly 20 percent of DOI's total hardware assets. This makes BLM's hardware assets the highest risk to all other bureau and office assets. When we asked BLM why KEVs remained open for over a year, its response was "priorities and lack of resources."

- BOR was accountable for 15 percent of the total number of KEVs overdue by at least 365 days as of the end of July 2023, despite only owning roughly 9 percent of DOI's total hardware assets. When we asked BOR why KEVs remained open for over a year, we learned that BOR believed many affected assets had been decommissioned. However, our analysis revealed that the assets BOR stated that it believed to be decommissioned had not yet been removed from the network and therefore were still vulnerable.
- OS was accountable for 10 percent of the total number of KEVs overdue by at least 365 days as of the end of July 2023, despite only owning roughly 5 percent of DOI's total hardware assets. When we asked the OS why KEVs remained open for over a year, we learned that there was confusion between the OS and the OCIO over which office was responsible for which assets and vulnerabilities. This is because both offices' assets are combined within the OS repository in the vulnerability management system ([redacted]) even though the OCIO is not an office within the OS.

[33] In July 2023, the hardware asset management system, [redacted], identified 201,353 assets.

Figure 4 illustrates the distribution of bureau and office hardware assets in comparison to the total number of KEVs that were 365 days or more past the CISA due date as of the end of July 2023.

Figure 4: Bureau and Office* Distribution of Hardware Assets (Outer Ring) Compared with Distribution of KEVs Overdue by 365 Days or More (Inner Ring) as of July 2023



Source: DOI OIG.

* DOI OIG was the only office that did not have any KEVs overdue by 365 days or more. OSMRE is omitted from the inner ring because it had less than 1 percent of the KEVs overdue by one year or more.

Additionally, BOD 22-01 does not allow for risk acceptance of KEVs, but both BOR and OS reported that they were either in the process of or had already accepted the risk of some of the open KEVs, in violation of this mandate. While agency authorizing officials generally have the authority to accept cybersecurity risks when mission needs outweigh the risk of a vulnerability, BOD 22-01 explicitly requires agencies to either remediate KEVs or remove vulnerable assets from agency networks "if the impacted product is end-of-life or cannot be updated otherwise." That is, risk acceptance is not an option for a KEV.

BOD 22-01 explicitly requires agencies to either remediate KEVs or remove vulnerable assets from agency networks "if the impacted product is end-of-life or cannot be updated otherwise."

We found FWS, NPS, and USGS had fewer overdue KEVs when compared to the number of hardware assets. These bureaus improved visibility into their networks by implementing additional vulnerability management capabilities as follows:

- USGS went beyond DOI's requirements and stated they have installed the vulnerability management tool's ([redacted]) additional software agents[34] on their computers, which allow them to better monitor devices that are not directly connected to the internal network.

- FWS and NPS stated that they have implemented supplemental vulnerability management tools because DOI's system did not have the capacity to fully meet their additional ad hoc scanning needs.[35]

While bureaus and offices are responsible for remediating their vulnerabilities in accordance with their own vulnerability remediation procedures, the OCIO stated it is responsible for providing tools and oversight to bureaus and offices to ensure compliance with DOI and Federal requirements, including CISA BOD 22-01 for KEVs and CISA BOD 19-02 for internet-accessible systems. However, we determined that the OCIO guidance was inadequate and that it provided insufficient oversight and historical data.

[34] In the context of vulnerability management, a software agent installed on a computer can scan the host on which it is installed and report discovered vulnerabilities to a management server.

[35] Ad hoc scans are one-time or on-demand vulnerability scans performed outside of the scheduled scanning period.

Conclusion and Recommendations

Conclusion

In the current cyber-threat environment, Federal agencies must quickly remediate vulnerabilities in their systems to reduce the window of opportunity for attackers. Quick remediation of security vulnerabilities in Federal information systems is critical to mitigate risks that could lead to fraud, waste, abuse, and mismanagement and establish a robust security posture.

We found that 9,384 KEVs were at least 30 days past CISA's remediation due dates and nearly half of those vulnerabilities were more than one year past due. CISA designated these vulnerabilities as KEVs because they identified them as being actively exploited. In addition, we found 153,665 critical- and high-impact vulnerabilities in DOI systems that were not remediated in accordance with CISA and DOI remediation timeframes. DOI must remediate vulnerabilities in a timely manner, as quickly patching vulnerabilities reduces the window of opportunity for attackers. If exploited, these vulnerabilities could have serious or severe adverse effects on DOI operations including, but not limited to, system takeover by malicious third parties, ransomware, or exposure of sensitive data. If DOI is not aware of or accurately reporting its security posture, its Federal-level risk-based decision making could be impeded and result in escalated risk of information system compromise.

The weaknesses that we identified occurred because the OCIO did not conduct effective oversight of bureau and office remediation activities to ensure remediation was appropriate and adhered to CISA and DOI requirements. Furthermore, because the OCIO relied on only the most current data and did not track historical data for vulnerabilities, it was unaware of the most critical vulnerabilities that had gone unmitigated for extended periods.

We make the following recommendations to help DOI strengthen its IT governance practices pertaining to vulnerability management and reduce the risk unmitigated vulnerabilities pose to DOI IT assets.

Recommendations Summary

We provided a draft of this report to the OCIO for review. The OCIO concurred with all recommendations. We clarified Recommendations 4 and 9 after reviewing OCIO's response. We consider all recommendations resolved. We determined that Recommendations 1 and 4 are significant and will be reported as such in our semiannual report to Congress in accordance with the Inspector General Act.[36] Below we summarize OCIO's response to our recommendations, as well as our comments on its response. See Appendix 4 for the full text of OCIO's response; Appendix 5 lists the status of each recommendation.

We recommend that the OCIO:

1. Require DOI bureaus and offices to prioritize vulnerability remediation according to risk as defined by the system owner and ensure that all overdue known exploited vulnerabilities are validated and remediated.

   OCIO Response: The OCIO concurred with our recommendation and stated that the OCIO "will direct all bureaus and offices to validate and remediate all overdue known exploited vulnerabilities in accordance with existing DOI security control standards." The OCIO provided October 30, 2025, as a target implementation date.

[36] The Inspector General Act of 1978, 5 U.S.C. § 405(b), requires inspectors general to prepare semiannual reports summarizing OIG activities during the immediately preceding 6-month periods ending March 31 and September 30. It also states that these semiannual reports should include an identification of each "significant recommendation" described in previous semiannual reports on which corrective action has not been completed.

OIG Comment: We consider this recommendation resolved, based on the OCIO's response. The recommendation will be considered implemented when the OCIO provides documentation demonstrating that it required bureaus and offices to prioritize vulnerability remediation according to risk as defined by the system owner and ensures that overdue known exploited vulnerabilities are validated and remediated.

2. Review and analyze DOI bureau and office vulnerability scan results against their internal procedures to identify and implement overall improvements across DOI.

   OCIO Response: The OCIO concurred with our recommendation and stated that "DOI OCIO will review and analyze DOI bureau and office vulnerability scan results against internal procedures to identify and implement overall improvements across DOI." The OCIO provided October 30, 2025, as a target implementation date.

   OIG Comment: We consider this recommendation resolved, based on OCIO's response. We will consider the recommendation implemented when OCIO provides documentation demonstrating that it reviewed and analyzed DOI bureau and office vulnerability scan results against their internal procedures to identify and implement overall improvement across DOI.

3. Query bureaus and offices for all current systems with publicly available interfaces and develop a DOI-wide inventory that maintains IP addressing and service ports, system ownership, and point of contact information.

   OCIO Response: The OCIO concurred with our recommendation and stated that "DOI OCIO will develop a DOI-wide inventory that maintains IP addressing and service ports, system ownership, and point of contact information." The OCIO provided October 30, 2025, as a target implementation date.

   OIG Comment: We consider this recommendation resolved, based on OCIO's response. We will consider the recommendation implemented when OCIO provides documentation demonstrating that it queried bureaus and offices for all current systems with publicly available interfaces and developed a DOI-wide inventory that maintains IP addressing and service ports, system ownership, and point of contact information.

4. Develop a process whereby all changes to publicly available systems and newly deployed systems are updated in a DOI-wide inventory and included in any security assessments and monitoring.

   OCIO Response: The OCIO concurred with our recommendation and stated that "DOI OCIO will develop a DOI-wide inventory of publicly available systems, to include newly deployed systems for inclusion in security assessments and monitoring." Additionally, to address this recommendation the OCIO stated in follow-up discussions that it will develop a process to build the inventory. The OCIO provided October 30, 2025, as a target implementation date.

   OIG Comment: We consider this recommendation resolved, based on OCIO's response and subsequent communication. We will consider the recommendation implemented when OCIO provides documentation demonstrating that it developed a process whereby all changes to publicly available systems and newly deployed systems are updated in a DOI-wide inventory and included in security assessments and monitoring.

5. Conduct regular reviews of all open vulnerabilities that are older than the required completion timeframes and ensure that any vulnerabilities that have not been closed are tracked in accordance with Federal requirements.

   OCIO Response: The OCIO concurred with our recommendation and stated that "DOI OCIO will conduct monthly enterprise Vulnerability Management reviews with DOI bureaus and offices to ensure all open vulnerabilities are tracked in accordance with Federal requirements." The OCIO provided December 30, 2025, as a target implementation date.

OIG Comment: We consider this recommendation resolved, based on OCIO's response. The recommendation will be considered implemented when OCIO provides documentation demonstrating regular reviews of all open vulnerabilities that are older than the required completion timeframes and ensures that any vulnerabilities that have not been closed are tracked in accordance with Federal requirements.

6. Establish a vulnerability management process that includes using historical data to identify and report vulnerabilities that have persisted beyond required remediation timeframes and sharing the data with bureaus and offices.

   OCIO Response: The OCIO concurred with our recommendation and stated that "DOI OCIO will establish an enterprise Vulnerability Management program using historical data to identify and report vulnerabilities that have persisted beyond required remediation timeframes and share the data with DOI bureaus and offices." The OCIO provided December 30, 2025, as a target implementation date.

   OIG Comment: We consider this recommendation resolved, based on OCIO's response. The recommendation will be considered implemented when OCIO provides documentation demonstrating it established a vulnerability management process that includes using historical data to identify and report vulnerabilities that have persisted beyond required remediation timeframes and shared the data with bureaus and offices.

7. Require bureaus and offices to use available tools to periodically evaluate for vulnerabilities persisting beyond approved timelines and prioritize their remediation.

   OCIO Response: The OCIO concurred with our recommendation and stated that "DOI OCIO concurs with this condition after receiving the notice of potential findings and recommendations [and] took immediate action to address the root cause and develop a resolution path. The OCIO will establish an enterprise Vulnerability Management program that will use available tools to periodically evaluate for vulnerabilities persisting beyond approved timelines and direct the appropriate parties to prioritize their remediation." The OCIO provided December 30, 2025, as a target implementation date.

   OIG Comment: We consider this recommendation resolved, based on OCIO's response. The recommendation will be considered implemented when OCIO provides documentation demonstrating it required bureaus and offices to use available tools to periodically evaluate for vulnerabilities persisting beyond approved timelines and prioritized their remediation.

8. Require bureaus and offices to remediate any vulnerabilities persisting beyond the timeframes required by Federal guidelines and Department policies.

   OCIO Response: The OCIO concurred with our recommendation and stated that "DOI OCIO will require DOI bureaus and offices to remediate vulnerabilities within appropriate timeframes." The OCIO provided October 30, 2025, as a target implementation date.

   OIG Comment: We consider this recommendation resolved, based on OCIO's response. The recommendation will be considered implemented when OCIO provides documentation demonstrating it required bureaus and offices to remediate any vulnerabilities persisting beyond the timeframes required by Federal guidelines and Department policies.

9. Require bureaus and offices to, once available, use updated guidance and resources provided by the Office of the Chief Information Officer, in response to Recommendation 4 of this report, to evaluate and prioritize remediation of vulnerabilities persisting beyond approved timelines.

   OCIO Response: The OCIO concurred with our recommendation and stated that "DOI OCIO will develop a DOI-wide inventory of publicly available systems including all changes to publicly available systems and newly deployed systems for inclusion in security assessments and monitoring. Appropriate entities will evaluate and prioritize remediation of vulnerabilities persisting beyond approved timelines." Additionally, the OCIO stated in follow-up discussions that it will require the use of

the guidance developed in response to Recommendation 4 to address this recommendation. The OCIO provided October 30, 2025, as a target implementation date.

OIG Comment: We consider this recommendation resolved, based on OCIO's response and subsequent communication. The recommendation will be considered implemented when OCIO provides documentation demonstrating it required bureaus and offices to use updated guidance and resources to evaluate and prioritize remediation of vulnerabilities persisting beyond approved timelines.

Appendix 1: Scope and Methodology

Scope

We inspected the U.S. Department of the Interior's (DOI's) cybersecurity risks by mining its Continuous Diagnostics and Mitigation (CDM) vulnerability management tool's ([redacted]) dataset feeds on the enterprise data collection tool ([redacted]) from July 2022 to July 2023. We inspected whether DOI identified software vulnerabilities and ensured they were remediated and accurately reported in accordance with Federal requirements. In addition, we coordinated with DOI's Office of the Chief Information Officer (OCIO) to obtain records and evaluate whether policies and procedures are in accordance with Federal requirements.

Our inspection focused only on DOI's CDM vulnerability management capability and associated vulnerability identification and remediation practices.

We were unable to fully report on whether internet-accessible information systems complied with Federal policies due to DOI's incomplete inventory management. Specifically, DOI's lack of an inventory of internet-accessible systems hindered our ability to fully categorize due dates for some vulnerabilities. We note that inventory management has been a persistent issue for DOI. In our 2018 inspection of DOI's email and web security mandates,[37] we included a finding that DOI relied on outside agencies to discover and report its internet-accessible websites.

Methodology

We conducted our inspection in accordance with the *Quality Standards for Inspection and Evaluation* as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work we performed provides a reasonable basis for our conclusions and recommendations.

We performed the following inspection tasks to test the operation and reliability of internal controls over activities related to our inspection:

- Conducting interviews with DOI's OCIO to gather all records of information on policies and procedures.
- Conducting a visual walkthrough of CDM tools and vulnerability management systems.
- Interviewing bureau and office personnel responsible for remediating vulnerabilities.[38]
- Reviewing DOI and Federal policies and procedures for vulnerability management.
- Mining software, hardware, and vulnerability data collected from DOI's CDM tools and DOI's enterprise data collection tool ([redacted]).
- Validating datasets using custom queries.
- Mining open vulnerabilities classified as critical and high for duration of overdue days (30, 60, 90, 180, and 365 days), ensuring vulnerabilities were not duplicated per device.

[37] *The Department of the Interior Generally Complied with Email and Web Security Requirements* (Report No. 2018-ITA-019), issued July 2018, https://www.doioig.gov/reports/inspection/department-interior-generally-complied-email-and-web-security-mandates.

[38] See http://www.doi.gov/bureaus for a full list of the DOI's bureaus and a link to a full list of all departmental offices. For this report, we use the bureau and office labels as they are defined in DOI's primary CDM vulnerability management tool, which differs from DOI's organizational structure.

- Determining whether vulnerability scans were conducted with credentials by extracting and analyzing vulnerability plug-in data.

We acquired seven terabytes of compressed data from DOI's enterprise collection tool. To mine and aggregate the data, we housed it locally within our own datastore, which is a repository of databases. Once in our datastore, we mined the overdue vulnerabilities by bureau for durations of overdue days (30, 60, 90, 180, and 365 days). We performed verifications using the original enterprise data collection tool ([redacted]) to ensure accuracy.

We focused our analysis on the tools DOI used to collect vulnerability data prior to their integration into the CDM Agency Dashboard because of data quality concerns. Poor data quality has affected the accuracy and reliability of the vulnerability data displayed in the CDM Agency Dashboard. The full dataset was also too large to analyze within our project timeframe, so we focused on analyzing data only from DOI's mandated vulnerability management tool ([redacted]). We then further reduced the size of the dataset by only looking at vulnerabilities identified as high or critical severity. While the Cybersecurity and Infrastructure Security Agency's KEV catalog includes vulnerabilities that are designated as medium or low, we did not include those known exploited vulnerabilities (KEVs) in our analysis.

We further analyzed the extracted vulnerabilities greater than 30 days old and found a total of 153,665. Because of the high number of vulnerabilities that were 30 days or more overdue, we conducted further analysis and identified that 9,384 of those vulnerabilities were open KEVs.

To support our findings during our fieldwork phase, we issued a Notice of Potential Findings and Recommendations (NPFR) to each bureau and office that had overdue KEVs on their network for 365 days or more. We determined that the full dataset of overdue KEVs was too large for the bureaus and offices to review and validate. After analyzing varying ages of overdue KEVs, we determined that limiting our dataset to overdue KEVs on their networks for 365 days or more would provide us with a small enough subset for the bureaus and offices to validate and respond to within project timelines.

We issued NPFRs to each bureau and office with data for vulnerabilities that:

- Were KEVs.
- Had a severity of critical or high.
- Existed on a device for greater than or equal to 365 days.

Appendix 2: Report Abbreviations

Abbreviation	Definition
BIA	Bureau of Indian Affairs
BIE	Bureau of Indian Education
BLM	Bureau of Land Management
BOD	Binding Operational Directive
BOEM	Bureau of Ocean Energy Management
BOR	Bureau of Reclamation
BSEE	Bureau of Safety and Environmental Enforcement
BTFA	Bureau of Trust Funds Administration
CDM	Continuous Diagnostics and Mitigation
CISA	Cybersecurity and Infrastructure Security Agency
CVE	Common Vulnerabilities and Exposures
DHS	U.S. Department of Homeland Security
DOI	U.S. Department of the Interior
DNS	Domain Name System
FWS	U.S. Fish and Wildlife Service
IP	Internet Protocol
IT	Information Technology
KEVs	Known Exploited Vulnerabilities
NIST	National Institute of Standards and Technology
NPS	National Park Service
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONRR	Office of Natural Resources Revenue
OS	Office of the Secretary
OSMRE	Office of Surface Mining Reclamation and Enforcement
USGS	U.S. Geological Survey

Appendix 3: Vulnerability Management Findings and Recommendations From Prior OIG Reviews

We have conducted four prior reviews of DOI's cybersecurity program that contained findings and recommendations specifically related to DOI's vulnerability management.

- In October 2016, we issued an evaluation report[39] that included a finding that all three bureaus reviewed failed to detect critical- and high-risk vulnerabilities on their high-value IT assets. Specifically, thousands of critical- and high-risk vulnerabilities were left unmitigated for years on three high-value IT assets operated by bureaus. These deficiencies occurred because bureaus did not use the most effective techniques for vulnerability detection, promptly mitigate discovered vulnerabilities, or quarantine systems when critical- and high-risk vulnerabilities went unmitigated. We also found that because DOI did not have a complete inventory of computers, it could not ensure that the vulnerability detection and mitigation process was applied to the entirety of its environment. As a result, some DOI computers may not have undergone vulnerability scanning and thus may contain undetected and uncorrected vulnerabilities.

- In February 2017, we issued an evaluation report[40] that included a finding that thousands of unmitigated critical and high vulnerabilities existed on a high-value IT asset. These deficiencies occurred because the bureaus did not effectively oversee the contractor responsible for implementing required security controls, promptly mitigate discovered vulnerabilities, and mitigate vulnerabilities associated with unsupported software by either removing the software or upgrading to a newer version. Moreover, we found that a lack of complete inventories at the bureaus could result in them being unable to ensure that the vulnerability detection and mitigation process was applied to the entirety of its environment. As a result, some bureau computers may not have undergone vulnerability scanning and may contain undetected and uncorrected vulnerabilities.

- In July 2018, we issued an inspection of DOI's email and web security mandates[41] that included a finding that DOI did not maintain its own inventory of publicly accessible websites. Instead, DOI relied on outside agencies to inform it of its publicly accessibly websites. Specifically, these outside agencies did not identify or scan 357 additional websites that were not identified on DOI's inventory and did not comply with security requirements. This occurred because DOI relied on outside agencies to discover and report its internet-accessible websites. As a result, these sites had a greater risk of leaking sensitive data and communications.

- In March 2021, we issued an evaluation report[42] that included a finding of 25 high-risk vulnerabilities associated with two identified assets that did not have patches applied in a timely manner. In some instances, patches were not applied in a timely manner due to limited availability of bureau security staff during the 35-day furlough period that occurred from December 22, 2018, to January 25, 2019. In other instances, the patches were scheduled when the identified assets were offline. We confirmed that the vulnerabilities identified were appropriately patched by the next subsequent vulnerability scan in February 2019.

---

[39] *U.S. Department of the Interior's Continuous Diagnostics and Mitigation Program Not Yet Capable of Providing Complete Information for Enterprise Risk Determinations* (Report No. ISD-IN-MOA-0004-2014-I—Revised), issued October 2016, https://www.doioig.gov/reports/evaluation/dois-cdm-program-not-capable-providing-complete-information-enterprise-risk.

[40] *Information Technology Security Weaknesses at a Core Data Center Could Expose Sensitive Data* (Report No. 2016-ITA-021), issued February 2017, https://www.doioig.gov/reports/evaluation/information-technology-security-weaknesses-core-data-center-could-expose.

[41] *The Department of the Interior Generally Complied with Email and Web Security Requirements* (Report No. 2018-ITA-019), issued July 2018, https://www.doioig.gov/reports/inspection/department-interior-generally-complied-email-and-web-security-mandates.

[42] *Weaknesses in a USGS System Leave Assets at Increased Risk of Attack* (Report No. 2019-ITA-003), issued March 2021, https://www.doioig.gov/reports/inspection-evaluation/weaknesses-usgs-system-leave-assets-increased-risk-attack.

The following figure provides the recommendations from these inspections and evaluations that relate to vulnerability management.

Figure 5: Status of Vulnerability Management Recommendations from Prior Reviews

Recommendation	Closure Request Date	Status	Action Required
ISD-IN-MOA-0004-2014-I-04 We recommend that DOI's Chief Information Officer incorporate and enforce the following items into its newly evolving vulnerability management program— a. enterprise-level monitoring and reporting of all devices and software packages; b. enterprise-level enforcement of consistent assessment, detection, prioritization, and remediation techniques; c. required elevated account credential usage for testing; d. enterprise-level monitoring and bureau accountability for patch deployment; and e. enterprise-level quarantining for critically vulnerable systems that are not patched in a pre-defined timeframe.	N/A – Still open	**Resolved**	In response to our 2016 report, the Office of the Chief Information Officer (OCIO) provided a target completion date of June 30, 2018. The OCIO has since changed this date to December 2025.
2016-ITA-021-04 We recommend that the Bureau of Indian Affairs (BIA) ensure that critical and high-risk vulnerabilities on BIA and BIE [Bureau of Indian Education] systems are mitigated within 30 days of detection in accordance with DOI policy.	08/2019	**Implemented**	BIA stated it developed a full vulnerability remediation/mitigation strategy that implements a logical process that begins with the discovery and identification of vulnerabilities and ends with continuous risk monitoring. Comprehensive procedural and process documentation now exists to ensure that critical- and high-risk vulnerabilities on BIA and BIE systems are mitigated in accordance with DOI policy.

Recommendation	Closure Request Date	Status	Action Required
2018-ITA-019 We recommend that OCIO develop a comprehensive inventory management program that includes periodic discovery scanning for all publicly accessible websites and IP ranges, including those with non-.gov domains.	03/2021	**Implemented**	The OCIO reported that it had established a registration system and issued policy direction to the bureaus and offices to register and maintain their inventory. The OCIO stated that it did not concur with the OIG's recommendation to conduct periodic discovery scanning because this would unnecessarily duplicate the Government-wide scanning program. The OCIO stated it will communicate gaps in scanning to the GSA to inform continual improvement of the Governmentwide scanning program.
2018-ITA-019 We recommend that OCIO evaluate the websites we discovered for compliance with OMB and DHS web security requirements and submit the missing websites to the General Services Administration (GSA) for inclusion.	05/2019	**Implemented**	The OCIO stated that it added any confirmed missing websites to the Department of the Interior Public Website Registry. The OCIO further stated it confirmed that all systems within the scope of the OIG report are covered by the DHS external vulnerability Cyber Hygiene Assessment scanning service.
2019-ITA-003-08 We recommend that the U.S. Geological Survey (USGS) ensure that the process to identify and mitigate high-risk vulnerabilities within 30 days, as required by OCIO policy, is followed.	08/2022	**Implemented**	USGS stated that it performed vulnerability remediation on the IT asset and performs monthly vulnerability scans to ensure ongoing vulnerabilities are addressed.

Appendix 4: Response to Draft Report

The OCIO response to our draft report follows on page 26.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

July 23, 2025

Memorandum

To: Nicki M. Miller
Assistant Inspector General for Audits, Inspections, and Evaluations
Office of Inspector General

From: Paul A. McInerny
Chief Information Officer PAUL MCINERNY Digitally signed by PAUL MCINERNY Date: 2025.07.23 17:40:12 -04'00'
Office of the Chief Information Officer

Subject: Office of the Chief Information Officer (OCIO) Response to Recommendations from OIG Report on Unmitigated Known Vulnerabilities (2023-ITA-007)

Thank you for the opportunity to review and comment on the draft report, entitled *The U.S. Department of the Interior Information Systems at Increased Risk Due to Unmitigated Known Vulnerabilities* (2023-ITA-007). The Department of the Interior (Department, Interior), Office of the Chief Information Officer (OCIO) appreciates the Office of Inspector General's (OIG's) work in planning this engagement, conducting its review, and issuing the report on our vulnerability management capability. The information contained in the report will assist us in successfully moving forward with the improvements to our cybersecurity program throughout the Department. The Interior/OCIO leadership understands the importance of strengthening the Department's cybersecurity capabilities to reduce risk to the enterprise and improve the resilience of the information technology environment in the face of constantly evolving adversaries. This memorandum including attachment(s) responds to the draft report and will be emailed to aie_reports@doioig.gov as requested.

If you have any questions, please contact Louis Eichenbaum, Acting Chief Information Security Officer, Cybersecurity Division, at louis_eichenbaum@ios.doi.gov and Rachel Sile, Acting Chief, Cybersecurity Operations Branch at rachel_sile@ios.doi.gov.

Attachment 1: Recommendations and Management Response

Cc: Sherrill E. Exum, Chief, Audit Management Division, Office of Financial Management
Rachel Sile, Acting Chief, Cybersecurity Operations Branch
Jason Swegle, Chief, Governance, Risk, and Compliance Branch, OCIO

Attachment 1: Recommendations and Management Responses to *The U.S. Department of the Interior Information Systems at Increased Risk Due to Known Vulnerabilities* (2023-ITA-007)

Recommendation 1: Require DOI bureaus and offices to prioritize vulnerability remediation according to risk as defined by the system owner and ensure that all overdue known exploited vulnerabilities are validated and remediated.

Management Response: Concur. DOI Office of the Chief Information Officer (OCIO) will direct all bureaus and offices to validate and remediate all overdue known exploited vulnerabilities in accordance with existing DOI security control standards.

Responsible Official: Louis Eichenbaum, Deputy CIO and Acting CISO, Cybersecurity Division

Task Managers: Rachel Sile, Acting Chief, Cybersecurity Operations Branch; Jason Swegle, Chief, Governance, Risk, and Compliance Branch

Target Date: October 30, 2025

Recommendation 2: Review and analyze DOI bureau and office vulnerability scan results against their internal procedures to identify and implement overall improvements across DOI.

Management Response: Concur. DOI OCIO will review and analyze DOI bureau and office vulnerability scan results against internal procedures to identify and implement overall improvements across DOI.

Responsible Official: Louis Eichenbaum, Deputy CIO and Acting CISO, Cybersecurity Division

Task Managers: Rachel Sile, Acting Chief, Cybersecurity Operations Branch

Target Date: October 30, 2025

Recommendation 3: Query bureaus and offices for all current systems with publicly available interfaces and develop a DOI-wide inventory that maintains IP addressing and service ports, system ownership, and point of contact information.

Management Response: Concur. DOI OCIO will develop a DOI-wide inventory that maintains IP addressing and service ports, system ownership, and point of contact information.

Responsible Official: Louis Eichenbaum, Deputy CIO and Acting CISO, Cybersecurity Division

Task Manager: Rachel Sile, Acting Chief, Cybersecurity Operations Branch; Stacy Richkun, Chief, Oversight, Planning, and Programming Branch

Target Date: October 30, 2025

Recommendation 4: Develop a process whereby all changes to publicly available systems and newly deployed systems are updated in a DOI-wide inventory and included in any security assessments and monitoring.

Management Response: Concur. DOI OCIO will develop a DOI-wide inventory of publicly available systems, to include newly deployed systems for inclusion in security assessments and monitoring.

Responsible Official: Louis Eichenbaum, Deputy CIO and Acting CISO, Cybersecurity Division

Task Managers: Rachel Sile, Acting Chief, Cybersecurity Operations Branch; Stacy Richkun, Chief, Oversight, Planning, and Programming Branch

Target Date: October 30, 2025

Recommendation 5: Conduct regular reviews of all open vulnerabilities that are older than the required completion timeframes and ensure that any vulnerabilities that have not been closed are tracked in accordance with Federal requirements.

Management Response: Concur. DOI OCIO will conduct monthly enterprise Vulnerability Management reviews with DOI bureaus and offices to ensure all open vulnerabilities are tracked in accordance with Federal requirements.

Responsible Official: Louis Eichenbaum, Deputy CIO and Acting CISO, Cybersecurity Division

Task Managers: Rachel Sile, Acting Chief, Cybersecurity Operations Branch; Stacy Richkun, Chief, Oversight, Planning, and Programming Branch

Target Date: December 30, 2025

Recommendation 6: Establish a vulnerability management process that includes using historical data to identify and report vulnerabilities that have persisted beyond required remediation timeframes and sharing the data with bureaus and offices.

Management Response: Concur. DOI OCIO will establish an enterprise Vulnerability Management program using historical data to identify and report vulnerabilities that have persisted beyond required remediation timeframes and share the data with DOI bureaus and offices.

Responsible Official: Louis Eichenbaum, Deputy CIO and Acting CISO, Cybersecurity Division

Task Manager: Rachel Sile, Acting Chief, Cybersecurity Operations Branch; Stacy Richkun, Chief, Oversight, Planning, and Programming Branch

Target Date: December 30, 2025

Recommendation 7: Require bureaus and offices to use available tools to periodically evaluate for vulnerabilities persisting beyond approved timelines and prioritize their remediation.

Management Response: Concur. DOI OCIO concurs with this condition after receiving the notice of potential findings and recommendations took immediate action to address the root cause and develop a resolution path. The OCIO will establish an enterprise Vulnerability Management program that will use available tools to periodically evaluate for vulnerabilities persisting beyond approved timelines and direct the appropriate parties to prioritize their remediation.

Responsible Official: Louis Eichenbaum, Acting CISO, Cybersecurity Division

Task Managers: Rachel Sile, Acting Chief, Cybersecurity Operations Branch

Target Date: December 30, 2025

Recommendation 8: Require bureaus and offices to remediate any vulnerabilities persisting beyond the timeframes required by Federal guidelines and Department policies.

Management Response: Concur. DOI OCIO will require DOI bureaus and offices to remediate vulnerabilities within appropriate timeframes.

Responsible Official: Louis Eichenbaum, Deputy CIO and Acting CISO, Cybersecurity Division

Task Managers: Rachel Sile, Acting Chief, Cybersecurity Operations Branch; Stacy Richkun, Chief, Oversight, Planning, and Programming Branch

Target Date: October 30, 2025

Recommendation 9: Require bureaus and offices to once available, use updated guidance and resources provided by the Office of the Chief Information Officer, in response to Recommendation 4 of this report, to evaluate and prioritize remediation of vulnerabilities persisting beyond approved timelines.

Management Response: Concur. DOI OCIO will develop a DOI-wide inventory of publicly available systems including all changes to publicly available systems and newly deployed systems for inclusion in security assessments and monitoring. Appropriate entities will evaluate and prioritize remediation of vulnerabilities persisting beyond approved timelines.

Responsible Official: Louis Eichenbaum, Deputy CIO and Acting CISO, Cybersecurity Division

Task Manager: Rachel Sile, Acting Chief, Cybersecurity Operations Branch

Target Date: October 30, 2025

Appendix 5: Status of Recommendations

Recommendation	Status	Action Required
2023-ITA-001-01 We recommend that the Office of the Chief Information Officer require DOI bureaus and offices to prioritize vulnerability remediation according to risk as defined by the system owner and ensure that all overdue known exploited vulnerabilities are validated and remediated.	Resolved	We will track implementation.
2023-ITA-007-02 We recommend that the Office of the Chief Information Officer review and analyze DOI bureau and office vulnerability scan results against their internal procedures to identify and implement overall improvements across DOI.	Resolved	We will track implementation.
2023-ITA-007-03 We recommend that the Office of the Chief Information Officer query bureaus and offices for all current systems with publicly available interfaces and develop a DOI-wide inventory that maintains IP addressing and service ports, system ownership, and point of contact information.	Resolved	We will track implementation.
2023-ITA-007-04 We recommend that the Office of the Chief Information Officer develop a process whereby all changes to publicly available systems and newly deployed systems are updated in a DOI-wide inventory and included in any security assessments and monitoring.	Resolved	We will track implementation.

Recommendation	Status	Action Required
2023-ITA-007-05 We recommend that the Office of the Chief Information Officer conduct regular reviews of all open vulnerabilities that are older than the required completion timeframes and ensure that any vulnerabilities that have not been closed are tracked in accordance with Federal requirements.	Resolved	We will track implementation.
2023-ITA-007-06 We recommend that the Office of the Chief Information Officer establish a vulnerability management process that includes using historical data to identify and report vulnerabilities that have persisted beyond required remediation timeframes and sharing the data with bureaus and offices.	Resolved	We will track implementation.
2023-ITA-007-07 We recommend that the Office of the Chief Information Officer require bureaus and offices to use available tools to periodically evaluate for vulnerabilities persisting beyond approved timelines and prioritize their remediation.	Resolved	We will track implementation.
2023-ITA-007-08 We recommend that the Office of the Chief Information Officer require bureaus and offices to remediate any vulnerabilities persisting beyond the timeframes required by Federal guidelines and Department policies.	Resolved	We will track implementation.

Recommendation	Status	Action Required
2023-ITA-007-09 We recommend that the Office of the Chief Information Officer require bureaus and offices to, once available, use updated guidance and resources provided by the Office of the Chief Information Officer in response to Recommendation 4 of this report to evaluate and prioritize remediation of vulnerabilities persisting beyond approved timelines.	Resolved	We will track implementation.

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

REPORT FRAUD, WASTE, ABUSE, AND MISMANAGEMENT

The Office of Inspector General (OIG) provides independent oversight and promotes integrity and accountability in the programs and operations of the U.S. Department of the Interior (DOI). One way we achieve this mission is by working with the people who contact us through our hotline.

WHO CAN REPORT?

Anyone with knowledge of potential fraud, waste, abuse, misconduct, or mismanagement involving DOI should contact the OIG hotline. This includes knowledge of potential misuse involving DOI grants and contracts.

HOW DOES IT HELP?

Every day, DOI employees and non-employees alike contact OIG, and the information they share can lead to reviews and investigations that result in accountability and positive change for DOI, its employees, and the public.

WHO IS PROTECTED?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act, and other applicable laws protect complainants. Specifically, 5 U.S.C. § 407(b) states that the Inspector General shall not disclose the identity of a DOI employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the course of the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-DOI employees who report allegations may also specifically request confidentiality.

If you wish to file a complaint about potential fraud, waste, abuse, or mismanagement in DOI, please visit OIG's online hotline at **www.doioig.gov/hotline** or call OIG's toll-free hotline number: **1-800-424-5081**