Report No. DOWIG-2026-092

~~CUI~~

INSPECTOR GENERAL

U.S. Department of War

JUNE 29, 2026

(U) Summary Report: Lessons Learned from DoW OIG Reports on Cyber Vulnerability and Patch Management

~~Controlled by: DoW OIG~~
~~Controlled by: Audit/Cyberspace Operations~~
~~CUI Category: OPSEC~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC: Acting Assistant Inspector General for Audit, Cyberspace Operations,~~ [redacted]

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

~~CUI~~

Pursuant to Executive Order 14347, "Restoring the United States Department of War," September 5, 2025, the Department of Defense Inspector General (DoD IG) and Office of Inspector General (DoD OIG) use the secondary titles of the Department of War Inspector General (DoW IG) and Office of Inspector General (DoW OIG), respectively. The use of these secondary titles does not in any way affect the primary statutory title or authorities of the DoD IG under The Inspector General Act of 1978, as amended (5 U.S.C. Chapter 4, Inspectors General), or the authorities or responsibilities of the DoD IG or DoD OIG pursuant to any laws, regulations, or policies.

OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF WAR
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

June 29, 2026

MEMORANDUM FOR DISTRIBUTION

SUBJECT: (U) Summary Report: Lessons Learned from DoW OIG Reports on Cyber Vulnerability and Patch Management (Report No. DOWIG-2026-092)

(U) This summary report is part of a series that presents key themes and lessons learned from our body of oversight work in several key areas. We provide these summaries to deliver helpful and timely information relevant to DoW priorities. As the DoW executes increasingly complex cyber offensive and defensive operations, applying prior lessons learned helps prevent repeated deficiencies and strengthens the DoW's ability to protect mission-critical networks, systems, and data.

(U) We reviewed DoW Office of Inspector General (DoW OIG) audit reports from the previous 7 years to identify trends and recurring challenges with vulnerability and patch management. Specifically, we identified systemic trends across 12 DoW OIG reports issued between March 2019 and May 2026 related to consistently scanning DoW networks for vulnerabilities, mitigating those vulnerabilities, and installing software updates timely. These lessons learned remain important today because risks tied to vulnerability and patch management continue to affect the Department's ability to protect its networks, systems, and data.

(U) The DoW OIG conducts regular oversight of actions taken by DoW Components to protect the Department's networks, systems, and data. The DoW OIG reports these findings in a timely manner to enable the DoW to strengthen its protections and improve its processes for addressing network and system vulnerabilities and installing software updates. We are providing this report for information and use; therefore, it does not contain recommendations.

(U) If you have any questions, please contact me at [redacted]

Sean J. Keaney
Acting Assistant Inspector General for Audit
Cyberspace Operations

(U) DISTRIBUTION:

SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARY OF WAR FOR ACQUISITION AND SUSTAINMENT
UNDER SECRETARY OF WAR FOR PERSONNEL AND READINESS
CHIEF INFORMATION OFFICER, DEPARTMENT OF WAR
COMMANDER, UNITED STATES CYBER COMMAND
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

(U) Introduction

(U) Department of War (DoW) organizations operate more than 15,000 unclassified and classified networks and cloud environments worldwide, collectively referred to as the DoW Information Network (DoWIN). As one of the largest network environments in the U.S. Government—supporting more than 3.2 million endpoints, 4 million computers, and 145,000 mobile devices as of FY 2025—the DoWIN remains a persistent target for adversaries seeking to compromise DoW systems and operations.[1] These threats require DoW Commanders and Directors to implement continuous, proactive, and well governed cybersecurity measures to defend the network.

(U) Recently, an artificial intelligence (AI) developer launched a cybersecurity initiative, in partnership with infrastructure companies, to address cybersecurity concerns raised by the capabilities of the developer's latest AI model. During the testing, that AI model was able to identify more than 10,000 high and critical vulnerabilities and create exploits in every major operating system and web browser. Advanced AI technology like this poses a significant risk to national security to the DoW if adversaries obtain access to the model. The AI model would outpace the DoW's ability to detect and respond to threats. To keep up with the latest AI models, the DoW must improve its processes for how quickly it identifies and mitigates vulnerabilities.

(U) Lessons Learned from Past DoW OIG Reports

(U) We identified lessons learned in 12 DoW OIG reports issued from March 2019 through May 2026 that included findings related to vulnerability and patch management. The 12 publicly available reports included 41 recommendations related to vulnerability and patch management, of which 6 are open and 35 are closed.[2] Previous DoW OIG reports identified recurring cybersecurity weaknesses related to vulnerability and patch management across multiple DoW Components that, if exploited, could allow malicious actors to gain unauthorized access to networks, systems, and data. DoW cybersecurity officials should revisit recommendations from previous DoW OIG reports, which recommend that officials consistently scan their networks for vulnerabilities, mitigate those vulnerabilities, and install software updates in a timely manner to reduce the risk of a successful cyber attack. Table 1 lists the 12 reports we reviewed and the associated lessons learned discussed in those reports.

[1] (U) An endpoint is any device that connects to a network such as laptops, desktop computers, mobile phones, tablets, servers, and network printers.

[2] (U) Open means that management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation. Closed means the DoW OIG verified that the agreed-upon corrective actions were implemented.

(U) Table 1. Lessons Learned in Past DoW OIG Reports

(U) Reports	Vulnerability Management	Patch Management
DOWIG-2026-083	X	
DODIG-2025-086	X	X
DODIG-2025-071	X	
DODIG-2025-053		X
DODIG-2023-041		X
DODIG-2022-061	X	
DODIG-2021-050*		
DODIG-2020-068	X	
DODIG-2020-067	X	
DODIG-2019-105	X	
DODIG-2019-089	X	
DODIG-2019-063	X	**(U)**

*(U) We identified best practices during this audit; therefore, the report does not include recommendations.
(U) Source: The DoW OIG.

(U) Vulnerability Management Challenges

(U) Previous DoW OIG reports identified recurring challenges in identifying and mitigating network vulnerabilities. Continuous and consistent network vulnerability scanning identifies security weaknesses that require mitigation before adversaries can exploit them. It helps to ensure that critical data, communication links, and weapons systems that our Service members rely on remain resilient and secure. Scanning complements patch management by serving as an objective auditing mechanism that confirms whether a vulnerability was resolved by installing a software patch. Continuous scanning sustains vulnerability management by providing up-to-date visibility into weaknesses and enabling risk-based prioritization and defined mitigation timelines. The following examples highlight these challenges and the actions organizations agreed to take to address them.

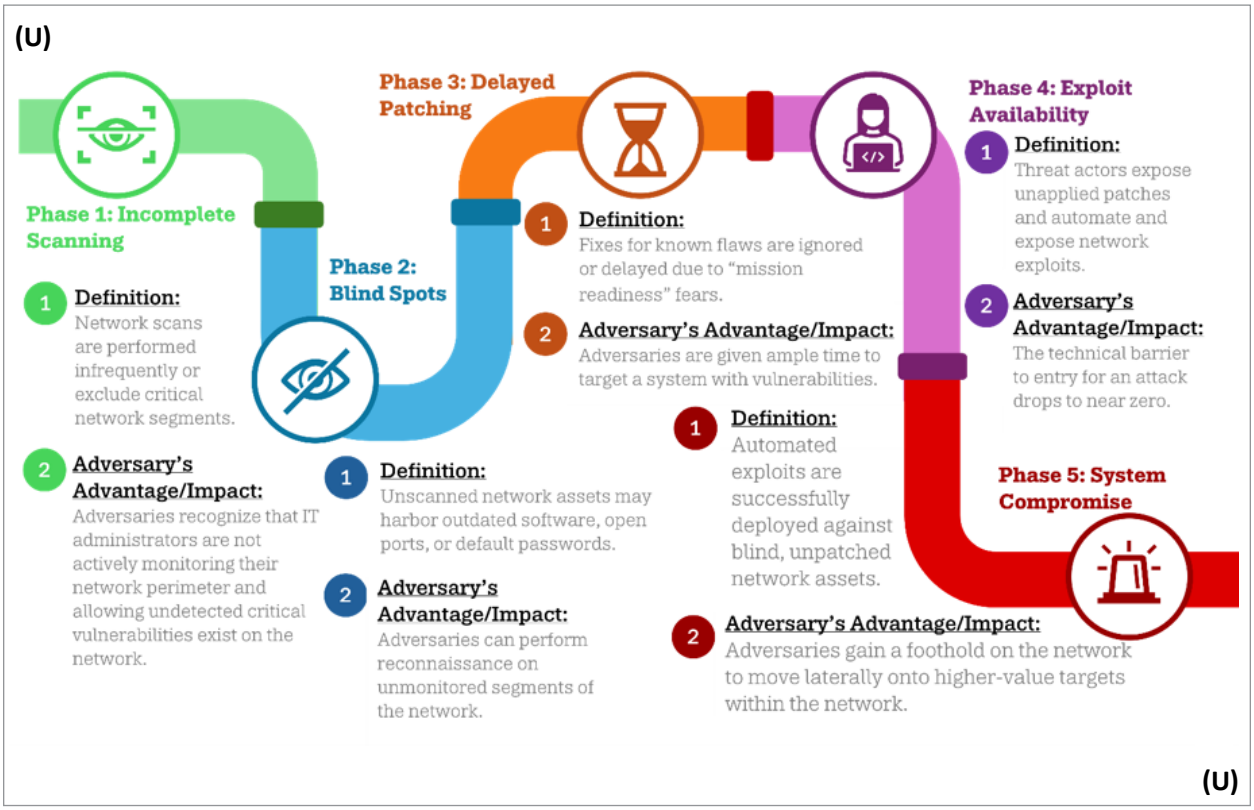
- (U) In a recent report, we determined that the Department of the Air Force did not always mitigate critical vulnerabilities. Based on our recommendation, the Air Force agreed to validate that identified vulnerabilities were mitigated effectively or document actions to be taken to mitigate any unmitigated vulnerabilities.
- (U) In another instance, we determined that contractors that process, transmit, and store DoW information did not identify and mitigate network and system vulnerabilities in a timely manner although contract terms required them to do so. In addition, network administrators of the contractors' networks did not develop plans of action and milestones for vulnerabilities that they could not mitigate. Based on our recommendations, the Director of Defense Research and Engineering for Research and

(U) Technology agreed to direct contracting officers to verify that contractors identify and mitigate vulnerabilities and develop plans of action and milestones for vulnerabilities that cannot be mitigated in a timely manner.

(U) Alternatively, in another report we identified best practices related to vulnerability scanning in which DoW Components assessed whether known cybersecurity risks existed on information technology they procured. Specifically, the Components ran vulnerability scans before procuring or using information technology products, or developed corrective action plans for vulnerabilities that could be mitigated immediately.

(U) Failing to regularly scan networks and mitigate vulnerabilities promptly can create a vulnerability risk pipeline that adversaries could use to move within the DoWIN and access sensitive mission data. Figure 1 illustrates how inconsistent vulnerability scanning and delayed mitigation can create a vulnerability risk pipeline—an escalating sequence of conditions that progressively increase an adversary's opportunities to penetrate the DoWIN. Each phase shows how routine cybersecurity lapses compound over time and how adversaries can exploit these weaknesses to gain unauthorized access to networks and mission-critical data.

(U) Figure 1. Vulnerability Risk Pipeline



(U) Source: The DoW OIG.

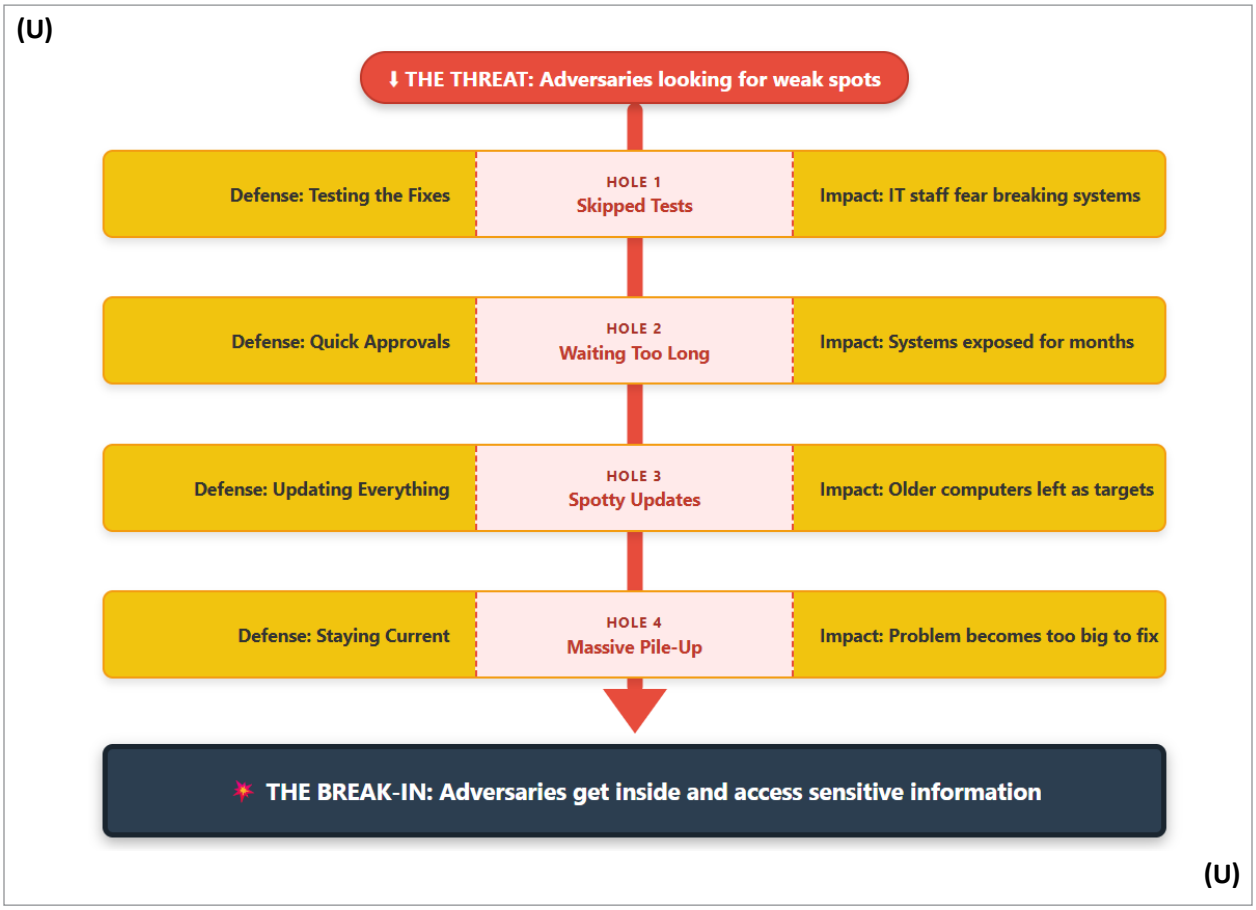
(U) Patch Management Challenges

(U) Previous DoW OIG reports identified recurring challenges related to installing software patches in a timely manner on vulnerable systems and networks. Patch management keeps the DoWIN resilient by fixing known software flaws before adversaries can exploit them. It works hand-in-hand with scanning—scanning finds the weaknesses, and patch management applies tested updates or configuration changes to close those gaps. Effective programs prioritize updates for vulnerabilities known to be actively exploited and set clear timelines to deploy those updates.

(U) In a recent management advisory, we determined that the Defense Information Systems Agency offered unmanaged applications with known cybersecurity vulnerabilities for instant messaging and social media, including one that allowed malicious code execution in Android mobile applications. This vulnerability was first published by the National Institute of Standards and Technology in August 2020. If adversaries were to successfully exploit this vulnerability on government-issued mobile devices, they could use the devices as an intelligence-gathering tool, allowing them to read sensitive emails, daily schedules, roster details, and internal command messages, directly compromising mission planning and readiness. In addition, adversaries could leverage the application's global positioning system, microphone, or camera, which can enable them to track the physical movements of military personnel, map out the patterns of secure facilities, or eavesdrop on sensitive briefings.

(U) When patches lag, publicly available exploits and code make it easier for adversaries to target unpatched systems and attempt access to DoWIN networks, increasing the risk of unauthorized access, data theft, service outages, and disruptions to mission operations. Clearing patch backlogs—starting with known-exploited vulnerabilities and systems that act as front doors into a network—directly lowers risk across the DoWIN. Figure 2 illustrates how missed testing, deferred approvals, and uneven deployment can create a patch backlog—an escalating sequence of conditions that expands opportunities for unauthorized access to mission-critical systems and data.

(U) Figure 2. Sequence of Patch Management Failures Enabling Adversary Access



(U) Source: The DoW OIG.

(U) Federal Information Security Modernization Act of 2014 Reporting

~~(CUI)~~ Since 2016, the DoW OIG has conducted annual reviews to assess the effectiveness of the DoW's information system policies, procedures, and practices and has issued annual independent evaluations in accordance with Public Law 113-283, "Federal Information Security Modernization Act of 2014 (FISMA)," December 18, 2014. As part of our recent FISMA reviews, DoW Components were asked, among other questions, "to what extent did the Components use vulnerability scanning and patch management?" In April 2025, for example, we reported that non-National Security Systems and systems . The lack of increases the risk that adversaries could exploit weaknesses on non-National Security Systems as a pivot point to move laterally into a National Security Systems.

(U) We have an ongoing FISMA review that will assess, in part, vulnerability and patch management—Project No. D2026-D000CP-0006.000, "FY 2026 Review of the DoD's Compliance with the FISMA of 2014," announced on December 3, 2025.

(U) Conclusion

(U) The pace of exploiting network vulnerabilities has accelerated—once a weakness is known, adversaries can leverage technology to target it within hours. It no longer takes weeks to weaponize known vulnerabilities. Given the advances of AI's ability to identify vulnerabilities and create exploits, DoW officials must reconsider their processes and timelines for managing identified vulnerabilities and software patches. Timely mitigation of network and software weaknesses—reinforced by current executive order requirements for secure and well-governed software practices—is essential to protecting DoW systems and networks. By applying the lessons learned from this body of work, the DoW can improve scanning completeness, reduce patch backlogs, enforce required mitigation timelines, and ensure that security weaknesses are addressed before adversaries can use them to compromise mission operations.

(U) Appendix

(U) Reports Reviewed to Identify Lessons Learned

(U) We reviewed DoW OIG audit reports from the previous 7 years to identify recurring challenges related to vulnerability and patch management. Table 2 lists the DoW OIG reports we reviewed to prepare this summary report. We are providing the list of reports as a resource for DoW management. The reports listed in the table contain additional details related to the lessons learned and past challenges the DoW OIG identified. Unrestricted DoW OIG reports can be accessed at https://www.dodig.mil/reports.html/.

(U) Table 2. List of DoW OIG Reports Reviewed

(U) Report Number	Report Title	Report Issue Date
DOWIG-2026-083	Audit of Cyber Vulnerabilities Impacting Department of the Air Force Defense Critical Infrastructure	May 13, 2026
DODIG-2025-086	Management Advisory: The DoD's FY 2024 Compliance with the Federal Information Security Modernization Act of 2014	April 16, 2025
DODIG-2025-071	Audit of Cyber Vulnerabilities Impacting Defense Critical Infrastructure	February 21, 2025
DODIG-2025-053	Audit of Cybersecurity of DoD Classified Mobile Devices	December 13, 2024
DODIG-2023-041	Management Advisory: The DoD's Use of Mobile Applications	February 9, 2023
DODIG-2022-061	Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors	February 22, 2022
DODIG-2021-050	Audit of Contracts for DoD Information Technology Products and Services Procured by DoD Components in Response to the Coronavirus Disease–2019 Pandemic	February 12, 2021
DODIG-2020-068	Audit of Security Controls Over the Department of Defense's Global Command and Control System–Joint Information Technology System	March 18, 2020
DODIG-2020-067	Followup Audit on Corrective Actions Taken by DoD Components in Response to DoD Cyber Red Team-Identified Vulnerabilities and Additional Challenges Facing DoD Cyber Red Team Missions	March 13, 2020
DODIG-2019-105	Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems	July 23, 2019
DODIG-2019-089	Audit of the DoD's Implementation of the Joint Regional Security Stacks	June 4, 2019
DODIG-2019-063	Followup Audit on the Military Departments' Security Safeguards Over SIPRNET Access Points	March 18, 2019 **(U)**

(U) Source: The DoW OIG.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF WAR

Whistleblower Protection
U.S. Department of War

Whistleblower Protection safeguards DoW employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoW OIG reports or activities, please contact us:

Legislative Affairs Division
legislative.affairs@dodig.mil

Public Affairs Division
public.affairs@dodig.mil

www.dodig.mil

DoD Hotline
www.dodig.mil/hotline

~~CUI~~

DEPARTMENT OF WAR OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

~~CUI~~