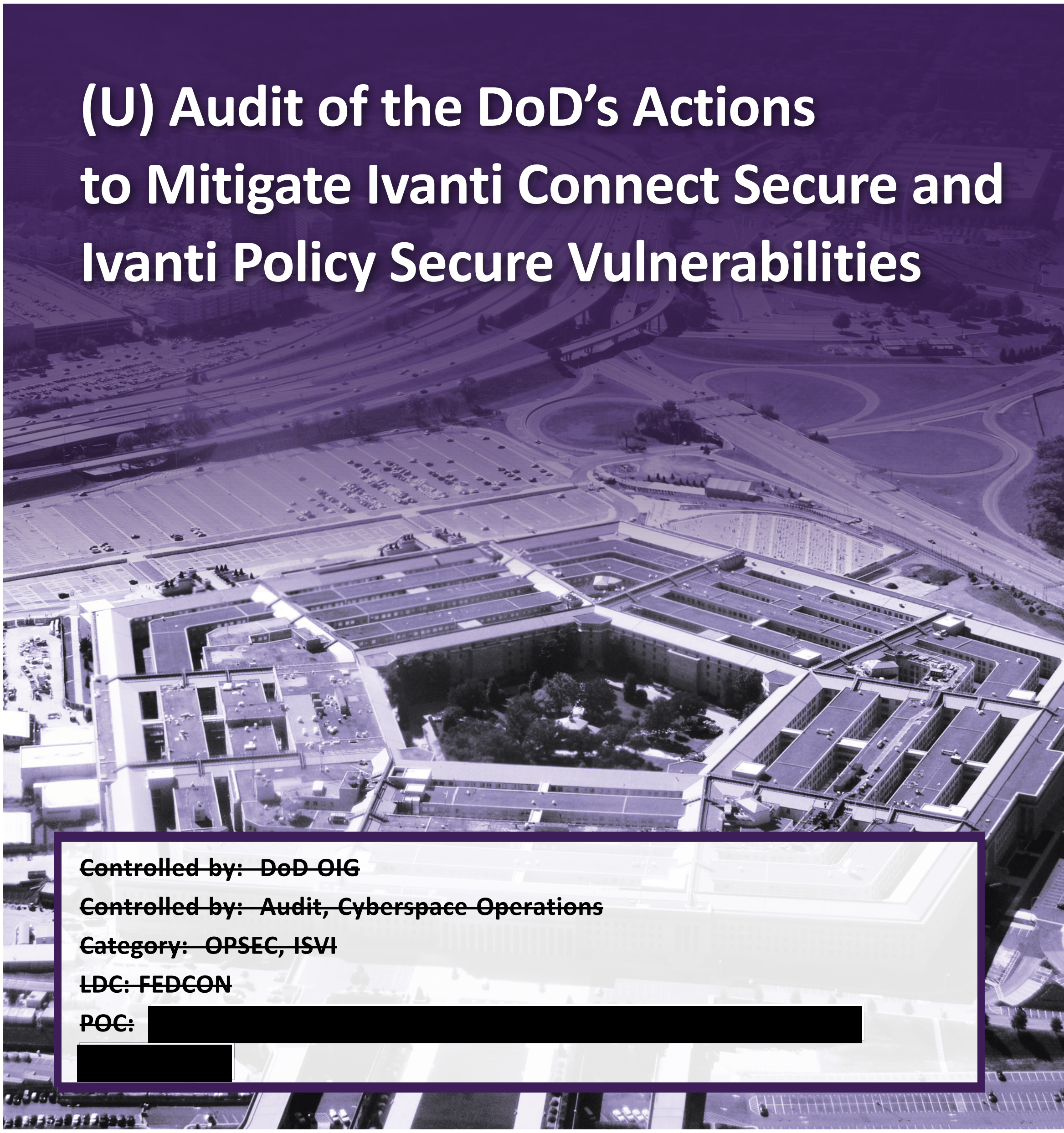
Report No. DODIG-2025-108

INSPECTOR GENERAL

U.S. Department of Defense

JUNE 4, 2025



(U) Audit of the DoD's Actions to Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

~~Controlled by: DoD OIG~~
~~Controlled by: Audit, Cyberspace Operations~~
~~Category: OPSEC, ISVI~~
~~LDC: FEDCON~~
~~POC:~~ [redacted]

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

(U) Results in Brief

(U) Audit of the DoD's Actions to Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

June 4, 2025

(U) Objective

(U) The objective of this audit was to determine whether the actions taken by DoD Components to identify, respond to, and mitigate vulnerabilities impacting Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) complied with DoD requirements.

(U) Background

~~(CUI)~~ Ivanti, Inc. provides information technology management and software solutions, including virtual private network (VPN) systems, such as ICS, which allow users to remotely connect to a network over the Internet through a secure tunnel. Between January 10, 2024, and February 8, 2024, Ivanti disclosed five critically severe or highly severe common vulnerabilities and exposures (CVEs) affecting ICS and IPS. Those CVEs could allow malicious actors to execute commands on a victim's network with elevated privileges. In response to the CVEs, Joint Force Headquarters-DoD Information Network (JFHQ-DODIN) issued multiple orders to the DoD Information Network areas of operation (DAOs) [redacted].

We reviewed the actions taken by five DAOs to comply with the JFHQ-DODIN orders related to Ivanti.

(U) Finding

~~(CUI)~~ [redacted] complied with the JFHQ-DODIN orders [redacted] ICS VPNs. However, [redacted] did not [redacted] This occurred because [redacted] relied on the results of [redacted] and did not officially notify [redacted] of the JFHQ-DODIN orders until after [redacted] to JFHQ-DODIN that they had no ICS VPNs. Although [redacted] officials at [redacted] independently learned of the JFHQ-DODIN orders, they also did not [redacted] the ICS VPNs on [redacted] because the VPNs were listed as Juniper devices instead of Ivanti devices in its inventory records.

~~(CUI)~~ [redacted] continued to use the ICS VPNs until JFHQ DODIN [redacted]. Once JFHQ DODIN [redacted] ICS VPNs, [redacted] requested, and JFHQ-DODIN officials approved, a plan of action and milestones (POA&M) that allowed [redacted] to continue using ICS until the VPNs could be replaced. However, [redacted] did not comply with all the mitigation requirements stated in the POA&M, including [redacted]. This occurred because neither JFHQ-DODIN, as the POA&M approver, nor [redacted], had a process in place for ensuring that [redacted] complied with the required mitigations.

~~(CUI)~~ [redacted] continued use of the ICS VPNs put DoD networks at a greater risk of compromise. Historically, malicious actors have used unsecured endpoints to gain unauthorized access to a network to extract data, install malicious software, or establish backdoors for future use.

(U) Results in Brief

(U) Audit of the DoD's Actions to Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

(U) Finding (cont'd)

~~(CUI)~~ [redacted] therefore, we are not making a recommendation to [redacted] to address the [redacted] devices.

(U) Recommendations

(U) We recommend that the DoD Chief Information Officer develop and implement a process requiring DoD Components to identify changes to their software, hardware, and firmware information and update their information technology inventories in a timely manner.

(U) We recommend that the JFHQ-DODIN Commander revise the process for developing orders to include a requirement to list all current, previous, and alternate names of hardware and software in the orders to the greatest extent possible and develop and implement a process to ensure that actions agreed to in POA&Ms are performed by the Component and to hold the DAO accountable for the Component's noncompliance with the POA&M. We also recommend that the JFHQ-DODIN Commander identify opportunities to make the orders process more effective and efficient and revise the process accordingly.

(U) Management Comments and Our Response

(U) The DoD Chief Information Officer provided comments on the recommendation too late to include them in the final report; therefore, the recommendation is unresolved. If the DoD Chief Information Officer does not submit additional comments, we will consider those comments as the management response to the final report.

(U) The JFHQ-DODIN Director of Operations, responding for the JFHQ-DODIN Commander, agreed with but only partially addressed one recommendation; therefore, the recommendation is unresolved. We request additional comments on the recommendation within 30 days. The Director agreed with and provided planned actions to address two recommendations; therefore, these recommendations are resolved, and open. We will close the recommendations once we verify that management has implemented the corrective actions. Please see the Recommendations Table on the next page for the status of recommendations.

(U) Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief Information Officer, Department of Defense	1	None	None
Commander, Joint Force Headquarters–Department of Defense Information Network	2.a	2.b, 2.c	None **(U)**

(U) Please provide Management Comments by July 7, 2025.

(U) Note: The following categories are used to describe agency management's comments to individual recommendations.

- **(U) Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **(U) Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **(U) Closed** – The DoD OIG verified that the agreed upon corrective actions were implemented.

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

June 4, 2025

MEMORANDUM FOR CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE
COMMANDER, JOINT FORCE HEADQUARTERS–DOD INFORMATION NETWORK

SUBJECT: (U) Audit of the DoD's Actions to Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities (Report No. DODIG-2025-108)

(U) This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) This report contains two recommendations that we consider unresolved. The DoD Chief Information Officer provided a response to the report too late to be included. We will review the comments to determine whether they addressed the recommendation. The Joint Force Headquarters–DoD Information Network Commander did not address the specifics of one recommendation. Therefore, the recommendations remain open. We will track the recommendations until management has agreed to take action that we determine to be sufficient to meet the intent of the recommendations and management officials submit adequate documentation showing that all agreed-upon actions are completed.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. Please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. Send your responses to either [redacted] if unclassified or [redacted] if classified SECRET.

(U) This report contains two recommendations that we consider resolved and open. We will close the recommendations when the Joint Force Headquarters–DoD Information Network Commander provides documentation showing that all agreed-upon actions to implement the recommendations are completed. Please provide us within 90 days your response concerning specific actions in process or completed on the recommendations. Send your response to either [redacted] if unclassified or [redacted] if classified SECRET.

(U) We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact me at [redacted]

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

(U) Contents

(U) Introduction

~~(CUI)~~ Finding. The DAOs Generally Complied with Ivanti-Related JFHQ-DODIN Orders but [redacted] Did Not

(U) Appendixes

(U) Management Comments

(U) Acronyms and Abbreviations

(U) Glossary

(U) Introduction

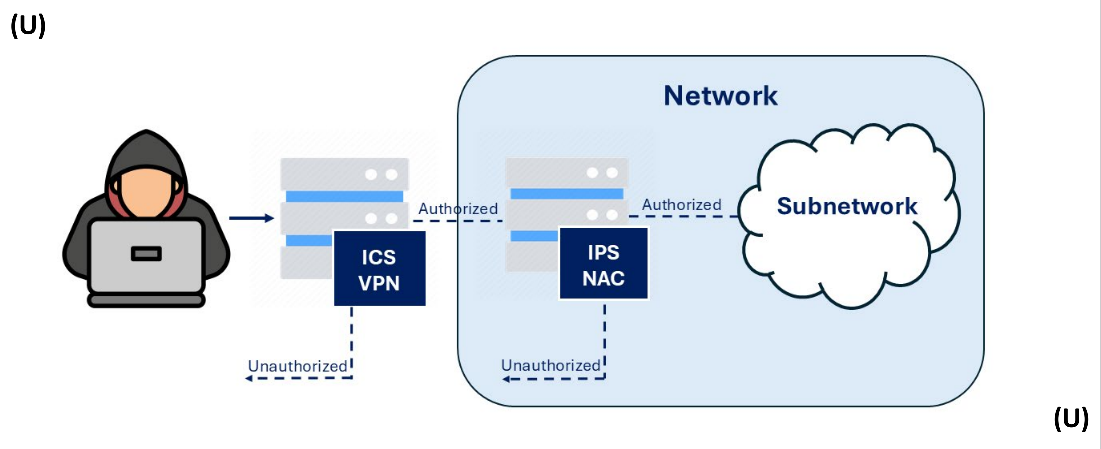
(U) Objective

(U) The objective of this audit was to determine whether the actions taken by DoD Components to identify, respond to, and mitigate vulnerabilities impacting Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) complied with DoD requirements.[1] See Appendix A for a discussion on the scope, methodology, and prior coverage related to the audit objective and the Glossary for a definition of technical terms.

(U) Background

(U) Ivanti, Inc. provides information technology management and software solutions, including virtual private network (VPN) systems, such as ICS, which allow users to remotely connect to a network over the Internet through a secure tunnel. IPS is a network access control (NAC) solution composed of hardware and software that is designed to provide network access to only authorized users and devices. Figure 1 illustrates a user attempting to access a network through an ICS VPN and IPS NAC.[2] In this example, the ICS VPN authenticates the user and authorizes or rejects access to the network. Once inside the network, the IPS NAC authenticates the user and their device and authorizes or rejects access to subnetworks and other resources.[3]

(U) Figure 1. Accessing a Network Through an ICS VPN and IPS NAC



(U) Source: The DoD OIG.

[1] (U) This report contains information that has been redacted because either the Department of Defense or Department of Homeland Security identified it as Controlled Unclassified Information that is not releasable to the public. Controlled Unclassified Information is Government-created or owned unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies.

[2] (U) Although the figure shows a possible setup using ICS and IPS, both devices are not required to be used together to grant network access to authorized users and devices.

[3] (U) A subnetwork is a logical subdivision of a network, creating a network within a network.

(U) Between January 10, 2024, and February 8, 2024, Ivanti disclosed five common vulnerabilities and exposures (CVEs) affecting ICS and IPS.[4] CVEs are a standard way of identifying, defining, and cataloging publicly disclosed cybersecurity vulnerabilities. CVEs are published on the CVE.org website and available for download or search as part of the CVE Program, the mission of which is to identify, define, and catalog CVEs. The CVE Program is operated by the MITRE Corporation and sponsored by the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA).

(U) On January 10, 2024, Ivanti disclosed that critically severe CVE-2023-46805 and highly severe CVE-2024-21887 were affecting ICS and IPS.[5] According to Mandiant, a U.S. cybersecurity firm, malicious actors could exploit the two CVEs to bypass authentication controls on ICS or IPS to gain unauthorized access to a victim's network. Malicious actors could then steal user credentials, corrupt files, or establish persistent, long-term access to a victim's network.

(U) After Ivanti's initial disclosure of the CVEs, Mandiant reported that attempts by malicious actors to exploit ICS and IPS vulnerabilities increased exponentially.[6] On January 31, 2024, Ivanti disclosed two additional highly severe CVEs affecting ICS and IPS (CVE-2024-21888 and CVE-2024-21893) and another highly severe CVE-2024-22024 on February 8, 2024. Mandiant reported that these CVEs could allow malicious actors to execute commands on a victim's network with elevated privileges.[7] In response to the CVEs, Ivanti published instructions for customers to follow to mitigate the ICS and IPS vulnerabilities, including running internal and external integrity checker tools, restoring the devices to factory settings, and installing vulnerability patches.[8]

~~(CUI)~~ Following Ivanti's disclosure of the CVEs, CISA issued an Emergency Directive (ED) followed by two Supplemental Directions (SDs) to all Federal civilian Executive Branch agencies to mitigate the vulnerabilities.[9] The Joint Force Headquarters–DoD Information Network (JFHQ-DODIN) issued multiple

[4] (U) Ivanti disclosed additional CVEs affecting ICS and IPS after February 2024 that were outside the scope of this audit.

[5] (U) The National Institute of Standards and Technology oversees the National Vulnerability Database that includes additional information about individual CVEs. The National Vulnerability Database uses the Common Vulnerability Scoring System to evaluate and assign each CVE a severity level—critical, high, medium, low, or none.

[6] (U) According to Ivanti, the number of threat actors attempting to exploit the vulnerabilities affecting ICS and IPS increased extremely rapidly after Ivanti's public disclosure of the vulnerabilities on January 10, 2024. Threat actors developed the ability to automate the exploitation of ICS and IPS vulnerabilities, allowing multiple attacks at a greater speed.

[7] (U) Elevated privileges allow information system users to perform system control, monitoring, administration functions, or security-relevant functions that ordinary users are not authorized to perform.

[8] (U) Internal and external integrity checkers scan and detect new or modified system files. Ivanti released four vulnerability patches for ICS and IPS between January 31 and February 14, 2024.

[9] (U) CISA directives do not apply to systems operated by the DoD or the Intelligence Community in accordance with sections 3553(d), (e)(2), (e)(3), and (h)(1)(B), title 44, United States Code.

~~(CUI)~~ orders to the DoD Information Network areas of operation (DAOs) [redacted].[10] See Table 1 for a timeline of Ivanti's disclosure of the CVEs and the Federal and DoD response.

(U) Federal and DoD Response to the ICS and IPS Vulnerabilities

(U) On January 19, 2024, CISA issued ED 24-01, which directed Federal civilian Executive Branch agencies to take immediate action to mitigate the ICS and IPS CVEs and report any indication of compromise.[11] On January 31, 2024, CISA issued SD V1, which directed affected Federal civilian agencies to disconnect ICS and IPS devices from their networks and continue threat hunting on any systems that were connected to, or recently connected to, the affected Ivanti products.[12] CISA allowed Federal civilian agencies to reconnect the Ivanti products to their networks after the agencies completed the mitigation actions. On February 9, 2024, CISA issued SD V2, which directed the Federal civilian agencies that reconnected Ivanti products to their networks to take additional mitigation actions.[13]

(U) For the DoD, the JFHQ-DODIN Director of Operations issued five Cyber Tasking Orders (CTOs), one Tasking Order (TASKORD), and three Fragmentary Orders (FRAGORDs) between January 9, 2024, and February 26, 2024, to address the ICS and IPS CVEs.[14] Table 1 is a timeline of the Ivanti CVE disclosures and the Federal and DoD response. See Appendix B for additional details about each of the JFHQ-DODIN orders.

(U) Table 1. Timeline of Ivanti CVEs and the Federal and DoD Response

~~(CUI)~~ Date	Event
January 8, 2024	Ivanti privately disclosed two CVEs to those customers most likely to be affected by the vulnerabilities, with instructions on how to determine whether their ICS or IPS devices were compromised and apply the initial mitigations.
January 9, 2024	JFHQ-DODIN issued CTO 24-010 [redacted] ~~(CUI)~~

[10] (U) There are 45 DAOs across the DODIN, which closely align with the DoD Components, that manage their assigned cyberspace.

[11] (U) CISA ED 24-01, "Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities," January 19, 2024.

[12] (U) CISA SD V1: ED 24-01, "Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities," January 31, 2024.

[13] (U) CISA SD V2: ED 24-01, "Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities," February 9, 2024.

[14] (U) JFHQ-DODIN issues CTOs to inform and instruct DAOs of necessary information and actions to protect the DODIN. A TASKORD is an order for specific tasks that are out of the ordinary and expected to be one-time requirements FRAGORDS are sequels to specific TASKORDS and can add, modify, or rescind tasks.

(U) Table 1. Timeline of Ivanti CVEs and the Federal and DoD Response (cont'd)

~~(CUI)~~ Date	Event
January 10, 2024	Ivanti publicly disclosed critically severe vulnerability CVE-2023-46805 and highly severe vulnerability CVE-2024-21887.
January 11, 2024	JFHQ-DODIN issued CTO 24-012 [redacted][1]
January 12, 2024	JFHQ-DODIN issued CTO 24-013 [redacted]
January 19, 2024	CISA issued ED 24-01 directing Federal civilian Executive Branch agencies to immediately mitigate the vulnerabilities impacting ICS and IPS.
January 24, 2024	JFHQ-DODIN issued TASKORD 24-0003, "Ivanti Zero Day," [redacted].[2]
January 30, 2024	JFHQ-DODIN issued CTO 24-031 [redacted].
January 31, 2024	Ivanti disclosed highly severe vulnerabilities CVE-2024-21888 and CVE-2024-21893.
	CISA issued SD V1 revising ED 24-01 and directing Federal civilian agencies to disconnect all ICS and IPS devices from agency networks, apply mitigations before bringing any product back into service, and continue threat hunting on any systems connected to—or recently connected to—the affected Ivanti products.
	JFHQ-DODIN issued FRAGORD 01 revising TASKORD 24-0003 and [redacted].
February 2, 2024	JFHQ-DODIN issued FRAGORD 02 revising TASKORD 24-0003 and [redacted].
February 5, 2024	JFHQ-DODIN issues CTO 24-037. Information in this CTO is classified.
February 8, 2024	Ivanti disclosed highly severe vulnerability CVE-2024-22024.
February 9, 2024	CISA issued SD V2 revising ED 24-01 and directing Federal civilian agencies to apply additional mitigations to any ICS and IPS devices and continue threat hunting on any systems connected to—or recently connected to—the affected Ivanti products.
February 26, 2024	JFHQ-DODIN issued FRAGORD 03, revising TASKORD 24-0003 and [redacted] ~~(CUI)~~

[1] (U) YARA is an acronym for Yet Another Recursive Acronym. It is an open-source software tool that uses malware detection patterns, called YARA rules, to identify and detect malicious software on networks.

[2] ~~(CUI)~~ [redacted].

(U) Source: The DoD OIG.

(U) JFHQ-DODIN issued the CTOs, TASKORD, and FRAGORDs in rapid succession and as a result, some of the new orders superseded or rescinded previously ordered tasks or made previously ordered tasks unnecessary. Figure 2 illustrates how the orders were superseded or rescinded by subsequent orders and the tasks that remained as of February 26, 2024.

(U) Figure 2. Superseded and Rescinded JFHQ-DODIN Orders and the Remaining Tasks

~~(CUI)~~

[redacted]

~~(CUI)~~

(U) Source: The DoD OIG.

~~(CUI)~~ As of February 26, 2024, four tasks had not been superseded, rescinded, or made unnecessary. For two of those tasks, JFHQ-DODIN did not require the DAOs to provide evidence of completion; therefore, during our site visits we asked the DAO officials if they completed these tasks, and the DAO officials confirmed that they had. However, because the ICS VPNs [redacted]:

- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted].

~~(CUI)~~ Therefore, we reviewed the two remaining tasks, which [redacted]:

- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted].

~~(CUI)~~ To determine whether the DAOs [redacted].

(U) DAOs Reviewed

~~(CUI)~~ In response to TASKORD 24-0003, [redacted]. We selected the following 8 of [redacted] DAOs for review, [redacted].[15]

1. ~~(CUI)~~ [redacted]
2. ~~(CUI)~~ [redacted]
3. ~~(CUI)~~ [redacted]
4. ~~(CUI)~~ [redacted]
5. ~~(CUI)~~ [redacted]
6. ~~(CUI)~~ [redacted]

[15] ~~(CUI)~~ [redacted]

7. ~~(CUI)~~ [redacted]
8. ~~(CUI)~~ [redacted]

~~(CUI)~~ We determined during the audit that [redacted] and the [redacted] did not have ICS or IPS devices, and the [redacted]. Therefore, we excluded those DAOs from our review. For detailed information about our selection of DAOs for review, see Appendix A.

(U) Finding

~~(CUI)~~ The DAOs Generally Complied with Ivanti-Related JFHQ-DODIN Orders but [redacted] Did Not

~~(CUI)~~ [redacted] complied with JFHQ-DODIN orders to [redacted] ICS VPNs but [redacted] did not. Specifically, [redacted] did not [redacted] ICS VPNs that were on [redacted].[16] This occurred because [redacted] relied on the results of [redacted] ICS VPNs and did not officially notify [redacted] of the JFHQ-DODIN orders until after [redacted] to JFHQ-DODIN that they had no ICS VPNs. Although [redacted] officials at [redacted] independently learned of the JFHQ-DODIN orders, they also did not [redacted] the ICS VPNs on [redacted] because the VPNs were listed as Juniper devices instead of Ivanti devices in the inventory records.[17]

~~(CUI)~~ [redacted] continued to use the ICS VPNs until JFHQ-DODIN [redacted]. Once JFHQ-DODIN [redacted] ICS VPNs, [redacted] officials requested, and JFHQ-DODIN officials approved, a plan of action and milestones (POA&M) that allowed [redacted] to continue using the ICS VPNs until they could replace the devices.[18] However, [redacted] did not comply with all of the mitigation requirements as stated in the POA&M, including [redacted]. In addition, neither JFHQ-DODIN, as the POA&M approver, nor [redacted], had a process in place for ensuring that [redacted] complied with the required mitigations.

[16] ~~(CUI)~~ [redacted] [redacted] was responsible for ensuring that [redacted] complied with the JFHQ-DODIN orders.

[17] ~~(CUI)~~ In 2020, Ivanti, Inc. acquired Pulse Secure, LLC, which had been doing business as Juniper Networks, Inc. until 2014. Juniper Networks, Inc. was the manufacturer of the devices when they were purchased by [redacted].

[18] (U) A POA&M is a corrective action plan that identifies tasks that need to be accomplished, the resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones.

~~(CUI)~~ [redacted] continued use of the [redacted] ICS VPNs in violation of the JFHQ-DODIN orders and POA&M mitigation requirements put the DODIN at greater risk of compromise. [redacted] devices, such as ICS VPNs, are [redacted], and vulnerabilities in those devices can be exploited by malicious actors to access the DODIN. Once inside the DODIN, those malicious actors can gain unauthorized access to other DoD networks, extract data, install malicious software, or establish backdoors.[19]

~~(CUI)~~ [redacted] Complied with JFHQ-DODIN Orders

~~(CUI)~~ [redacted] complied with the JFHQ-DODIN orders to [redacted] ICS VPNs. The JFHQ-DODIN orders [redacted].

~~(CUI)~~ To determine whether the DAOs complied with the JFHQ-DODIN orders, we verified [redacted]. Table 2 describes the number of ICS VPNs used in the [redacted], and when the DAOs complied with the tasks in JFHQ-DODIN TASKORD 24-0003 and FRAGORD 01.

(U) Table 2. JFHQ-DODIN Order Compliance Dates for DAOs Reviewed

~~(CUI)~~ [redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
			~~(CUI)~~

(U) Source: The DoD OIG.

[19] (U) A Backdoor is an undocumented way of gaining access to a computer system. Establishing a backdoor could allow continued unauthorized access to a system even after the initial breach is identified and remediated.

~~(CUI)~~ [redacted] Did Not Ensure that [redacted] ICS VPNs on [redacted]

~~(CUI)~~ [redacted] did not ensure that [redacted] ICS VPNs on the [redacted] in accordance with the JFHQ-DODIN orders.[20] [redacted] relied on the results of [redacted] ICS VPNs and did not officially notify [redacted] of the JFHQ-DODIN orders until after [redacted] JFHQ-DODIN that they had no ICS VPNs. Although [redacted] officials at [redacted] independently learned of the JFHQ-DODIN orders, they also did not [redacted] the ICS VPNs on [redacted] because the VPNs were listed as Juniper devices instead of Ivanti devices in the inventory records.

~~(CUI)~~ The [redacted] stated that at the time the JFHQ-DODIN orders were issued, [redacted] and instead relied on [redacted], such as ICS VPNs.[21] [redacted] did not identify any ICS VPNs on [redacted] networks and based on [redacted] reported to JFHQ-DODIN that they did not have any [redacted] Ivanti devices on their network.

~~(CUI)~~ Network scans can miss devices for various reasons; for example, if a device is powered off, not responsive, or incorrectly configured. Because network scans can miss devices, organizations can employ other methods, such as a review of the network inventory to ensure that all devices are identified. For [redacted] mission networks [redacted], the inventory is managed by network support personnel, but [redacted] did not distribute the JFHQ-DODIN orders to [redacted] until [redacted] after JFHQ-DODIN's [redacted] for the DAOs to [redacted] in their AO and [redacted].

~~(CUI)~~ Although the JFHQ-DODIN orders were not officially distributed to [redacted] until after the JFHQ-DODIN [redacted] independently became aware of the JFHQ-DODIN Ivanti-related orders in January 2024.[22]

[20] (U) Mission networks support operations or exercises and are not a part of the larger enterprise network, which includes the information technology infrastructure of the whole organization.

[21] ~~(CUI)~~ [redacted]

[22] ~~(CUI)~~ [redacted].

~~(CUI)~~ The Director explained that as part of their cybersecurity operations, [redacted] officials regularly reviewed JFHQ-DODIN orders for the most recent cybersecurity vulnerabilities affecting the DODIN. The Director stated that in response to the Ivanti-related orders, [redacted] officials reviewed the inventory of mission network assets, which included the network hardware, software, and firmware but did not identify any Ivanti devices. The Director stated that the ICS VPNs on [redacted] because the VPNs were listed as Juniper devices in the inventory records because at the time the devices were purchased, Juniper Networks, Inc. was the manufacturer of the devices.

~~(CUI)~~ On [redacted], JFHQ-DODIN scanned the DODIN and identified that [redacted] ICS VPNs were still in use by [redacted] the devices. JFHQ-DODIN officials [redacted] the VPNs and alerted [redacted] officials. In [redacted] began using a [redacted], so they no longer need to rely on [redacted] those types of devices on their networks. In [redacted] began distributing JFHQ-DODIN and [redacted] orders directly to the Information System Security Managers at each installation, who are responsible for ensuring compliance with the orders. Because those actions were taken during our audit, we are not making recommendations concerning scanning tools or orders distribution in this report. However, to reduce the risk that devices may not be identified if the manufacturer name has changed, we recommend that the DoD Chief Information Officer develop and implement a process requiring DoD Components to identify changes to their software, hardware, and firmware information, such as changes to manufacturer or device names, and update their information technology inventories in a timely manner. We also recommend that the JFHQ-DODIN Commander revise the process for developing orders, including a requirement to list all current, previous, and alternate names of hardware and software in the orders to the greatest extent possible.

~~(CUI)~~ JFHQ-DODIN and [redacted] Did Not Ensure that [redacted] Complied with the POA&M Allowing Temporary Use of the ICS VPNs on [redacted]

~~(CUI)~~ JFHQ-DODIN and [redacted] did not ensure that [redacted] complied with the POA&M allowing temporary use of the ICS VPN on [redacted]. When JFHQ-DODIN officials [redacted] ICS VPN [redacted]. On [redacted] administrators worked with [redacted] officials to submit an emergency exception request to JFHQ-DODIN

~~(CUI)~~ to allow [redacted] to reconnect the ICS VPNs because [redacted] provides [redacted]. JFHQ-DODIN officials approved the emergency exception on [redacted], and a POA&M on [redacted], that allowed [redacted] to continue using the ICS VPNs until they could be replaced.[23] The POA&M included actions that [redacted] officials stated that they had already taken to mitigate the cybersecurity risk to the DODIN of using the ICS VPNs, including resetting the device to factory settings and applying the latest patches in accordance with the Ivanti Playbook.[24]

~~(CUI)~~ JFHQ-DODIN and [redacted] did not ensure that [redacted] complied with all mitigation actions stated in the POA&M. For example, the POA&M stated that [redacted] officials planned to only [redacted] the ICS VPNs for [redacted]. According to JFHQ-DODIN records, [redacted] the ICS VPNs was [redacted]. Table 3 identifies the dates the ICS VPNs were [redacted].

~~(CUI)~~ *Table 3. ICS VPN Use and* [redacted]

[redacted]

(U) LEGEND

[redacted]

[redacted]

(U) Source: The DoD OIG.

[23] ~~(CUI)~~ [redacted] officials confirmed that the ICS VPNs were replaced [redacted]

[24] (U) JFHQ-DODIN developed the "JFHQ-DODIN Ivanti Secure Playbook" with information from CISA and the National Security Agency that included instructions for running internal and external integrity checkers, resetting the devices to factory defaults, installing the mitigation patches, and how to identify evidence of compromise on the devices or malicious activity on the network.

~~(CUI)~~ [redacted] officials explained that after the POA&M was approved, they realized that [redacted] access to [redacted] was greater than they initially understood and allowed the ICS VPNs to remain connected for longer periods of time than described in the POA&M. [redacted] officials also stated that [redacted], and that instead of [redacted] the devices, they would leave the ICS VPNs connected until [redacted]. However, the POA&M was not updated [redacted].

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted].[25] [redacted] Therefore, in signing the POA&M, [redacted] accepted the risk of [redacted] continued use of the ICS VPNs and should have monitored [redacted] compliance with the POA&M.[26]

~~(CUI)~~ [redacted] officials stated that their only role was the “middle man” between JFHQ DODIN and [redacted] DAO and, therefore, they were not responsible for ensuring that [redacted] complied with the POA&M. [redacted] officials stated that they assumed JFHQ-DODIN was monitoring the VPNs. Despite having the tools and data to know when [redacted] ICS VPNs, JFHQ-DODIN did not have a process to oversee that the actions taken by [redacted] were in accordance with the approved POA&M or to hold [redacted] accountable for noncompliance. Therefore, we recommend that the JFHQ-DODIN Commander develop and implement a process to ensure that DoD Components take all actions agreed to in POA&Ms and to hold the respective DoD Component and the DAO accountable if the DoD Component does not comply with the agreed actions.

[25] ~~(CUI)~~ [redacted]

[26] (U) JFHQ-DODIN’s online POA&M submission form warns the DAO “by signing you confirm that your organization has accepted risks associated to this POAM [sic].”

~~(CUI)~~ [redacted] Continued Use of the ICS VPNs Put [redacted] and DODIN at Greater Risk of Compromise

~~(CUI)~~ [redacted] continued use of the ICS VPNs put DoD networks at a greater risk of compromise. Historically, malicious actors have used unsecured endpoints to gain unauthorized access to a network to extract data, install malicious software, or establish backdoors for future use. If [redacted] had been compromised, malicious actors potentially could have [redacted].

(U) The continued use of the ICS VPNs also put the DODIN at greater risk of compromise. According to Mandiant, malicious actors that exploited the CVEs affecting ICS and IPS on non-DoD networks were able to bypass multifactor authentication, move laterally onto connected networks, access and steal non-public data, and establish backdoors on the networks. Additionally, malicious actors could harvest credentials or other sensitive data stored on ICS and IPS, such as user passwords, certificates, and administrator credentials, to access configuration files or management interfaces and easily compromise an entire network.

~~(CUI)~~ CISA officials confirmed that [redacted]. From the DAOs we reviewed, [redacted] found indicators of potential compromise; however, those devices were taken offline from the networks. The DoD continues to monitor its networks for anomalous activities, and DAOs are required to notify JFHQ-DODIN through [redacted].

(U) Other Matters of Interest

~~(CUI)~~ During the audit, multiple DAOs reported that the Ivanti TASKORD and FRAGORDs were hard to immediately act on because JFHQ-DODIN used inconsistent language to identify the Ivanti products that required action, did not ensure that the orders were machine-readable, and distributed the orders on a classified network even though the information was not classified.[27] For example, the JFHQ-DODIN orders interchangeably used the name of two different Ivanti products and included contradictory information about whether the orders applied to [redacted] [redacted] devices. The Ivanti TASKORD directed the DAOs to [redacted]

[27] (U) Machine readable refers to information or data that is in a format, typically XML or CSV, that can be easily processed by a computer without human intervention while ensuring that no meaning is lost. The attachments to the CTOs are often PDFs, a format that is not designed for machine readability.

~~(CUI)~~ [redacted] but the next order, FRAGORD 01, used the term [redacted][28]

~~(CUI)~~ Officials from the DAOs stated that they needed to request clarification from JFHQ-DODIN before executing the tasks because the inconsistencies in the language created uncertainty. According to the JFHQ-DODIN Deputy Chief of Current Operations, JFHQ-DODIN intended for the DAOs to [redacted]. The Deputy Chief of Current Operations stated that JFHQ-DODIN officials relayed their intent to the DAOs verbally [redacted].[29] However, JFHQ-DODIN did not clearly and formally state this intent in the TASKORD or subsequent FRAGORDs.

(U) In addition, the CTOs included important information, such as lists of malicious Internet Protocol addresses to be blocked, YARA rules, and indicators of compromise, within the orders or as attachments. The DAOs had to manually enter the information into their systems because these documents were not machine-readable, which increased the response time and the potential for input error. Finally, JFHQ-DODIN distributed the TASKORD and FRAGORDs on the Secret Internet Protocol Router Network even though they could have been distributed on the Non-classified Internet Protocol Router Network because the documents were marked Controlled Unclassified Information (CUI) and did not contain any classified information.

(U) DAO officials stated that it took time and resources to transfer the orders to the Non-classified Internet Protocol Router Network before they could distribute them to all the DAO subcomponents, which would have delayed the immediate response required by the orders.[30] Therefore, we recommend that the JFHQ-DODIN Commander review the process for developing and distributing orders and responding to DAO questions, identify opportunities to make the process more effective and efficient, and revise the process accordingly.

[28] (U) Ivanti Pulse Secure is the software component of ICS. It is also known as Ivanti Secure Access Client and was formerly named Pulse Secure Client.

[29] ~~(CUI)~~ JFHQ-DODIN holds [redacted].

[30] (U) DAO officials stated that some subcomponents do not have ready access to the Secret Internet Protocol Router Network.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the DoD Chief Information Officer develop and implement a process requiring DoD Components to identify changes to their software, hardware, and firmware information, such as changes to manufacturer or device names, and update their information technology inventories in a timely manner.

(U) Management Comments Received Late

(U) We received DoD Chief Information Officer comments on the draft report too late to include them in the final report. Therefore, the recommendation is unresolved. If the DoD Chief Information Officer does not submit additional comments, we will consider those comments as the management response to the final report.

(U) Recommendation 2

(U) We recommend that the Commander, Joint Force Headquarters–DoD Information Network:

a. **(U) Revise the process for developing orders, including a requirement to list all current, previous, and alternate names of hardware and software in the orders to the greatest extent possible.**

(U) Joint Force Headquarters Comments

(U) The JFHQ-DODIN Director of Operations, responding for the JFHQ-DODIN Commander, agreed stating that JFHQ-DODIN attempted to provide all relevant information in its orders, while also distributing the orders quickly to counter ongoing cyber activity. The Director also stated that JFHQ-DODIN would continue to improve the order process as new tools and capabilities provide better insight into DODIN technologies.

(U) Our Response

(U) Comments from the Director partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. We acknowledge that JFHQ-DODIN must balance the need to quickly issue orders with the desire to include more detailed information in the orders. However, including the alternative names in the orders will improve the likelihood that the DAOs will identify the products and mitigate the vulnerabilities. JFHQ-DODIN is in the best position during a cybersecurity incident to obtain the alternate names of the

(U) affected products when JFHQ-DODIN officials are in contact with the vendors of affected software and hardware. Therefore, we request that the Director provide additional comments within 30 days of the final report that include actions to address the recommendation.

b. **(U) Develop and implement a process to ensure that DoD Components take all actions agreed to in plans of actions and milestones and to hold the respective DoD Component and Department of Defense Information Network area of operations accountable if the DoD Component does not comply with the agreed actions.**

(U) Joint Force Headquarters Comments

(U) The JFHQ-DODIN Director of Operations, responding for the JFHQ-DODIN Commander, agreed stating that JFHQ-DODIN should be able to monitor the completion of POA&Ms and hold organizations accountable when they fail to comply. The Director stated that JFHQ-DODIN had limited tools and personnel to actively monitor POA&M compliance and must rely on the DAO Commander or Director to exercise oversight of their DAO. The Director also stated that JFHQ-DODIN planned to implement more robust compliance monitoring and oversight of POA&Ms when it is elevated to a subordinate unified command under the U.S. Cyber Command.

(U) Our Response

(U) Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved and open. We will close the recommendation once the Director provides documentation verifying that JFHQ-DODIN developed and implemented a process to monitor the completion of actions agreed to in POA&Ms and hold organizations accountable when they fail to comply.

c. **(U) Review the process for developing and distributing orders and responding to questions from the DoD Information Network Areas of Operation, identify opportunities to make the process more effective and efficient, and revise the process accordingly.**

(U) Joint Force Headquarters Comments

(U) The JFHQ-DODIN Director of Operations, responding for the JFHQ-DODIN Commander, agreed, stating that JFHQ-DODIN issued orders on the Secret Internet Protocol Router Network to prevent DAOs from having to monitor three networks for the orders. The Director also stated that JFHQ-DODIN officials were seeking

(U) additional resources to facilitate the implementation, issuance, monitoring, and other support for orders across all classifications when JFHQ-DODIN is elevated to a subordinate unified command under the U.S. Cyber Command.

(U) Our Response

(U) Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved and open. We will close the recommendation when the Director provides documentation showing that JFHQ-DODIN reviewed and revised the orders process.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from March 2024 through May 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) This report was reviewed by the DoD Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. In preparing and marking this report, we considered any comments submitted by the DoD Components about the CUI treatment of their information. If the DoD Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

(U) To answer our audit objective and determine whether the actions taken by DoD Components complied with the DoD requirements related to the ICS and IPS vulnerabilities, we reviewed documentation from eight DAOs detailing the actions taken to identify, respond to, and mitigate vulnerabilities. We interviewed officials from CISA, JFHQ-DODIN, and the National Security Agency to understand the vulnerabilities affecting the ICS and IPS devices and the vulnerability mitigation processes implemented by the U.S. Government and DoD. We reviewed multiple CISA, JFHQ-DODIN, and National Security Agency Ivanti mitigation orders.

(U) In addition, we interviewed DoD officials from the DAOs to understand how they responded to and mitigated the vulnerabilities affecting ICS and IPS. We assessed the information the DAOs provided to determine whether their responses to the vulnerabilities affecting ICS and IPS complied with DoD requirements. Specifically, we met and interviewed officials from the following DAOs.

- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]

- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]

(U) We reviewed and analyzed the following DoD and JFHQ-DODIN policies and procedures and JFHQ-DODIN orders.

- (U) DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022
- (U) DoD Manual 8530.01, "DoD Cybersecurity Activities Support Procedures," May 31, 2023
- (U) DoD Instruction 8531.01, "DoD Vulnerability Management," September 15, 2020
- ~~(CUI)~~ [redacted]
- (U) JFHQ-DODIN TASKORD 24-0003, "Ivanti Zero Day," January 24, 2024
- (U) JFHQ-DODIN FRAGORD 01 to TASKORD 24-0003, "Ivanti Zero Day," January 31, 2024
- (U) JFHQ-DODIN FRAGORD 02 TO TASKORD 24-0003, "Ivanti Zero Day," February 2, 2024
- (U) JFHQ-DODIN FRAGORD 03 TO TASKORD 24-0003, "Ivanti Zero Day," February 26, 2024
- (U) JFHQ-DODIN CTO 24-010, January 9, 2024
- (U) JFHQ-DODIN CTO 24-012, January 11, 2024
- (U) JFHQ-DODIN CTO 24-013, January 12, 2024
- (U) JFHQ-DODIN CTO 24-031, January 30, 2024

(U) Selection of DAOs for Review

(~~CUI~~) JFHQ-DODIN divides the DODIN into 45 DAOs. TASKORD 24-0003 required the DAOs to [redacted]. We obtained and reviewed the [redacted], reports from JFHQ-DODIN's scans of the DODIN for ICS and IPS on January 10, 2024, and information from interviews with JFHQ-DODIN to determine our scope of [redacted] DAOs from the total number of 45 DAOs. We included DAOs in our scope if the DAO [redacted], the JFHQ-DODIN scans of the DODIN reported the [redacted], or the JFHQ-DODIN officials informed us of [redacted] [redacted].

~~(CUI)~~ We selected 8 of [redacted] DAOs for review. We included [redacted] and [redacted] in our selection because JFHQ-DODIN officials reported that [redacted] were continuing to use their ICS VPNs. We then selected [redacted] of the remaining [redacted] for review.

~~(CUI)~~ After the selection of the DAOs for review, we excluded [redacted] from further review because we confirmed that neither DAO used or owned any ICS or IPS devices and reported using other Ivanti devices outside of our scope. We also excluded [redacted] from further review because [redacted] identified ICS VPNs on its network, but the devices were not [redacted] and therefore were not subject to the JFHQ-DODIN orders. Table 4 lists [redacted] DAOs that reported having Ivanti products and our selection of 8 DAOs for review.

(U) Table 4. Selection of DAOs for Review

~~(CUI)~~ DAOs	[redacted]	[redacted]
U.S. Air Force Cyber Command	[redacted]	[redacted]
U.S. Army Cyber Command	[redacted]	[redacted]
U.S. Coast Guard Cyber Command	[redacted]	[redacted]
Defense Advanced Research Projects Agency	[redacted]	[redacted]
Department of Defense Cyber Crime Center	[redacted]	[redacted]
Defense Contract Audit Agency	[redacted]	[redacted]
Defense Contract Management Agency	[redacted]	[redacted]
Defense Counterintelligence and Security Agency	[redacted]	[redacted]
Defense Commissary Agency	[redacted]	[redacted]
Defense Finance and Accounting Service	[redacted]	[redacted]
Defense Health Agency	[redacted]	[redacted]
Defense Human Resources Activity	[redacted]	[redacted]
Defense Intelligence Agency	[redacted]	[redacted]
Defense Information Systems Agency	[redacted]	[redacted]
Defense Logistics Agency	[redacted]	[redacted]
Defense Legal Services Agency	[redacted]	[redacted]
Defense Media Activity	[redacted]	[redacted]
Department of Defense Education Activity	[redacted]	[redacted]
Defense Prisoners of War/Missing in Action Accounting Agency	[redacted]	[redacted]
Defense Security Cooperation Agency	[redacted]	[redacted]

~~(CUI)~~

(U) Table 4. Selection of DAOs for Review (cont'd)

~~(CUI)~~ DAOs	[redacted]	[redacted]
Defense Technical Information Center	[redacted]	[redacted]
Defense Threat Reduction Agency	[redacted]	[redacted]
Defense Technology Security Agency	[redacted]	[redacted]
U.S. Fleet Cyber Command	[redacted]	[redacted]
High Performance Computing Modernization Program	[redacted]	[redacted]
Irregular Warfare Technical Support Directorate	[redacted]	[redacted]
Joint Staff	[redacted]	[redacted]
U.S. Marine Corps Forces Cyberspace Command	[redacted]	[redacted]
Missile Defense Agency	[redacted]	[redacted]
National Geospatial-Intelligence Agency	[redacted]	[redacted]
National Reconnaissance Office	[redacted]	[redacted]
National Security Agency	[redacted]	[redacted]
Office of Local Defense Community Cooperation	[redacted]	[redacted]
Pentagon Force Protection Agency	[redacted]	[redacted]
Test Resource Management Center	[redacted]	[redacted]
U.S. Africa Command	[redacted]	[redacted]
U.S. Central Command	[redacted]	[redacted]
U.S. Cyber Command	[redacted]	[redacted]
U.S. European Command	[redacted]	[redacted]
U.S. Indo-Pacific Command	[redacted]	[redacted]
U.S. Northern Command	[redacted]	[redacted]
U.S. Special Operations Command	[redacted]	[redacted]
U.S. Southern Command	[redacted]	[redacted]
U.S. Space Command	[redacted]	[redacted]
U.S. Strategic Command	[redacted]	[redacted]
U.S. Transportation Command	[redacted]	[redacted]
Washington Headquarters Services	[redacted]	[redacted] ~~(CUI)~~

(U) Source: The DoD OIG.

(U) Internal Control Assessment and Compliance

(U) We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. Specifically, we assessed whether the DAOs' actions to identify, respond to, and mitigate vulnerabilities were executed in accordance with DoD orders. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

(U) Use of Computer-Processed Data

~~(CUI)~~ We used computer-processed data to perform this audit. Sources of computer-processed data included reports of JFHQ-DODIN's network scans identifying network assets connected to the DODIN. To test the reliability of the data, we asked for printouts showing when [redacted] ICS VPNs were [redacted] [redacted] from the network, and we verified the data were reliable for the purposes of our audit by having JFHQ-DODIN officials demonstrate the scanning process, which produced identical results.

(U) Use of Technical Assistance

(U) The DoD OIG Quantitative Methods Division provided assistance in selecting the DAOs for review.

(U) Prior Coverage

(U) During the last 5 years, the DoD Office of Inspector General (DoD OIG) and the Government Accountability Office (GAO) issued three reports discussing Ivanti products and services, VPN vulnerabilities, or cyber incident response. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/. Unrestricted GAO reports can be accessed at http://www.gao.gov.

(U) DoD OIG

(U) Report No. DODIG-2022-125, "Audit of DoD Components' Response to the SolarWinds Orion Compromise," September 1, 2022

~~(CUI)~~ The DoD OIG determined the actions taken by the DoD to identify, respond to, and mitigate any compromise to DoD networks and systems that resulted from its use of SolarWinds Orion software. [redacted]

(U) GAO

(U) Report No. GAO-24-105658, "Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirement," December 4, 2023

(U) The GAO conducted a review to describe the capabilities agencies use to prepare for and respond to cybersecurity incidents, evaluate the extent to which agencies have made progress in preparing for cybersecurity incident response, and describe the challenges agencies face in preparing for incident response and the efforts to address them. There were no recommendations for the DoD in this report.

(U) Report No. GAO-23-105084, "DOD Cybersecurity Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared," November 14, 2022

(U) The GAO analyzed how the DoD has established and implemented processes to report and notify leadership of cyber incidents that affect DoD information networks, reported and shared information about selected defense industrial base cyber incidents, and has experienced data breaches of personal identifiable information and established and implemented a process to notify affected individuals of the breach. The GAO made six recommendations; however, none of the recommendations were related to the audit.

(U) Appendix B

(U) Summary of JFHQ-DODIN Orders

- ~~(CUI)~~ CTO 24-010, issued on January 9, 2024, [redacted].[31] [redacted].
- ~~(CUI)~~ CTO 24-012, issued on January 11, 2024, [redacted].
- ~~(CUI)~~ CTO 24-013, issued on January 12, 2024, [redacted].
- ~~(CUI)~~ TASKORD 24-0003, "Ivanti Zero Day," issued on January 24, 2024, [redacted]:
    - ~~(CUI)~~ [redacted];
    - ~~(CUI)~~ [redacted];
    - ~~(CUI)~~ [redacted]
    - ~~(CUI)~~ [redacted];[32] and
    - ~~(CUI)~~ [redacted].
- ~~(CUI)~~ CTO 24-031, issued on January 30, 2024, [redacted].
- ~~(CUI)~~ TASKORD 24-0003 FRAGORD 01, issued on January 31, 2024, [redacted].

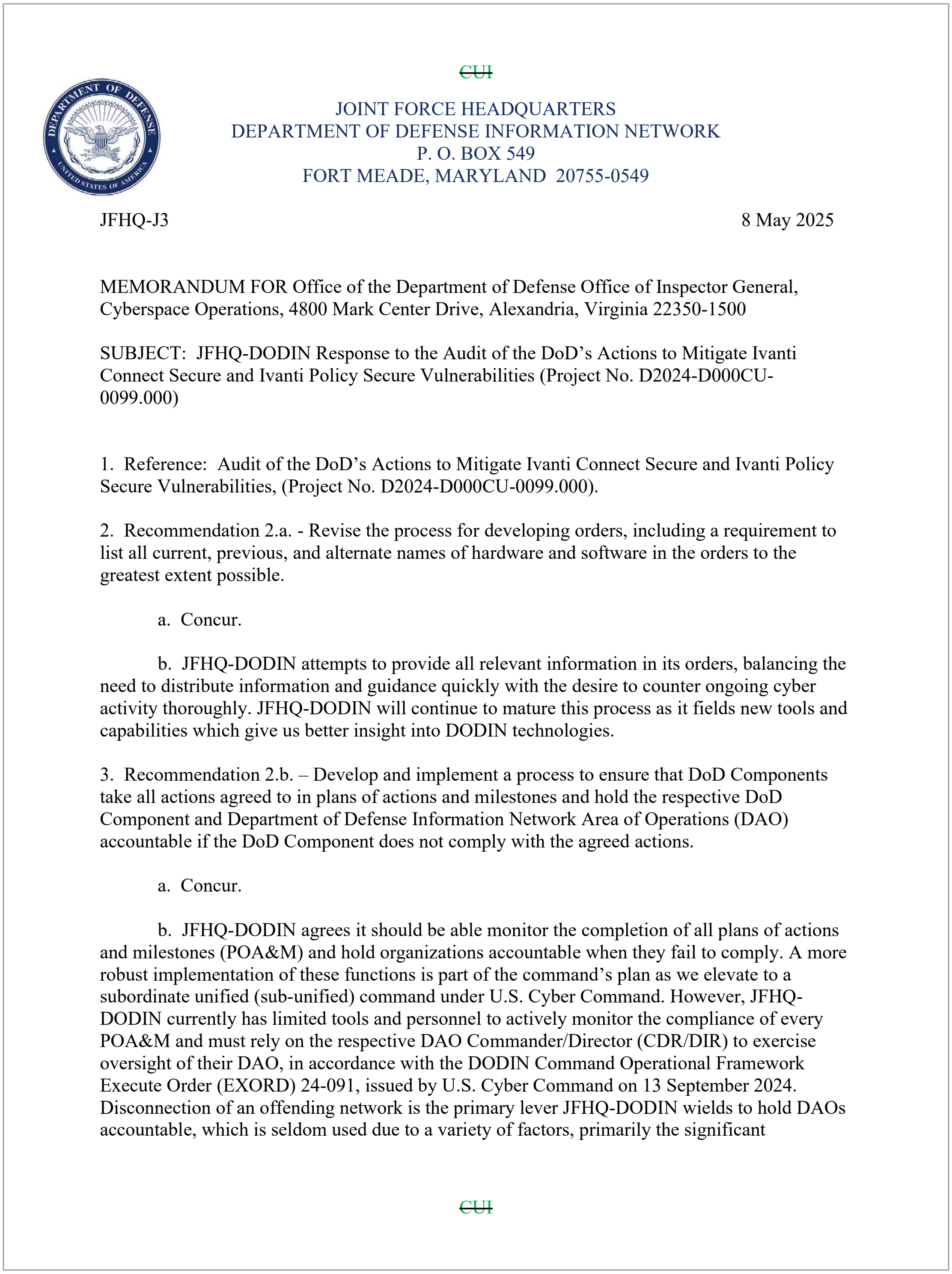
[31] (U) Ivanti, Inc., "Ivanti Connect Secure (ICS): CVE-2023-46085 & CVE-2024-21887 – Triage Guidance," January 8, 2024, (correct CVE number is CVE-2023-46805).

[32] (U) DoD Manual 8530.01, "Cybersecurity Activities Support Procedures," May 31, 2023, requires the DoD Components to designate a CSSP to direct and manage network operations and cybersecurity activities. JFHQ-DODIN directed DAOs to ensure that the ICS VPNs were included as part of the network operations managed by the CSSPs. At the time of the audit, the DoD had 26 authorized CSSPs, including the Navy Cyber Defense Operations Command and U.S. Army Cyber Command. As of February 2025, the DoD has 29 authorized CSSPs.

- ~~(CUI)~~ TASKORD 24-0003 FRAGORD 02, issued on February 2, 2024, [redacted].
- (U) CTO 24-037, issued on February 5, 2024. Information in this CTO is classified.
- ~~(CUI)~~ TASKORD 24-0003 FRAGORD 03, issued on February 26, 2024, [redacted].

(U) Management Comments

(U) Joint Force Headquarters–DoD Information Network



~~CUI~~

JOINT FORCE HEADQUARTERS
DEPARTMENT OF DEFENSE INFORMATION NETWORK
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

JFHQ-J3 8 May 2025

MEMORANDUM FOR Office of the Department of Defense Office of Inspector General, Cyberspace Operations, 4800 Mark Center Drive, Alexandria, Virginia 22350-1500

SUBJECT: JFHQ-DODIN Response to the Audit of the DoD's Actions to Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities (Project No. D2024-D000CU-0099.000)

1. Reference: Audit of the DoD's Actions to Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities, (Project No. D2024-D000CU-0099.000).

2. Recommendation 2.a. - Revise the process for developing orders, including a requirement to list all current, previous, and alternate names of hardware and software in the orders to the greatest extent possible.

a. Concur.

b. JFHQ-DODIN attempts to provide all relevant information in its orders, balancing the need to distribute information and guidance quickly with the desire to counter ongoing cyber activity thoroughly. JFHQ-DODIN will continue to mature this process as it fields new tools and capabilities which give us better insight into DODIN technologies.

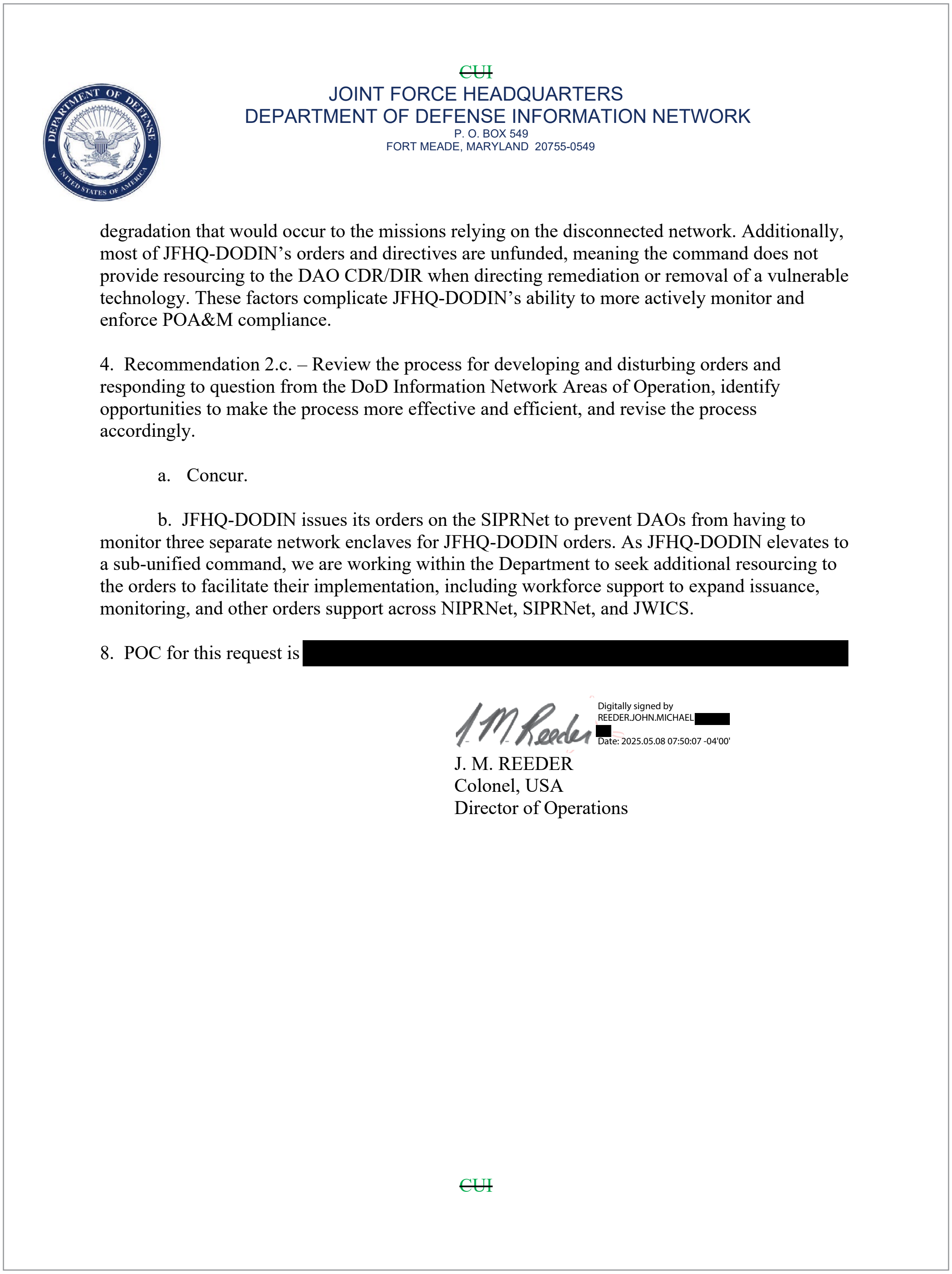
3. Recommendation 2.b. – Develop and implement a process to ensure that DoD Components take all actions agreed to in plans of actions and milestones and hold the respective DoD Component and Department of Defense Information Network Area of Operations (DAO) accountable if the DoD Component does not comply with the agreed actions.

a. Concur.

b. JFHQ-DODIN agrees it should be able monitor the completion of all plans of actions and milestones (POA&M) and hold organizations accountable when they fail to comply. A more robust implementation of these functions is part of the command's plan as we elevate to a subordinate unified (sub-unified) command under U.S. Cyber Command. However, JFHQ-DODIN currently has limited tools and personnel to actively monitor the compliance of every POA&M and must rely on the respective DAO Commander/Director (CDR/DIR) to exercise oversight of their DAO, in accordance with the DODIN Command Operational Framework Execute Order (EXORD) 24-091, issued by U.S. Cyber Command on 13 September 2024. Disconnection of an offending network is the primary lever JFHQ-DODIN wields to hold DAOs accountable, which is seldom used due to a variety of factors, primarily the significant

~~CUI~~

(U) Joint Force Headquarters–DoD Information Network (cont'd)



~~CUI~~

JOINT FORCE HEADQUARTERS
DEPARTMENT OF DEFENSE INFORMATION NETWORK
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

degradation that would occur to the missions relying on the disconnected network. Additionally, most of JFHQ-DODIN's orders and directives are unfunded, meaning the command does not provide resourcing to the DAO CDR/DIR when directing remediation or removal of a vulnerable technology. These factors complicate JFHQ-DODIN's ability to more actively monitor and enforce POA&M compliance.

4. Recommendation 2.c. – Review the process for developing and disturbing orders and responding to question from the DoD Information Network Areas of Operation, identify opportunities to make the process more effective and efficient, and revise the process accordingly.

a. Concur.

b. JFHQ-DODIN issues its orders on the SIPRNet to prevent DAOs from having to monitor three separate network enclaves for JFHQ-DODIN orders. As JFHQ-DODIN elevates to a sub-unified command, we are working within the Department to seek additional resourcing to the orders to facilitate their implementation, including workforce support to expand issuance, monitoring, and other orders support across NIPRNet, SIPRNet, and JWICS.

8. POC for this request is [redacted]

J M Reeder

Digitally signed by REEDER.JOHN.MICHAEL[redacted]
Date: 2025.05.08 07:50:07 -04'00'

J. M. REEDER
Colonel, USA
Director of Operations

~~CUI~~

(U) Acronyms and Abbreviations

~~(CUI)~~ [redacted]	[redacted]
(U) AO	Area of Operation
(U) CISA	Cybersecurity and Infrastructure Security Agency
(U) CSSP	Cybersecurity Service Provider
(U) CTO	Cyber Tasking Order
(U) CUI	Controlled Unclassified Information
(U) CVE	Common Vulnerabilities and Exposures
(U) DAO	DODIN Area of Operations
(U) DODIN	DoD Information Network
~~(CUI)~~ [redacted]	[redacted]
(U) ED	Emergency Directive
~~(CUI)~~ [redacted]	[redacted]
(U) FRAGORD	Fragmentary Order
~~(CUI)~~ [redacted]	[redacted]
(U) ICS	Ivanti Connect Secure
(U) IPS	Ivanti Policy Secure
(U) JFHQ-DODIN	Joint Force Headquarters–Department of Defense Information Network
~~(CUI)~~ [redacted]	[redacted]
(U) NAC	Network Access Control
(U) POA&M	Plan of Action and Milestones
~~(CUI)~~ [redacted]	[redacted]
(U) SD	Supplemental Direction
(U) TASKORD	Tasking Order
(U) VPN	Virtual Private Network
(U) YARA	Yet Another Recursive Acronym

(U) Glossary

(U) Backdoor. An undocumented way of gaining access to a computer system.

(U) Common Vulnerabilities and Exposures. A standard way to identify, define, and catalog publicly disclosed cybersecurity issues.

(U) Controlled Unclassified Information. Information created or possessed on behalf of the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and government-wide policies.

(U) Integrity Checker. A tool that scans software and detects new or modified system files.

(U) Internet Protocol Address. A unique number that identifies a device connected to the Internet that is used to send and receive data.

(U) Multifactor Authentication. An identification verification method in which a user has to provide two or more factors to prove their identity. Factors include something known to the user (for example, a personal identification number or password), something in the user's possession (for example, a cryptographic identification device or token), or a physical aspect of the user (such as biometric information).

(U) Non-Classified Internet Protocol Router Network. A network used by DoD personnel to exchange unclassified information.

(U) Plan of Action and Milestones. A document that identifies tasks that need to be accomplished, the resources required to accomplish the elements of the plan, any milestones in the meeting tasks, and scheduled completion dates for the milestones.

(U) Subnetwork. A subnetwork is a logical subdivision of a network creating a network within a network.

(U) Threat Hunting. A proactive approach to identify unknown threats on a network.

(U) Virtual Private Network. An encrypted connection over the Internet from a device to a network.

(U) Yet Another Recursive Acronym. A tool used to identify and classify malicious software.

Whistleblower Protection

U.S. Department of Defense

Whistleblower Protection safeguards DoD 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 DoD OIG reports or activities, please contact us:

Legislative Affairs Division
703.604.8324

Public Affairs Division
public.affairs@dodig.mil; 703.604.8324

www.dodig.mil

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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