Report No. DODIG-2025-126

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

JULY 18, 2025

(U) Evaluation of a Line of Effort in the DoD's Implementation of the Combined Joint All-Domain Command and Control (CJADC2) Strategy

~~Controlled by: DoD OIG~~
~~Controlled by: Evaluations Intelligence Division~~
~~CUI Category: OPSEC~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC: DoD OIG SIEO/PM~~ [redacted]

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

~~CUI~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

(U) Results in Brief

(U) Evaluation of a Line of Effort in the DoD's Implementation of the Combined Joint All-Domain Command and Control (CJADC2) Strategy

July 18, 2025

(U) Objective

(U) The objective of this evaluation was to assess the effectiveness with which the DoD developed and implemented the Combined Joint All-Domain Command and Control (CJADC2) line of effort to modernize mission partner information sharing—one of five lines of effort in the implementation plan for the CJADC2 strategy.

(U) Background

(U) CJADC2 is the DoD's concept to improve command and control across all the Military Services and with allies and partners (mission partners). The CJADC2 implementation plan calls for establishing the foundation for the use of data-centric security, an approach to information security that emphasizes protecting the data itself rather than only the underlying systems or infrastructure.

(U) Finding

~~(CUI)~~ The DoD is making progress to implement one of CJADC2's lines of effort—to modernize mission partner information sharing using data-centric security. [redacted] However, the architecture that the Air Force is developing to establish the connections between DoD commands and partner networks does not have clearly defined standards for full operational capability or minimum viable capability release.

(U) Finding (cont'd)

(U) Further complicating CJADC2 implementation was the DoD's lack of an information domain assessment framework, meaning that the DoD did not have a standard, comprehensive, and repeatable process to assess risk and authorize data-centric security for mission partner environments or networks.

~~(U//FOUO)~~ These conditions occurred because the approach outlined in the CJADC2 implementation plan may not comply with current policies and standards for information sharing with foreign partners. [redacted]

(U) The DoD continues to share classified information with allies and partners. However, the connections are separate networks, rather than one integrated network; therefore, they do not support the CJADC2 strategy's goal of systems integration where each partner's command and control system can be accessed, viewed, and acted on by every other approved partner.

(U) Recommendations

(U) We recommend that the responsible Air Force official define minimum viable capability release standards for the CJADC2 environment to better determine policy constraints and required exception processes. We also recommend that the DoD Chief Information Officer:

- (U) develop and implement an appropriate information domain assessment framework, and
- (U) develop policy that establishes data tagging and labeling standards for the mission partner environment.

(U) Results in Brief

(U) Evaluation of a Line of Effort in the DoD's Implementation of the Combined Joint All-Domain Command and Control (CJADC2) Strategy

(U) Management Actions Taken

(U) During the evaluation, the DoD Information Security Risk Management Committee approved an information domain assessment framework. Therefore, recommendation 2 is closed.

(U) Management Comments and Our Response

(U) The official Performing the Duties of the DoD Chief Information Officer and the Department of the Air Force Acting Chief Information Officer agreed with the remaining recommendations; therefore, those recommendations are resolved but will remain open. We will close those recommendations when we verify that management officials have implemented actions required to fully address the recommendations.

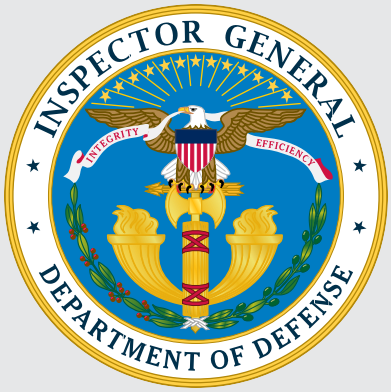
(U) Please see the Recommendations Table on the next page for the status of the recommendations.

(U) Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
DoD Chief Information Officer	None	3	2
Air Force Program Executive Officer for Cyber and Networks	None	1	None **(U)**

(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.


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

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

July 18, 2025

MEMORANDUM FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
DIRECTOR, JOINT STAFF
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

SUBJECT: (U) Evaluation of a Line of Effort in the DoD's Implementation of the Combined Joint All-Domain Command and Control (CJADC2) Strategy (Report No. DODIG-2025-126)

(U) This final report provides the results of the DoD Office of Inspector General's evaluation. 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) The DoD Chief Information Officer took action sufficient to address Recommendation 2, and we consider that recommendation closed. Additionally, the DoD Chief Information Officer and the Department of the Air Force Chief Information Officer agreed to address the remaining recommendations presented in the report; therefore, those recommendations are resolved but will remain open. We will close those recommendations when you provide us documentation showing that all agreed-upon actions to implement the recommendations are completed. Therefore, 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 evaluation. If you have any questions, please contact [redacted]

Randolph R. Stone
Assistant Inspector General for Evaluations
Space, Intelligence, Engineering, and Oversight

(U) Contents

(U) Introduction

(U) Objective

(U) The objective of this evaluation was to assess the effectiveness with which the DoD developed and implemented the Combined Joint All-Domain Command and Control (CJADC2) line of effort to modernize mission partner information sharing.[1]

(U) Background

(U) Traditionally, each Military Service developed its own command and control (C2) network that could not interface with networks of other Military Services. CJADC2 is the DoD's concept to connect sensors and networks from all the Military Services into a single network.[2] CJADC2 is a joint warfighting function enabled by technology.[3] It is not a single technology, system, or tool. CJADC2 enables the Combined Joint Force Commander's ability to command and control military forces across warfighting domains with allies and partners.

~~(CUI)~~ C2 is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.[4] [redacted][5]

~~(CUI)~~ [redacted]

[1] (U) This report contains information that has been redacted because it was identified by the DoD as Controlled Unclassified Information (CUI) that is not releasable to the public. CUI 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) In 2023, the DoD rebranded Joint All-Domain Command and Control (JADC2) as Combined—or CJADC2—to reflect a renewed emphasis on "combined" efforts with international partners, as well as different military commands. "Combined" is the DoD term for forces of two or more allies working together, while "joint" is the term for forces from two or more U.S. Military Departments working together. We use the term CJADC2 throughout this report for consistency.

[3] (U) A joint function is a grouping of capabilities and activities that enable joint force commanders to synchronize, integrate, and direct joint operations. Joint Publication 3-0, "Joint Campaigns and Operations," June 18, 2022, describes seven joint functions common to joint operations: command and control (C2), information, intelligence, fires, movement and maneuver, protection, and sustainment.

[4] (U) DoD Dictionary of Military and Associated Terms, February 2025.

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

~~(CUI)~~ [redacted]

(U) In March 2022, the Deputy Secretary of Defense issued a classified "Joint All-Domain Command and Control Strategy Implementation Plan" that established five lines of effort. The CJADC2 implementation plan calls for establishing a foundation to transition to a data-centric information environment by employing services that are data-centric capable. However, this approach may not be compliant with current policies and standards for information sharing with foreign mission partners.

(U) CJADC2 Line of Effort 5: Modernize Mission Partner Information Sharing

(U) This evaluation focused on line of effort 5: "modernize mission partner information sharing." Mission partners are "partners with which the DoD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government, State and local governments, allies, coalition members, host nations and other nations, multinational organizations, non-governmental organizations, and the private sector." A Mission Partner Environment (MPE) is the "operating framework that enables C2 and intelligence information sharing for planning and execution, as a mission partner, across the full range of military operations at a single security level with a common language. An MPE capability provides the ability for … [mission partners] to exchange information with all participants within a specific partnership or coalition."[6] For the purpose of current CJADC2 efforts and this evaluation, the mission partners are coalition armed forces, and the MPE is the network that allows the sharing of information up to the Secret level with those mission partners.

(U) According to the DoD CJADC2 strategy:

> (U) "[i]deal mission partner system integration is realized when data from each partner's [command and control] systems can be accessed, viewed, and acted [on] by every other approved partner. However, emerging missions, large coalitions, and evolving technologies present ongoing obstacles to achieving this goal. Ultimately, [CJADC2] system interoperability is foundational for conducting combined and partnered operations with speed, precision, relevance, and security.

[6] (U) DoD Directive 5101.22E, "DoD Executive Agent (DoD EA) for DoD Mission Partner Environment (MPE)," August 5, 2020.

> (U) This [line of effort] strives to broaden and improve the Joint Force's ability to exchange information and coordinate actions and effects in all types of combined operations."[7]

(U) The "modernize mission partner information sharing" line of effort has four objectives:

1. (U) Employ a robust, resilient modernized MPE capability at the Secret and below releasable classification level;
2. (U) Align capabilities to North Atlantic Treaty Organization (NATO) Federated Mission Networking spiral specifications to empower Coalition interoperability;[8]
3. (U) Incorporate information sharing capabilities through engagement with mission partners; and
4. (U) Develop command and control systems, and tactics, techniques and procedures that are compatible with mission partner capabilities.

(U) Differences Between Network-Centric Security and Data-Centric Security

(U) The DoD's CJADC2 implementation plan calls for establishing a foundation to transition to data-centric capable systems. Data-centric security focuses on protecting sensitive data itself as the primary concern, securing it throughout its lifecycle regardless of where it resides and applying security controls directly to data. Net-centric security focuses on securing the network boundaries and access points. A data-centric approach involves identifying sensitive data, tagging and classifying it based on its data type, and implementing appropriate security controls and policies to protect it to reduce the impact of data breaches.[9] Data-centric security is still maturing and zero trust principles help organizations to reduce the effect of a breach and improve their overall security posture by continuously verifying the identity of users and devices.[10] Zero trust is an enabling framework that verifies every access request, and is needed to make data-centric security possible. Data-centric security embeds protection at the individual data object level, allowing data to protect itself, rather than the traditional methods

[7] (U) DoD, "Summary of the Joint All-Domain Command and Control (JADC2) Strategy," March 2022.

[8] (U) DoD Instruction 8110.01, "Mission Partner Environment Information Sharing Capability Implementation for the DoD," June 30, 2021, states that Federated Mission Networking is a common set of standards, protocols, and interfaces that will be used to enable the sharing of DoD data, information, and information technology services in accordance with NATO specifications.

[9] (U) Data tagging or labeling is the act of associating tags as metadata to an object by identifying, labeling, and describing its information. The data tagging and labeling can support access controls, and how community of interests interact within a zero trust environment.

[10] (U) Zero trust is an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust focuses on verifying every access request, protecting data, and segmenting networks.

(U) used to protect data, which rely on the infrastructure where the data resides to protect it, often described as "network-centric" security. In a data-centric security architecture, the attributes of the data, the metadata, can be used for access-control decisions and implementing appropriate security controls and policies to protect it.[11]

(U) Supporting Roles and Responsibilities

(U) The CJADC2 Implementation Plan and other CJADC2 documents specify a variety of supporting roles and responsibilities for the DoD components.

(U) Joint Staff Directorate for Command, Control, Communications, and Computers/Cyber

(U) The Joint Staff Directorate for Command, Control, Communications, and Computers/Cyber (J-6) is the Office of Primary Responsibility for managing the objectives and tasks for the CJADC2 line of effort to modernize mission partner information sharing. The CJADC2 Strategy Implementation Plan assigned each task within an objective to Offices of Primary Responsibility, and if needed, to Offices of Coordinating Responsibility that are responsible for working on the task. The Joint Staff J-6 Coalition Interoperability Division is responsible for tracking the progress for each task and reporting the status of those tasks to the CJADC2 Cross Functional Team.[12]

(U) Secretary of the Air Force

(U) In February 2019, the Deputy Secretary of Defense designated the Secretary of the Air Force as the DoD MPE Executive Agent to update the overall portfolio of coalition command and control networks and intelligence information sharing capabilities.[13] The Secretary of the Air Force established the Mission Partner Capabilities Office to execute DoD MPE executive agent responsibilities. The Mission Partner Capabilities Office is responsible for designing, resourcing, and sustaining DoD MPE systems to provide interoperable enterprise command, control, and information sharing between the DoD and mission partners.

---

[11] (U) See DoD OIG Report No. DODIG-2025-090, "(U) Audit of the DoD's Compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust," April 29, 2025, for additional details on zero trust.

[12] (U) The CJADC2 Cross Functional Team is the venue through which capability developers discuss, identify, collaborate, and recommend opportunities to improve C2 information sharing and interoperability within the Service and warfighting domains. The CJADC2 Cross Functional Team's primary responsibility is the implementation of the DoD CJADC2 Strategy.

[13] (U) Secretary of the Air Force responsibilities are guided by DoD Directive 5101.22E, "DoD Executive Agent (DoD EA) for DoD Mission Partner Environment (MPE)," August 5, 2020, and DoD Instruction 8110.01, "Mission Partner Environment Information Sharing Capability Implementation for the DoD," June 30, 2021.

(U) The Mission Partner Capabilities Office proposed the Secret and Below Releasable Environment (SABRE) as the future enterprise solution to give combatant commands the ability to collaborate and share information with mission partners by enabling chat, email, file sharing, voice, and video teleconferencing between mission partners. SABRE is an architecture consisting of hardware and software within a data-centric, zero trust Secret releasable environment for secure and seamless collaboration, coordination, and information sharing with mission partners.[14]

(U) In May 2023, the Air Force:

- (U) realigned the DoD Executive Agent for DoD MPE responsibilities to the Secretary of the Air Force Office of the Chief Information Officer;
- (U) realigned enterprise MPE modernization and implementation responsibilities, including development of SABRE, to an office that subsequently became the Program Executive Officer for Cyber and Networks under the Office of the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics; and
- (U) retained legacy enterprise MPE capabilities sustainment with the Mission Partner Capabilities Office under the Administrative Assistant to the Secretary of the Air Force.

(U) DoD Information Security Risk Management Committee

~~(CUI)~~ The DoD Information Security Risk Management Committee (ISRMC) is responsible for ensuring that risk-related considerations for individual information systems, including authorization decisions, are viewed from a DoD-wide perspective about the overall strategic goals and objectives of the DoD in carrying out its missions and business functions.[15] The DoD ISRMC also ensures that the management of information technology-related security risks is consistent across the DoD, reflects organizational risk tolerance, and is considered along with other organizational risk in order to ensure mission or business success. [redacted]

[14] (U) The SABRE Milestone Decision Authority is the Program Executive Officer for Cyber and Networks. The Milestone Decision Authority is the individual with the authority to approve the entry of an acquisition program into the next phase of the acquisition program. SABRE is an Acquisition Category level III equivalent program, which means that it has not been designated as a "major system" by the Milestone Decision Authority; has an estimated dollar value less than $200 million in FY 2020 constant dollars for research, development, and test and evaluation; and has less than $920 million in FY 2020 constant dollars for procurement.

[15] (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (Incorporating Change 1, October 7, 2019).

~~(CUI)~~ [redacted][16]

~~(CUI)~~ The DoD ISRMC is the risk executive function responsible for accepting enterprise cybersecurity risk for the DoD. [redacted][17]

(U) DoD Chief Information Officer

(U) The DoD CIO is the Principal Staff Assistant to the Secretary of Defense for information technology and is responsible for all matters relating to the DoD information enterprise. The DoD CIO established a Risk Management Framework to establish and apply cybersecurity requirements and cyberspace operational risk management functions to all programs, systems, and technologies in the DoD, regardless of the acquisition or procurement method. The DoD CIO is a member of the CJADC2 Cross Functional Team with a principal role in reviewing and certifying that CJADC2 capabilities meet DoD standards. The DoD CIO is responsible for developing the Information Domain Assessment Framework (IDAF) for data-centric networks. The IDAF is a repeatable and scalable assessment process that provides systematic assessment criteria to support operational and technical risk evaluation and decisions for data-centric system information domains.

(U) National Security Agency Director

(U) The NSA Director is the National Manager for National Security Systems.[18] Some NSA roles and responsibilities include overseeing cross-domain activities across the U.S. Government to ensure a common approach to advising federal agency CIOs on issues related to cross-domain solutions and developing guidance and technologies to improve the security and capabilities of cross-domain solutions.

[16] (U) Department of Defense Information Security Risk Management Committee Charter, October 2024. Flag-level or Senior Executive Service (SES) personnel from within their organization represent each principal voting member at the meeting.

[17] (U) A cross-domain solution is a form of controlled interface that provides the ability to manually or automatically access and transfer information between different security domains.

[18] (U) A National Security System is any information system used or operated by an agency or a contractor of an agency, or other organization on behalf of an agency, (1) the function, operation, or use of which involves intelligence activities; cryptologic activities related to national security; C2 of military forces; equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions or (2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(U) National Security Memorandum 8 authorizes the National Manager for National Security Systems to guide and direct national security system owners through issuances, such as Emergency Directives and Binding Operational Directives (BODs).[19] A BOD is a compulsory direction to Executive Branch departments and agencies for purposes of safeguarding Federal information and information systems.

~~(U//FOUO)~~ [redacted]

- ~~(U//FOUO)~~ [redacted][20]
- ~~(U//FOUO)~~ [redacted][21] [redacted][22]

[19] (U) National Security Memorandum 8, "Memorandum on Improving the Cyber Security of National Security, Department of Defense, and Intelligence Community Systems," January 19, 2022.

[20] ~~(U//FOUO)~~ [redacted]

[21] ~~(U//FOUO)~~ [redacted]

[22] ~~(U//FOUO)~~ [redacted]

(U) Chief Digital and Artificial Intelligence Officer

~~(CUI)~~ The Chief Digital and Artificial Intelligence Officer (CDAO) is responsible for supporting CJADC2 through the continued development of data integration and developing software tools to digitize battle management. [redacted]

(U) Theater-Specific Mission Partner Environment Initiatives

(U) While SABRE is being developed, each combatant command is expected to continue to develop and sustain theater-specific MPE networks that support communication with different mission partners. The Air Force Mission Partner Capability Office is the program office for these various MPE networks. Similar to the CJADC2 SABRE initiative, some combatant commands have their own initiatives to use data-centric security to connect the different Secret-releasable level MPE security enclaves in their areas of responsibility to share information.

~~(CUI)~~ For example, the U.S. Central Command (USCENTCOM) is developing a "Collaborative Partner Environment" that it intends to use to connect the different Secret-releasable level MPE security enclaves in its area of responsibility through a single interface. [redacted] This net-centric approach to coalition information sharing limits the United States and coalition partners from rapid collaboration and information sharing.

~~(CUI)~~ Similar to USCENTCOM, the U.S. Indo-Pacific Command (USINDOPACOM) is developing a "USINDOPACOM Mission Network" that it also intends to use to connect the different Secret-releasable level mission partner security enclaves in its area of responsibility through a single interface. [redacted] Like the Air Force's SABRE, USINDOPACOM intends to use a zero trust architecture network featuring data-centric security to ensure that data is protected at the object level.[23] [redacted]

[23] (U) The DoD Office of Inspector General is also conducting an audit of cybersecurity controls over the U.S. Indo-Pacific Command Mission Partner Environment to assess the effectiveness of USINDOPACOM's cybersecurity controls over access to information in its mission partner environment (Project No. D2024-D000CS-0186.000).

~~(CUI)~~ [redacted][24]

[24] ~~(U//FOUO)~~ [redacted]

(U) Finding

(U) The DoD Is Making Progress to Implement CJADC2's Effort to Modernize Mission Partner Information Sharing by Establishing the Foundation for Data-Centric Capable Domains, but Did Not Have an Information Domain Assessment Framework

~~(CUI)~~ The DoD is making progress to implement CJADC2's line of effort to modernize mission partner information sharing by establishing the foundation for data-centric capable information domains. [redacted] The DoD selected the SABRE system, which is currently under development, as the DoD-wide enterprise solution to establish Secret-level and below connections between DoD commands and ally and partner networks. However, SABRE does not have clearly defined full operational capability or minimum viable capability release standards.

~~(U//FOUO)~~ This occurred because the CJADC2 implementation plan calls for a transition to a data-centric environment to share classified information with foreign partners. However, this approach is not compliant with current policies and standards for information sharing. [redacted]

(U) Further complicating CJADC2 implementation was the DoD's lack of an IDAF, meaning that the DoD did not have a standard, comprehensive, and repeatable process to assess risk and consider whether it is appropriate to authorize data-centric security for mission partner environments or networks.

(U) Therefore, the DoD continues to share classified information with allies and partners through multiple bilateral networks. However, these separate networks do not support CJADC2's goal of systems integration where each partner's command and control system "can be accessed, viewed, and acted upon by every other approved partner."[25]

[25] (U) DoD, "Summary of the Joint All-Domain Command and Control (JADC2) Strategy," March 2022.

(U) The DoD Is Making Progress Establishing the Foundation for Developing Data-Centric Domains to Modernize Information Sharing

~~(CUI)~~ The DoD is making progress to develop and implement CJADC2's line of effort to modernize mission partner information sharing by establishing the foundation for developing data-centric capable information domains. [redacted] [26] [redacted] [27] [redacted] However, the SABRE program does not have clearly defined FOC or minimum viable capability release standards.

(U) The combatant commands currently have numerous net-centric systems for mission partner information sharing. The Mission Partner Capabilities Office identified SABRE as the DoD's enterprise solution for the DoD, allies, and partners as part of their efforts to develop and modernize information sharing due to the stand-alone systems the combatant commands were fielding.

(U) The Combatant Commands Have Numerous Net-Centric Systems for Mission Partner Information Sharing

~~(CUI)~~ Combatant commands have numerous net-centric systems for mission partner information sharing; however, these bilateral systems do not meet the goals of CJADC2. CJADC2 has a stated goal of integrated systems where each partner's command and control system "can be accessed, viewed, and acted on by every other approved partner." [redacted]

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

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

~~(CUI)~~ [redacted] The figure is an Air Force Mission Partner Capability Office depiction of DoD Secret-Releasable level mission partner networks.

(U) Figure. DoD Secret-Releasable Level Mission Partner Environment Networks

[redacted]

(U) Source: The Air Force Mission Partner Capability Office.

(U) The DoD is developing data-centric information domains as part of an ongoing process to modernize information sharing with foreign mission partners. These efforts would allow the existing net-centric networks to be consolidated, reduce the cost of numerous bilateral systems, and have access controls that limit the information available to each partner. Therefore, the figure illustrates the importance of CJADC2's modernizing mission partner information sharing line of effort.

(U) SABRE Is the DoD's Enterprise Mission Partner Solution

~~(U//FOUO)~~ The DoD identified the SABRE network, which is under development by the Air Force, as the DoD's enterprise solution to establish Secret-level and below connections between DoD commands and partner networks. This critical task enables access to each partner's data-centric command and control data by an approved partner. [redacted]

~~(U//FOUO)~~ [redacted]

(U) However, the technology to develop data-centric information domains is outpacing the policy that governs the DoD's data-centric information sharing. Full realization of global mission partner information sharing will require continued technology and policy development.

~~(CUI)~~ [redacted] However, the Air Force Program Executive Officer for Cyber and Networks did not clearly define FOC for SABRE.[28] According to program personnel, this occurred because SABRE is software and services acquisition built around software requirements, so it will not likely have a clearly defined FOC.

~~(CUI)~~ [redacted][29] [redacted]

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

[28] (U) According to the Defense Acquisition University Glossary, a Systems Requirement Document defines the system-level functional and performance requirements for a system. It translates warfighter capability-based requirements into performance-based acquisition requirements for a system or subsystem in any program milestone or phase.

(U) According to the Defense Acquisition University Glossary, a full operational capability is attained when all units or organizations in the force structure scheduled to receive a system have received it and have the capability to employ and maintain it.

[29] (U) "Five Eyes" refers to the group of intelligence-sharing countries consisting of Australia, Canada, New Zealand, and the United Kingdom, along with the United States.

~~(CUI)~~ We observed SABRE, along with the USINDOPACOM Mission Network, in the Joint Staff–led 2024 Project Olympus coalition capability demonstration and assessment. [redacted] However, as a result of the lack of clear criteria for FOC, [redacted] we were unable to determine the extent to which the deployment of the SABRE network would be able to support the CJADC2 line of effort to modernize mission partner information sharing.

(U) Subsequent to our evaluation, the Secretary of Defense directed all DoD Components to adopt the Software Acquisition Pathway as the preferred pathway for all software development components of business and weapon system programs.[30] As a result, according to DoD CIO and SABRE program office personnel, the SABRE program is removing the terms IOC and FOC, and using the terms "minimum viable product" and "minimum viable capability release."[31]

(U) Therefore, the Air Force Program Executive Officer for Cyber and Networks should define the Secret and Below Releasable Environment minimum viable capability release standards to better determine policy constraints and the required exception processes and ensure that the system is developed in compliance with these requirements.

(U) The DoD Did Not Have an Information Domain Assessment Framework for Data-Centric Security

(U) The DoD did not have an IDAF, which means that it did not have a standard, comprehensive, and repeatable process to assess and authorize data-centric security for MPE information domains or networks. The current non-standardized approaches to reviewing data-centric network security increase operational and technical risk for the DoD and mission partners. Additionally, no DoD CIO or CDAO standards exist for tagging and labeling for MPE networks.

[30] (U) Secretary of Defense memorandum, "Directing Modern Software Acquisition to Maximize Lethality," March 6, 2025.

[31] (U) According to the Defense Acquisition University Glossary, a minimum viable product is an early version of the software to deliver or field basic capabilities to users to evaluate and provide feedback on. A minimum viable capability release is the initial set of features suitable to be fielded in an operational environment that provides value to the warfighter or end user in a rapid timeline.

(U) Lack of a Standardized Process to Review Data-Centric Security Increases Operational and Technical Risk

~~(U//FOUO)~~ DoD Directive 5144.02 requires the DoD CIO to establish cybersecurity requirements and cyberspace operational risk management functions for all information domains. The lack of a standardized process to assess risk for data-centric networks occurred because the CJADC2 implementation plan calls for a transition to data-centric information domains by employing services that are data-centric capable to share classified information with foreign partners. [redacted] As a result, operational commanders are implementing information domains using non-standard criteria and assessment parameters.

~~(CUI)~~ The non-standard approach increases operational and technical risk for the DoD and mission partners. For example, the USINDOPACOM Mission Network is a joint and multi-coalition capability providing mission partners with accessible data between the United States and partner nations. [redacted] The creation of DoD-wide enterprise-level solutions requires a standardized understanding of risk across DoD Components to inform commanders and authorizing officials to support their risk-based decisions.

(U) DoD Directive 5144.02 states that the DoD CIO is responsible for all matters relating to the DoD information enterprise, network policy, and standards. DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Systems," states that the DoD CIO establishes and applies cybersecurity requirements and cyberspace operational risk management functions to all programs, systems, and technologies in the DoD, regardless of the acquisition or procurement method.[32] The Instruction states that the DoD ISRMC performs certain enterprise-level risk acceptance determinations. In this context, if the DoD ISRMC in its risk management function accepts a risk on behalf of the DoD information enterprise, "the receiving organization may not refuse to deploy the system." However, according to a Joint Staff J-6 staff official, the DoD's existing Risk Management Framework could not effectively assess the cybersecurity of a data-centric network.

[32] (U) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Systems," July 19, 2022.

(U) In April 2024, the DoD ISRMC developed a first draft of an IDAF for data-centric security. In December 2024, the DoD ISRMC reviewed an updated draft of an IDAF for evaluating MPE information domains, and authorizing data security toward a standard, comprehensive, and repeatable process.

(U) Therefore, we recommend that the DoD Chief Information Officer develop and implement an Information Domain Assessment Framework for Mission Partner Environments. In March 2025, the DoD ISRMC approved an IDAF with the caveats that the DoD ISRMC would revisit the IDAF in six months to determine lessons learned and any necessary process changes, to include an intelligence threat assessment.[33]

(U) No DoD CIO or CDAO Standard Exists for Tagging and Labeling for Mission Partner Environment Networks

(U) In addition to the lack of an IDAF for data-centric MPEs, the DoD CIO and CDAO have not developed policies or standards for data tagging and labeling of information for MPEs.[34] DoD Directive 5144.02 states that the DoD CIO is required to establish cybersecurity requirements and cyberspace operational risk management functions for all information domains. In addition, DoD Instruction 8520.04, "Access Management for DoD Information Systems," states that the CDAO should develop policy that incorporates requirements for tagging data and data sets.[35]

(U) Although establishing the CJADC2 data enterprise is a different CJADC2 line of effort, establishing a common set of data tags for MPEs is vital to supporting mission partner information sharing.[36] For example, users who create a product that is releasable to certain foreign partners but not others must understand the data tagging standards that will allow the MPE to limit access to the product to certain allies and partners.

~~(CUI)~~ According to a Joint Staff J-6 staff official and a DoD CIO staff official, the DoD CIO and the CDAO have not developed policy or standards for tagging and labeling information for data-centric domains and data security in MPE networks.

---

[33] (U) As discussed in the Recommendations, Management Comments, and Our Response section of the report, Management Actions, during the evaluation, the DoD CIO and the DoD ISRMC took action to address the recommendation. Specifically, on March 21, 2025, the DoD ISRMC approved an IDAF "as the authoritative framework to evaluate information domains" with the caveats that the DoD ISRMC would revisit the IDAF in six months to determine lessons learned and any necessary process changes, to include an intelligence threat assessment.

[34] (U) Data tagging or labeling is the act of associating tags as metadata to an object by identifying, labeling, and describing its information. Data tagging and labeling can support access controls and how community of interests interact within a zero trust environment.

[35] (U) DoD Instruction 8520.04, "Access Management for DoD Information Systems," September 3, 2024.

[36] ~~(CUI)~~ The CDAO is the lead for CJADC2 line of effort 1 to establish the CJADC2 data enterprise, [redacted]

~~(CUI)~~ The data-centric approach has outpaced the DoD's ability to develop the tagging and labeling policy. [redacted] According to DoD CIO and Joint Staff J-6 personnel, the DoD must develop policy for tagging and labelling information to standardize data sharing with allies and partners on data-centric networks.

(U) Therefore, the DoD Chief Information Officer, in coordination with the Chief Digital and Artificial Intelligence Officer, should develop and implement policy that establishes the standards for the tagging and labeling of information shared on the Mission Partner Environment.

(U) The Absence of an IDAF and Lack of Clear Criteria for SABRE FOC Limit Partners' Abilities to Connect to Needed Mission Partner Environments

(U) The lack of a standard, comprehensive, and repeatable process to assess and authorize data-centric security for MPE information domains and the lack of clear criteria for SABRE FOC resulted in the following effects.

- ~~(U//FOUO)~~ [redacted][37]
- ~~(CUI)~~ [redacted] As a result, the Project Manager could not provide clear criteria for FOC.[38]
- ~~(CUI)~~ The DoD ISRMC addressed zero trust and data-centric solutions on a case-by-case basis. [redacted]

[37] ~~(U//FOUO)~~ [redacted]

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

~~(CUI)~~ [redacted] This non-standard approach increased operational and technical risk for the DoD and mission partners. The IDAF is intended to be the standard, comprehensive, and repeatable process to assess and authorize data-centric security, which could be a roadmap for future SABRE growth.

- ~~(CUI)~~ As a result of the limitations on connecting information domains to foreign information systems, the DoD continues to share classified information with allies and partners through multiple bilateral networks. [redacted] However, these separate networks do not support CJADC2's goal of systems integration where each partner's command and control system "can be accessed, viewed, and acted upon by every other approved partner."[39]

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the Air Force Program Executive Officer for Cyber and Networks define the Secret and Below Releasable Environment network minimum viable capability release standards to better determine policy constraints and the required exception processes and ensure that the system is developed in compliance with these requirements.

(U) Department of the Air Force Chief Information Officer Comments

(U) The Department of the Air Force Acting CIO, responding on behalf of the Air Force Program Executive Officer for Cyber and Networks and the DoD Mission Partner Environment (MPE) Executive Agent, agreed with recommendation. The Acting CIO stated that, in April 2025, the Program Executive Officer Cyber and Networks approved the Acquisition Strategy to Support Agile Development, Security, and Operations using a combination of software pathway and acquisition of services pathway. The Acting CIO provided an estimated completion date of August 2025.

[39] (U) DoD, "Summary of the Joint All-Domain Command and Control (JADC2) Strategy," March 2022.

(U) Our Response

(U) Comments from the Department of the Air Force Acting CIO addressed the specifics of the recommendation. Therefore, the recommendation is resolved but will remain open. We will close the recommendation when we verify that the Air Force Program Executive Office has implemented actions to fully address the recommendation.

(U) Recommendation 2

(U) We recommend that the DoD Chief Information Officer develop and implement an information domain assessment framework for Mission Partner Environments.

(U) DoD Chief Information Officer Comments

(U) The official Performing the Duties of the DoD CIO agreed and took action during the evaluation to address the recommendation. Specifically, on March 21, 2025, the DoD ISRMC approved the "DoD Information Domain Assessment Framework." The IDAF standardizes the DoD's mechanism to assess information domains supporting DoD mission partner environments.

(U) Our Response

(U) The actions taken by the official Performing the Duties of DoD CIO and the DoD ISRMC addressed the recommendation; therefore, the recommendation is closed.

(U) Recommendation 3

(U) We recommend that the DoD Chief Information Officer, in coordination with the Chief Digital and Artificial Intelligence Officer, develop and implement policy that establishes the standards for the tagging and labeling of information shared on the Mission Partner Environments.

(U) DoD Chief Officer Comments

(U) The official Performing the Duties of the DoD CIO agreed with the recommendation. The DoD CIO stated that as the co-chair of the DoD MPE Executive Steering Committee, which includes the CDAO, they are developing the standards for tagging and labeling for MPE. Coordinated efforts focus on data tagging federation, policy refinement through experimentation, and the development of digital policy registration aligned with the NATO Allied Communications Policy 240.[40]

[40] (U) NATO Combined Communications-Electronics Board, Allied Communications Publication 240, "Data-Centric Interoperability Concepts and Design Requirements," October 10, 2023.

(U) Department of the Air Force Chief Information Officer Comments

(U) The Department of the Air Force Acting CIO, responding on behalf of the DoD MPE Executive Agent, agreed and stated that the DoD CIO is working closely with the CDAO to address the recommendation.

(U) Our Response

(U) Comments from the official Performing the Duties of the DoD CIO and the Department of the Air Force Acting CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation when we verify that the DoD CIO has implemented actions to fully address the recommendation.

(U) Appendix

(U) Scope and Methodology

(U) We conducted this evaluation from July 2024 through May 2025 in accordance with the "Quality Standards for Inspection and Evaluation," published in December 2020 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the evaluation to ensure that objectives are met and that we perform the evaluation to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent and relevant to lead a reasonable person to sustain the findings, conclusions, and recommendations.

(U) To accomplish our objective, we:

- (U) requested information about CJADC2 line of effort for mission partner information sharing policies, organizational roles and responsibilities, and goals from the Office of the Under Secretary of Defense for Research and Engineering, DoD CIO, CDAO, Joint Staff J-6, Military Departments and Services, and selected combatant commands;
- (U) interviewed CJADC2 personnel from the Office of the Under Secretary of Defense for Research and Engineering, DoD CIO, CDAO, Joint Staff J-6, Joint Staff Directorate for Joint Force Development (J-7), Military Departments, and Service headquarters in the National Capital Region to provide context to the data and documentation we received; and
- (U) interviewed combatant command CJADC2 mission partner information sharing leads at USCENTCOM, USINDOPACOM, and U.S. European Command to determine to what extent the line of effort is implemented at the theater level.

(U) We conducted site visits to:

- (U) interview SABRE program personnel at Hanscom Air Force Base, Massachusetts, to identify and assess the progress of MPE and SABRE efforts;
- (U) interview Joint Staff J-6 Deputy Directorate South for Cyber and C4 Integration (DDS C5I) in Suffolk, Virginia, to interview personnel, observe operations, and review plans and progress to meet CJADC2 line of effort for mission partner information sharing requirements; and
- (U) observe a portion of the Project Olympus and Bold Quest 2024 coalition capability demonstration and assessment at Camp Lejeune, North Carolina.

(U) We reviewed applicable guidance, including:

- (U) DoD Directive 5101.22E, "Executive Agent (DoD EA) for DoD Mission Partner Environment (MPE)," August 5, 2020;
- (U) DoD Instruction 8110.01, "Mission Partner Environment Information Sharing," June 30, 2021; and
- ~~(CUI)~~ [redacted]

(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) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this evaluation.

(U) Prior Coverage

(U) During the last 5 years, the DoD Office of Inspector General (DoD OIG) and the Government Accountability Office (GAO) issued five reports discussing CJADC2 related efforts. The DoD OIG has one additional ongoing project.

(U) Unrestricted DoD OIG reports can be accessed at www.dodig.mil/reports. Unrestricted GAO reports can be accessed at http://www.gao.gov.

(U) DoD OIG

(U) Report No. DODIG-2025-090, "Audit of the DoD's Compliance with the FY 2022 National Defense Authorization Act's Requirements Concerning Zero Trust," April 29, 2025 (The report contains CUI)

> (U) The DoD generally complied with the FY 2022 National Defense Authorization Act's requirements for zero trust by developing its zero trust strategy, principles, and reference architecture. However, the Zero Trust Portfolio Management Office had not completed developing policies specific to operational technology, critical data, infrastructures, and weapon systems. The Zero Trust Portfolio Management Office Director stated that once they complete research to identify viable zero trust solutions for those environments, the policies will be developed.

(U) Report No. DODIG-2021-076, "Evaluation of Combatant Commands' Communication Challenges with Foreign Partner Nations during the Coronavirus Disease–2019 Pandemic and Mitigation Efforts," March 28, 2022 (Report is classified SECRET//NOFORN)

(U) The objective of this evaluation was to determine how the geographic combatant commands mitigated communication problems with partner nations during the COVID-19 pandemic and how these mitigation strategies should be employed in future operations where face-to-face interaction is not possible. The report recommended that the DoD CIO, in coordination with the Under Secretary of Defense for Intelligence and Security, conduct a needs assessment to better understand the technological limitations of U.S. foreign partners and how they impact the combatant command's ability to communicate and collaborate with these partners. This assessment should inform recommendations for DoD enterprise technology solutions to improve communications interoperability with foreign partners.

(U) In response to the recommendation, the DoD CIO provided the Mission Partner Environment Capability Definition Package, dated January 16, 2023, which provided validated MPE requirements to support resourcing, capability solutions development, and materiel solution fielding and implementation. The recommendation to the DoD CIO was closed.

(U) The DoD OIG is also conducting an audit to assess the effectiveness of USINDOPACOM's cybersecurity controls over access to information in its mission partner environment. (Project No. D2024-D000CS-0186.000)

(U) GAO

(U) Report No. GAO-25-106454, "Defense Command and Control: Further Progress Hinges on Establishing a Comprehensive Framework," April 2025

(U) The GAO concluded that the DoD had yet to build a framework that can guide CJADC2-related investments across the DoD or make progress toward its goals. In the absence of clear direction, DoD Components will continue to pursue their command and control projects largely in isolation, which will likely result in achieving CJADC2 more slowly and inefficiently. The GAO recommended that the DoD develop a framework for CJADC2 that helps guide investments and measures progress; devise a mechanism for sharing lessons learned; and identify and address key challenges in achieving its CJADC2 goals.

(U) Report No. GAO-23-105495, "Battle Management: DOD and Air Force Continue to Define Joint Command and Control Efforts," January 13, 2023

(U) The GAO concluded that the DoD was in the early stages of developing CJADC2 and released initial guidance, including a strategy that outlines broad goals. However, the DoD had not yet defined the details, such as which existing systems will contribute to CJADC2 and what future capabilities need to be developed. A House of Representatives report directed the DoD to report on the scope, cost, and schedule of the overall CJADC2 effort, and the DoD was in the early stages of determining those elements.

(U) In a prior April 2020 report, the GAO recommended that the Air Force develop a plan to mature technologies, develop a cost estimate, and conduct an affordability analysis for its Advanced Battle Management System. Since then, the Air Force took steps to address the 2020 recommendations through acquisition and planning documents but needed to do more to fully address them.

(U) Report No. GAO-20-389, "Defense Acquisitions: Action Is Needed to Provide Clarity and Mitigate Risks of the Air Force's Planned Advanced Battle Management System," April 16, 2020

(U) The GAO concluded that the Air Force was developing the Advanced Battle Management System—a network to connect U.S. forces during military operations across land, sea, space, and cyberspace. Through cloud-based data sharing, sensors on drones, aircraft, ships, and other weapon systems would gather and aggregate real-time intelligence, surveillance, and reconnaissance information. The GAO found that the Air Force had not developed a complete plan for the system—such as identifying which technologies would be included and the cost—putting it at risk for schedule delays, cost growth, and other issues if they do not work together as intended. The GAO made four recommendations, including that the Air Force develop and brief the Congress quarterly on a plan to mature technologies, a cost estimate, and an affordability analysis. Furthermore, the Air Force should formalize the Advanced Battle Management System management structure and decision-making authorities.

(U) Management Comments

(U) DoD Chief Information Officer

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JUN 18 2025

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General "Evaluation of the DoD's Implementation of Combined Joint All-Domain Command and Control (CJADC2) Strategy, May 14, 2025 (D2024-DEV0SI-0130.000) Draft Report

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Draft Report "Evaluation of the DoD's Implementation of Combined Joint All-Domain Command and Control (CJADC2) Strategy, May 14, 2025 (D2024-DEV0SI-0130.000).

DoD IG RECOMMENDATION 2: We recommend that the DoD Chief Information Officer develop and implement an information domain assessment framework for Mission Partner Environments.

DoD CIO RESPONSE: DoD CIO agrees with the DoD IG recommendation.

The DoD CIO developed and as the co-chair, for the DoD Information Security Risk Management Committee (ISRMC) approved the "*DoD Information Domain Assessment Framework*" on 21 March 2025, standardizing the Departmental mechanism to assess information domains supporting DoD mission partner environments. The recommendation is met by the issuance of this memorandum (attached).

DoD IG RECOMMENDATION 3: We recommend that the DoD Chief Information Officer, in coordination with the Chief Digital and Artificial Intelligence Officer (CDAO), develop and implement policy that establishes the standards for the tagging and labeling of information shared on the Mission Partner Environments.

DoD CIO RESPONSE: DoD CIO agrees the DoD IG recommendation.

The DoD CIO, as the co-chair for the DoD Mission Partner Environment Executive Steering Committee, which includes the CDAO, is developing the standards for tagging and labeling for MPE. Coordinated efforts focus on data tagging federation, policy refinement through experimentation, and the development of digital policy registration aligned with the NATO Allied Communications Policy 240.

A security review to verify "Unclassified" (U) markings in the report has been completed and there are no additional recommendations.

The point of contact for this matter is [redacted]

Katherine Arrington
Performing the Duties of the
Chief Information Officer of the
Department of Defense

Attachment:
As stated

(U) Department of the Air Force Chief Information Officer

DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

OFFICE OF THE SECRETARY

9 June 2025

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: SAF/CNS
1120 Air Force Pentagon
Washington, DC 20330

SUBJECT: Department of the Air Force Response to DoD Office of Inspector General Draft Report, "Evaluation of a Line of Effort in the DoD's Implementation of the Combined Joint All-Domain Command and Control (CJADC2) Strategy" (Project No. D2024-DEV0SI-0130.000)

1. In response to the DoDIG draft report assessing the effectiveness with which the DoD developed and implemented the Combined Joint All-Domain Command and Control line of effort to modernize mission partner information sharing, the Department of the Air Force concurs with the report as written.

2. SAF/CN as the DoD Mission Partner Environment Executive Agent, in coordination with the DoD Chief Information Officer, Joint Staff J6, and Program Executive Office Cyber & Networks, are addressing the following recommendations identified in this report:

RECOMMENDATION 1: The DODIG recommends Program Executive Office Cyber & Networks define the Secret and Below Releasable Environment Minimum Viable Capability release standards to better determine policy constraints and the required exception processes and ensure the system is developed in compliance with these requirements.

DAF RESPONSE: The DoD Mission Partner Environment Executive Agent agrees with the recommendation to define Secret and Below Releasable Environment Minimum Viable Capability release standards. In April 2025, Program Executive Office Cyber & Networks approved the Acquisition Strategy to support Agile DevSecOps using a combination of Software Pathway and Acquisition of Services Pathway. **Estimated Completion Date: August 2025**

RECOMMENDATION 2: The DODIG recommends DoD Chief Information Officer develop and implement a Mission Partner Environment Information Domain Assessment Framework.

(U) Department of the Air Force Chief Information Officer (cont'd)

DAF RESPONSE: The DoD Mission Partner Environment Executive Agent agrees with the recommendation to define a Mission Partner Environment Information Domain Assessment Framework. DoD Chief Information Officer established the Information Domain Technical Advisory Board with the formal charter signed in March 2025. The Mission Partner Environment Information Domain Assessment Framework was approved by the Information Security Risk Management Committee in April 2025 and will be utilized for future approval of Information Domains. **Estimated Completion Date: Ongoing**

RECOMMENDATION 3: The DODIG recommends the DoD Chief Information Officer, in coordination with the Chief Digital and Artificial Intelligence Officer, develop and implement policy that establishes the standards for the tagging and labeling of information shared on the Mission Partner Environments.

DAF RESPONSE: The DoD Mission Partner Environment Executive Agent agrees with the recommendation for the Chief Digital and Artificial Intelligence Officer to develop and implement policy that establishes the standards for the tagging and labeling of information shared on the Mission Partner Environments. DoD Chief Information Officer is working closely with the Chief Digital and Artificial Intelligence Officer to address this recommendation. **Estimated Completion Date: Ongoing**

3. The SAF/CN point of contact is [redacted]

OROZCO.JENNIF ER.M[redacted]

JENNIFER M. OROZCO, SES, DAF
Acting Chief Information Officer

(U) Acronyms and Abbreviations

(U) BOD	Binding Operational Directive
(U) CJADC2	Combined Joint All-Domain Command and Control
(U) C2	Command and control
(U) CDAO	Chief Data and Artificial Intelligence Officer
(U) CIO	Chief Information Officer
(U) FOC	Full Operational Capability
(U) IDAF	Information Domain Assessment Framework
(U) IOC	Initial Operational Capability
(U) ISRMC	Information Security Risk Management Committee
(U) Joint Staff J-6	Joint Staff Directorate for Command, Control, Communications, and Computers/Cyber
(U) MPE	Mission Partner Environment
(U) NATO	North Atlantic Treaty Organization
(U) NSA	National Security Agency
(U) SABRE	Secret and Below Releasable Environment
(U) USINDOPACOM	U.S. Indo-Pacific Command
(U) USCENTCOM	U.S. Central Command

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