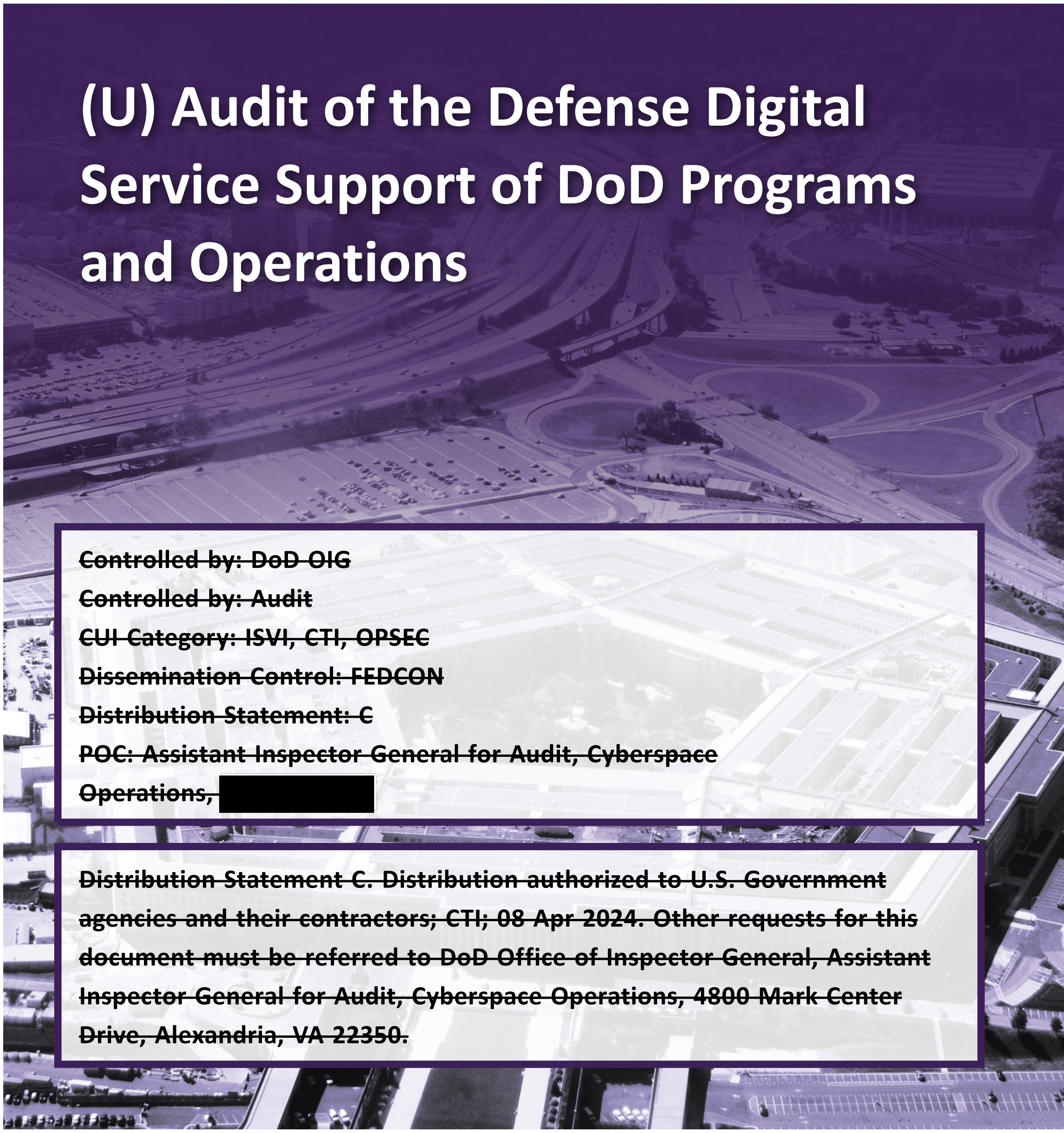
Report No. DODIG-2024-087

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

MAY 29, 2024



(U) Audit of the Defense Digital Service Support of DoD Programs and Operations

~~Controlled by: DoD OIG~~
~~Controlled by: Audit~~
~~CUI Category: ISVI, CTI, OPSEC~~
~~Dissemination Control: FEDCON~~
~~Distribution Statement: C~~
~~POC: Assistant Inspector General for Audit, Cyberspace Operations,~~ [redacted]

~~Distribution Statement C. Distribution authorized to U.S. Government agencies and their contractors; CTI; 08 Apr 2024. Other requests for this document must be referred to DoD Office of Inspector General, Assistant Inspector General for Audit, Cyberspace Operations, 4800 Mark Center Drive, Alexandria, VA 22350.~~

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

~~CUI~~

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

(U) Results in Brief

(U) Audit of the Defense Digital Service Support of DoD Programs and Operations

May 29, 2024

(U) Objective

(U) The announced objective of this audit was to determine whether Defense Digital Service (DDS) engagements achieved their intended purpose and were executed in accordance with DoD and Federal policies. On January 18, 2023, the DoD Hotline received a complaint alleging that the Chief Digital and Artificial Intelligence Office (CDAO), particularly DDS officials, relied on waivers they granted themselves to use unauthorized information technology tools and services in violation of DoD policy. We expanded the scope of our audit to include a review of those allegations.

(U) Background

(U) In 2015, the Secretary of Defense established the DDS to increase the DoD's digital innovation and modernize DoD practices and procedures by leveraging expertise from the private sector. The majority of DDS engagements result in a prototype digital application or technological solution that is then transferred to the DoD Component that requested the engagement for further development, funding, and maintenance. DDS engagements can also produce in-depth reports of findings and recommendations, quick technical fixes, or advice.

(U) On February 1, 2022, the Deputy Secretary of Defense established the CDAO, and the DDS was realigned under the CDAO.

(U) Findings

(U) We determined that 5 of the 10 DDS engagements we reviewed met their intended purpose, but we were unable to determine whether the other 5 engagements did because DDS officials did not maintain adequate and proper records of the purpose, work completed, and results of those engagements. This occurred because the Office of the Secretary of Defense did not establish effective internal controls to ensure DDS implemented Federal and DoD records management policies. In addition, the Washington Headquarters Services, which was required to provide guidance to DDS officials on the creation and organization of a records management program and ensure compliance with records management policies, did not ensure that a program was established. Without adequate and proper records of all DDS engagements, DoD officials cannot analyze the effectiveness of DDS efforts and DDS officials cannot identify lessons learned or best practices, which are necessary to implement reproducible processes that can be used throughout the DoD.

(U) We substantiated the allegation that DDS officials relied on waivers of DoD policies they improperly granted to use unauthorized information technology tools and services in violation of the DDS Charter and DoD policy. The waivers enabled the DDS to use unauthorized digital service tools, including cloud-based software development platforms and collaboration software, to store, process, and transmit controlled unclassified information. This occurred because the Office of the Secretary of Defense did not establish effective internal controls to ensure that the DDS Director exercised their authorities as intended. As a result, the DDS Directors exposed DoD information to additional cybersecurity risk and increased the risk of compromise.

(U) Results in Brief

(U) Audit of the Defense Digital Service Support of DoD Programs and Operations

(U) Recommendations

(U) We made 15 recommendations to address the findings of this report. Among other recommendations, we recommended that the CDAO:

- (U) in coordination with the Washington Headquarters Services Director, develop, resource, and implement a records management program;
- (U) develop a clear waiver request process for CDAO directorates that includes a requirement to document and maintain records of the requests; and in coordination with the Defense Information Systems Agency Chief Information Officer, assess the hardware, software, cloud services, networks, and any other tools used by the DDS since 2015 to ensure compliance with DoD cybersecurity requirements.

(U) Management Comments and Our Response

(U) The CDAO agreed with and provided planned actions to address seven of the recommendations; therefore, these recommendations are resolved but remain open. We will close the recommendations once we verify that management has implemented the agreed upon actions.

(U) The CDAO, responding for the CDAO Chief Information Officer and Authorizing Official, agreed with, but did not provide planned actions to address an additional seven recommendations and Washington Headquarters Services Director disagreed with one recommendation. Therefore, these recommendations are unresolved, and we request that the CDAO Chief Information Officer and Authorizing Official and the Washington Headquarters Services Director provide comments addressing the recommendations, within 30 days, in response to the final report.

(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
Chief Digital and Artificial Intelligence Officer	None	A.1, A.2, B.3, B.4.a, B.4.b, B.4.c, B.5	None
Director, Washington Headquarters Services	A.3	None	None
Chief Information Officer and Authorizing Official, Chief Digital and Artificial Intelligence Office	B.1.a, B.1.b, B.1.c, B.1.d, B.2.a, B.2.b, B.2.c	None	None **(U)**

(U) Please provide Management Comments by June 28, 2024.

(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
INTEGRITY EFFICIENCY
DEPARTMENT OF DEFENSE

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

May 29, 2024

MEMORANDUM FOR CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER
DIRECTOR, WASHINGTON HEADQUARTERS SERVICES
DIRECTOR, DEFENSE DIGITAL SERVICES, CHIEF INFORMATION AND ARTIFICIAL INTELLIGENCE OFFICE

SUBJECT: (U) Audit of the Defense Digital Service Support of DoD Programs and Operations (Report No. DODIG-2024-087)

(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 eight recommendations that are considered unresolved because the Chief Information Officer and Authorizing Official, Chief Digital and Artificial Intelligence Office and the Washington Headquarters Services Director did not agree or did not fully address the recommendations. We will track these recommendations until management has agreed to take actions that we determine to be sufficient to meet the intent of the recommendations and submit adequate documentation showing that all agreed-upon actions are completed.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, within 30 days please provide us your response concerning specific actions in process or alternative corrective actions proposed on the eight unresolved recommendations. Send your response to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET.

(U) This report contains seven recommendations that we consider resolved and open. We will close these recommendations when the Chief Digital and Artificial Intelligence Officer provides us documentation showing that all agreed-upon actions are completed. Therefore, within 90 days please provide us your response concerning specific actions in process or completed on the seven resolved recommendations. Send your response to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET.

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

FOR THE INSPECTOR GENERAL:

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

(U) Contents

(U) Introduction

(U) Finding A. DDS Officials Did Not Consistently Maintain Records of Engagements

(U) Finding B. DDS Directors Exceeded the Authorities Granted in the DDS Charter

(U) Contents (cont'd)

Appendixes

(U) Introduction

(U) Objective

(U) The announced objective of this audit was to determine whether Defense Digital Service (DDS) engagements achieved their intended purpose and were executed in accordance with DoD and Federal policies.[1] On January 18, 2023, the DoD Hotline received a complaint alleging that the Chief Digital and Artificial Intelligence Office (CDAO), particularly DDS officials, relied on waivers of DoD policies they granted themselves to use unauthorized information technology tools and services in violation of DoD policy.[2] Therefore, we expanded the objective and scope of our audit to review those allegations. Please see Appendix A for a discussion on the scope, methodology, and prior coverage related to the audit objective.

(U) We announced this audit on August 2, 2021. On July 7, 2022, we responded to a congressional inquiry to a specific DDS engagement concerning millions of dormant Internet Protocol version 4 (IPv4) addresses.[3] In addition, during the audit, we identified concerns with the DoD's use of unauthorized unmanaged mobile applications on DoD mobile devices and issued a management advisory on February 9, 2023, addressing those concerns.[4] Although both of those efforts extended the time needed to complete this audit, the findings and recommendations in this report remain relevant. Please see Appendix B for additional information on the congressional inquiry and management advisory.[5]

(U) Background

(U) Digital services include the development and delivery of digital data, software, applications, and services (technical guidance, training, or best practices) across multiple platforms, devices, and delivery mechanisms, such as the cloud, web and mobile applications, and social media. On November 18, 2015, the Secretary of Defense established the DDS to increase the DoD's digital innovation and modernize DoD practices and procedures by leveraging expertise from the private sector.

[1] (U) For the purposes of this report, "engagements" mean the Projects, Discovery Sprints, Rapid Response, and Tech Navigators that the DDS completes. For a description of the types of engagements, please see Appendix C.

[2] (U) On February 1, 2022, the Deputy Secretary of Defense established the CDAO, integrating the Joint Artificial Intelligence Center, the Office of the Chief Data Officer, the Office of Advancing Analytics, and the DDS into one organization.

[3] (U) Each machine connected to the Internet has an address known as an Internet Protocol address. Internet Protocol version 4 addresses are the addresses used since 1983.

[4] (U) Report No. DODIG-2023-041, "Management Advisory: The DoD's Use of Mobile Applications," February 9, 2023.

[5] (U) This report contains information that has been redacted because it was identified by the Department of Defense 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.

(U) On January 5, 2017, the Secretary of Defense issued DoD Directive 5105.87, "Director, Defense Digital Service (DDS)" (DDS Charter).[6] The DDS Charter states that the DDS' mission is to "work on specific projects or programs in support of the DoD in a 'hands-on' way to materially improve digital services." To achieve its mission, the DDS uses private sector best practices, talent, and technology intended to transform the way digital services are delivered within the DoD.

(U) The DDS hires employees, such as software engineers, product managers, and user experience researchers on 2-year contracts with the option to extend for another 2 years, after which they return to the private sector.[7] Since 2015, the DDS has conducted more than 90 digital service engagements in areas including artificial intelligence, insider threat, the global positioning system, military pay, and cybersecurity vulnerabilities. The majority of DDS engagements result in a prototype digital application or technological solution that is then transferred to a DoD Component for further development, funding, and maintenance.[8] DDS engagements can also produce in-depth reports of findings and recommendations, quick technical fixes, or advice.

(U) On February 1, 2022, the Deputy Secretary of Defense established the Office of the CDAO and designated the CDAO as the intervening supervisor between the DDS and the Office of the Secretary of Defense (OSD).[9] The CDAO's mission is to accelerate the DoD's use of data, analytics, and artificial intelligence to benefit its decision-making processes and advance capabilities. The DDS was realigned under the CDAO.

(U) DDS Engagement Selection Process

(U) The DDS Charter states that the DDS Director, in consultation with DoD Components and in coordination with the Secretary of Defense, is responsible for identifying engagements with the potential to improve digital services and for selecting engagements for execution based on their impact to the DoD. The DDS had four strategic priorities.

- (U) Force Protection – Develop a suite of tools for operational units to protect Service members.

[6] (U) DoD Directive 5105.87, "Director, Defense Digital Services (DDS)," January 5, 2017, Change 1 effective December 4, 2019. As of January 2024, the DDS Charter has not been canceled by CDAO policy, and a new CDAO Charter has not yet been issued.

[7] (U) A user experience researcher studies what the end users of a system or product need to enhance the design process for the products, services, or software.

[8] (U) A prototype is a physical or digital model built to evaluate and demonstrate its feasibility or usefulness.

[9] (U) Deputy Secretary of Defense memorandum, "Establishment of the Chief Digital and Artificial Intelligence Officer," December 8, 2021.

- (U) Secure Systems – Secure the DoD’s digital and physical assets and provide secure operational platforms.
- (U) Rapid Response – Address immediate problems by providing accessible technical experts for short-term missions.
- (U) Near Peer – Address adversaries advancing beyond our technologies.

(U) During the time of our review, the engagement selection process normally began with a request to the DDS from the OSD or a DoD Component; however, the DDS could also initiate cybersecurity-related engagements.[10] The DDS used three selection criteria when selecting an engagement. First, the DDS determined whether the proposed engagement addressed a critical, life-endangering gap for the DoD. Second, the DDS determined whether the engagement would radically change systems and processes that protect troops, secure physical and digital assets, and put the DoD ahead of our adversaries. Finally, the DDS determined whether DDS employees had the talents and skills required to assist with the requested engagement. If the proposed engagement met the three criteria and fell into one of the DDS strategic priorities, the DDS would select the engagement for execution and determine the appropriate engagement category.[11]

- (U) Portfolios – Long-term engagements made up of multiple engagements on the same subject.[12]
- (U) Projects – Individual engagements that develop and deliver technology to solve problems.
- (U) Discovery Sprints – Observational engagements that help DoD Components overcome organizational and technical challenges.
- (U) Rapid Response – Fast technical engagements that result in quick fixes or possible paths forward.
- (U) Tech Navigators – Advisory engagements that address technological challenges.

(U) DDS Engagements Selected for Review

(U) We identified 92 engagements initiated by the DDS from November 2015 to July 2021. The DDS grouped the engagements based on engagement category and strategic priority, and we nonstatistically selected 10 engagements for review as detailed in Table 1. Please see Appendix A for more information about our sample.

[10] (U) According to DDS officials, the DDS engagement selection process was revised in November 2023 to help the DDS meet its new mission to deliver better services to the warfighter through design and technology.

[11] (U) Please see Appendix C for more details about the engagement categories.

[12] (U) We included the individual engagements that make up a Portfolio in our universe of engagements.

(U) Table 1. Sample of DDS Engagements Selected for Review

~~(CUI)~~ Engagement Category	Strategic Priority	DDS Engagement
Discovery Sprints	Force Protection	[redacted] September 2020
		[redacted] *DoD Component Supported*: [redacted]
	Secure Systems	[redacted] September – October 2020
		[redacted] *DoD Component Supported*: [redacted]
Projects	Force Protection	[redacted] November 2018
		[redacted] *DoD Component Supported*: [redacted]
	Force Protection	[redacted] July 2019 – Present
		[redacted] *DoD Component Supported*: [redacted]
	Secure Systems	[redacted] April – November 2018
		[redacted] *DoD Component Supported*: [redacted]
	Secure Systems	[redacted] April – August 2019
		[redacted] *DoD Component Supported*: [redacted]
	Near-Peer	[redacted] March 2020 – December 2022
		[redacted] *DoD Component Supported*: [redacted] ~~(CUI)~~

(U) Table 1. Sample of DDS Engagements Selected for Review (cont'd)

~~(CUI)~~ Engagement Category	Strategic Priority	DDS Engagement
Rapid Response	Rapid Response	[redacted] September 2017
		[redacted] *DoD Component Supported*: [redacted]
	Rapid Response	[redacted] March 2020 – October 2021
		[redacted] *DoD Component Supported*: [redacted]
Tech Navigators	Secure Systems	[redacted] June – November 2019
		[redacted] *DoD Component Supported*: [redacted] **~~(CUI)~~**

(U) Source: The DoD OIG.

*~~(CUI)~~ [redacted]

(U) Finding A

(U) DDS Officials Did Not Consistently Maintain Records of Engagements

(U) We determined that 5 of the 10 DDS engagements we reviewed met their intended purpose, but we were unable to determine whether the other 5 engagements met their intended purpose because DDS officials did not maintain adequate and proper records of the purpose, work completed, and results of those engagements. Federal and DoD records management policies require Components to create, maintain, and preserve adequate and proper records, including documentation of agency organization, functions, policies, procedures, decisions, and activities. In addition, the DoD records management policy requires DoD Component heads to establish, resource, and maintain a records management program within their organizations.

(U) The DDS did not maintain adequate and proper records because the OSD did not establish effective internal controls to ensure the DDS implemented Federal and DoD records management policies.[13] In addition, the Washington Headquarters Services (WHS), which was required to provide guidance to DDS officials on the creation and organization of a records management program and ensure compliance with Federal and DoD records management policies, did not ensure that DDS officials established a records management program.[14]

(U) We acknowledge that the DDS was established, in part, to improve the deployment of digital services in the DoD through rapid engagements; however, DDS officials were not exempt from the Federal and DoD requirements to maintain engagement records as evidence of the DDS' organization, functions, policies, procedures, decisions, and activities. Without engagement records, DoD officials cannot analyze the effectiveness of DDS efforts to improve digital services in the DoD and DDS officials cannot identify lessons learned or best practices, which are necessary to implement reproducible processes that can be used throughout the DoD. Moreover, because DDS officials transition every 2 years, the lack of records negatively affected the continuity and impact of engagements, as DDS officials and incoming personnel had only limited historical knowledge of the ongoing and prior engagements.

[13] (U) On September 1, 2021, the Deputy Secretary of Defense disestablished the Office of the Chief Management Officer and reassigned the responsibilities of overseeing OSD records management programs to the Director of Administration and Management.

[14] (U) The DDS Charter states that the DDS is a WHS-serviced office. According to DoD Directive 5110.04, "Washington Headquarters Services," March 27, 2013 (Incorporating Change 1, March 23, 2023), WHS is required to provide broad range of administrative, management, and common support services, including human resources and security clearance services, facilities and facility operations, financial management, and acquisition and contracting. WHS is also required to provide oversight of designated DoD-wide statutory and regulatory programs, such as the OSD records management program, for DoD Components and other Federal entities.

(U) Federal and DoD Policies

(U) Section 3101, title 44, United States Code, requires that the head of each Federal agency make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency. Title 36 Code of Federal Regulations section 1222.22, "What records are required to provide for adequate documentation of agency business?" states that to meet their obligation for adequate and proper documentation, agencies must require the creation and maintenance of records that:

- (U) document the persons, places, things, or matters dealt with by the agency;
- (U) facilitate agency officials and their successors in office to take action;
- (U) make possible scrutiny by Congress or other duly authorized agencies of the Government;
- (U) protect the financial, legal, and other rights of the Government and of persons directly affected by the Government's actions;
- (U) document the development and execution of basic policies, decisions, and actions, including all substantive decisions and commitments reached orally (person-to-person, by telecommunications, or in conference) or electronically; and
- (U) document important board, committee, or staff meetings.

(U) DoD Instruction 5015.02, "DoD Records Management Program," requires DoD Components to implement a record management program to create, maintain, use, and preserve records to document the "transaction of business and mission."[15] The Instruction states that DoD Components should implement records management controls and accountability standards necessary to capture, manage, and preserve Component records, including electronic records and messages. It also states that effective and efficient management of records provides the information for decision-making, mission planning and operations, business continuity, and preservation of U.S. history.

(U) Administrative Instruction (AI) 15, "Office of the Secretary of Defense Records and Information Management Program," May 3, 2013 (Incorporating Change 2, November 17, 2020), establishes responsibilities and administrative procedures for the management of records and information in accordance with Federal and DoD records management policies.[16] Specifically, the Instruction outlines the responsibilities of the WHS and the head of a WHS-serviced Component for the creation, organization, maintenance, use, and disposition of records and information.

[15] (U) DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, Incorporating Change 1, August 17, 2017.

[16] (U) The Office of the Director of Administration and Management issued a revised version of AI 15, "OSD Records and Information Management Program," on November 27, 2023.

(U) The DDS Met the Intended Purpose for Five of the Engagements Reviewed

~~(CUI)~~ We determined that 5 of the 10 DDS engagements we reviewed—[redacted] [redacted] [redacted] [redacted] and [redacted]—met their intended purpose. To determine whether the DDS engagements achieved their intended purpose, we reviewed records regarding the planning, execution, and transfer of the engagements to the DoD Component requestor and interviewed DDS project managers and DoD Component personnel who worked on the engagements. For all five DDS engagements, we were either able to obtain sufficient documentation or use a combination of the documentation and interviews with DDS and DoD Component officials to determine that the engagements met their intended purpose.

~~(CUI)~~ DDS records for the [redacted] and [redacted] engagements included information concerning the expectations and responsibilities of the DDS, plans of execution for the engagement, key decisions made, progress reviews with the DoD Component requestor, and the results of the engagement. For example, for the [redacted] engagement, [redacted]

~~(CUI)~~ Although the DDS records for the [redacted] [redacted] and [redacted] engagements did not contain all of the information concerning the decisions made, work completed, or the transfer of the finished engagement to the DoD Component, the DDS officials who worked on the engagements still worked for the DoD and were able to verbally provide that information, which we corroborated with the DoD Component requestor. For example, during the [redacted] engagement, [redacted]

~~(CUI)~~ [redacted] The DDS project manager provided records that allowed us to understand the engagement, including the plans, deliberations, and determinations made throughout the engagement, but the records did not include evidence that DDS efforts resulted in [redacted] We met with the DDS project manager and [redacted] officials who explained the level of support provided and actions taken by the DDS during the engagement and that the support provided by the DDS met the intended purpose of the engagement.

(U) The DDS Lacked the Records to Support That Five of the Engagements Reviewed Met Their Intended Purpose

~~(CUI)~~ We were unable to determine whether the other five DDS engagements we reviewed—[redacted], [redacted] [redacted] [redacted] and [redacted]—met their intended purpose because DDS officials did not maintain sufficient records of the engagement. Specifically, DDS officials did not have records of the initial request from the DoD Component, decisions made during the engagement, the work completed, and the result of the engagement. Furthermore, the records that DDS officials maintained for these engagements were inconsistent, and the quality, quantity, and type of records varied widely.

~~(CUI)~~ For example, DDS officials were unable to provide adequate records for the [redacted] and [redacted] engagements. For the [redacted] engagement, [redacted][17] DDS officials provided the final report to us, but they had no additional information about the engagement, such as notes from meetings with [redacted] officers or evidence that [redacted] officials received a report or accepted the DDS' recommendations. In addition, [redacted] could not locate any records or personnel with direct knowledge of this engagement. For the [redacted] engagement, in 2018, [redacted] DDS officials provided a charter and periodic progress reviews of the engagement but did not have records about the decisions made or work completed. DDS officials were also unable to provide contact information for the [redacted] officials who were involved in the engagement. Additionally, the

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

~~(CUI)~~ DDS project managers responsible for the engagements no longer worked at the DDS, and the former DDS Director could provide only limited information about the engagements to the audit team. Furthermore, DDS officials stated that they did not conduct after-action reviews to determine the effectiveness of the solution provided or identify lessons learned for any of the engagements in our sample.

(U) The DDS Did Not Establish a Records Management Program

~~(CUI)~~ DDS officials did not establish a records management program because the OSD did not establish effective internal controls to ensure that the DDS implemented Federal and DoD records management policies. DDS officials stated that since 2015, they have electronically stored information and documentation about engagements in shared environments, such as a shared [redacted] and group [redacted] messages.[18] However, AI 15 states that shared environments do not provide the functionality of a recordkeeping system unless the organization applies manual and automated processes to ensure that information can be easily retrieved, identified, and managed. The Instruction states that managing records in a shared environment requires intervention to manage naming conventions, version control, personally identifiable information, access control, and separation of personal from official records. The former DDS Director stated that because of the lack of records management processes in place under previous directors for the shared environments, some older engagement data had been lost. Additionally, the former DDS Director stated that in October 2020, they provided verbal, strategic-level guidance to the DDS project managers regarding identifying, approving, and managing engagements. Finally, the former DDS Director stated that they also required DDS officials to begin using [redacted] collaboration software to manage the requests for support, approval, progress, and transfer plans for new engagements.[19] However, the DDS officials did not use [redacted] to manage all of the engagements in our sample, and the verbal guidance the Director provided did not include processes and procedures to create and maintain adequate and proper records for engagements or to conduct after-action reviews to identify lessons learned and best practices. Furthermore, the former Director did not formalize the guidance in a written policy or procedure. DDS officials stated that DDS personnel are required to take the mandatory DoD trainings which includes records management training. However, the WHS officials could not verify that any DDS personnel had completed the records management training. Therefore, the CDAO, in coordination with the WHS

[18] ~~(CUI)~~ [redacted] is a cloud storage service that allows users to collaborate on and share files from computers, mobile devices, or tablets. [redacted] is a messaging application for businesses that allows for group messaging, as well as file sharing, reminders, and video calls.

[19] ~~(CUI)~~ [redacted] is a collaboration tool that allows users to organize, share, and create files together.

~~(CUI)~~ Director, should develop, resource, and implement a records management program that includes records management training for all personnel in accordance with Federal and DoD records management requirements. In addition, the CDAO should implement a formal after-action review process to determine the success and effectiveness of the DDS engagements.

(U) In addition, the WHS did not ensure that DDS officials established a records management program as required by AI 15. According to the Instruction, the WHS Director is responsible for directing and administering the records and information management program for the WHS-serviced Components. The Instruction also states that the WHS Director is required to provide guidance to the WHS-serviced Components on the creation, organization, maintenance, use, and disposition of records and information and ensure compliance with Federal and DoD records management policies. Although WHS officials were not able to locate the emails, they stated that they reached out to DDS officials by email about establishing a records management program and to schedule an inspection of the program twice, but those emails went unanswered. As a result, the WHS officials did not ensure that DDS officials established a records management program. Because the DDS has been re-aligned under the CDAO, it will be a part of the CDAO's records management program; however, there may be other WHS-serviced Components that, like the DDS, do not have a records management program. Therefore, the WHS Director should ensure that each head of a WHS-serviced Component has established and resourced a records and information management program within their organization in accordance with DoD policies.

(U) Lack of Adequate and Proper Records Hinders the Ability to Determine DDS Success

(U) Without adequate documentation of the DDS engagements, DoD officials cannot analyze the effectiveness of DDS efforts to improve digital services in the DoD. Without historical data or after-action reviews, DoD and DDS officials are also unable to assess the DoD's use or impact of the solutions provided by the DDS. In addition, DDS officials cannot identify lessons learned or best practices, which are necessary to implement reproducible processes that can be used throughout the DoD and to improve their operations and future engagements.

(U) Moreover, because DDS officials transition every 2 years, the lack of records negatively affected the continuity and impact of engagements, as DDS officials and incoming personnel have only limited historical knowledge of prior engagements. These frequent personnel transitions increase the importance of creating consistent records to maintain continuity throughout the engagements. To ensure that the DDS meets its mission to improve digital services throughout the DoD, the DDS must implement policies that outline repeatable and clear processes to ensure the continuity, consistency, and effectiveness of its operations.

(U) Management Comments on the Finding and Our Response

(U) Washington Headquarters Services Comments

(U) The WHS Director provided comments on the finding, stating that they had concerns with the DoD OIG report's assertion that the WHS was at fault for the DDS' failure to implement a records management program. The Director stated that records management guidance is readily available on the DoD website and that the OSD and DoD policies clearly state that Component Heads are responsible for establishing a records management program within their organizations. The Director included a timeline of the creation of the DDS, the Joint Artificial Intelligence Center, and the CDAO prepared by the Senior Historian, History and Library Directorate, OSD Historical Office and a list of suggested revisions to the body of the report.

(U) The WHS Director also included comments from the WHS Director of the Executive Services Directorate (ESD) with their response. The ESD Director stated that it is factually inaccurate to state in the report that the WHS Director is responsible for directing and administering the Records and Information Management Programs for WHS-serviced Components pursuant to AI 15. They stated that the WHS Director is assigned only one responsibility in AI 15 and that is to designate the ESD Director as the OSD Senior Agency Official for Records Management.

(U) Our Response

(U) We disagree that the WHS lacked responsibility for ensuring that WHS-serviced Components established a records management program. AI 15 requires that the WHS Chief, Records and Privacy and Declassification Division (RDD), ESD, institute and oversee a records management evaluation program to ensure compliance with Federal and DoD policy.[20] The DDS had not established a records management program and; therefore, were not in compliance with Federal and DoD policy. WHS officials acknowledged that they did not conduct an evaluation of the DDS records management program. Had they conducted an evaluation, WHS officials would have identified the noncompliance and reported it to the appropriate officials.

[20] (U) AI 15, "OSD Records and Information Management Program," May 3, 2013. This language remained unchanged in the updates to AI 15 on April 19, 2017 and November 17, 2020.

(U) We also disagree that the report is factually inaccurate regarding the WHS Director's responsibilities. We acknowledge that AI 15 was reissued on November 27, 2023, and the responsibilities for the WHS Director were revised to only require the WHS Director to designate the ESD Director to serve as the OSD Senior Agency Official for Records Management. However, the A1 15 versions in effect during the scope of this audit assigned the WHS Director the responsibilities to direct and administer the records and information management program for the WHS-serviced Components; provide guidance to the WHS-serviced Components on the creation, organization, maintenance, use, and disposition of records and information; and ensure compliance with Federal and DoD records management policies, as we state on p. 11 of this report.

(U) We reviewed the list of suggested revisions to the report and made two minor editorial changes. Specifically, we revised "DoD" to "OSD" records management program in footnote 14 and "2015" to "2013" in the reference to AI 15 on page 7. The other suggested revisions were related to defining the WHS Director's roles and responsibilities, redirecting recommendations to other parties, and incorporating records management requirements into Finding B. We did not make those revisions because we properly defined the WHS Director's roles and responsibilities based on the guidance in effect during the audit, we directed the recommendations to the Components and officials that can best implement them, and Finding B is specific to the waiver process and not records management.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation A.1

(U) We recommend that the Chief Digital and Artificial Intelligence Officer, in coordination with the Washington Headquarters Services Director, develop, resource, and implement a records management program that includes records management training for all personnel in accordance with Federal and DoD records management requirements.

(U) Chief Digital and Artificial Intelligence Office Comments

(U) The CDAO agreed, stating that they are working with the WHS to hire two records managers, initiate a staff assistance visit for program setup, and establish good governance and a records management plan by January 2025. The CDAO directed the DDS Director to implement a process to document and centrally manage all official records throughout the duration of a project by September 2024. The CDAO stated that records management training is mandatory for all CDAO employees and tracked through iCompass.[21]

[21] (U) iCompass is the learning management system for the OSD, the WHS, and the Pentagon Force Protection Agency. The WHS manages the iCompass system.

(U) Washington Headquarters Services Comments

(U) Although not required to comment, the WHS Director stated that the Chief of the OSD Records and Information Management Program, WHS, reached out to CDAO staff and provided them with a Records and Information Management Program development plan, an offer of staff assistance visits, and an estimate for the cost of contractor support to help CDAO budget for potential records management personnel. The WHS Director stated that CDAO staff had not yet responded to the Chief's outreach efforts.

(U) Our Response

(U) Comments from the CDAO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation when the CDAO provides documentation verifying the implementation of a records management program that meets Federal and DoD requirements.

(U) Recommendation A.2

(U) We recommend that the Chief Digital and Artificial Intelligence Officer implement a formal after-action review process to determine the success and effectiveness of the Defense Digital Services' engagements.

(U) Chief Digital and Artificial Intelligence Office Comments

(U) The CDAO agreed, stating that for every project, no matter the size or duration, the DDS completes an after-action report. The CDAO added that the after-action report includes important details and decisions, lessons learned, best practices, deliverables, and impact that is provided to CDAO leadership and validated by the CDAO Executive Director to ensure completeness and accuracy.

(U) Our Response

(U) Comments from the CDAO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CDAO provides documentation verifying that an after-action process was implemented to include submitting at least one completed after-action review report with evidence that it was provided to CDAO leadership and validated by the CDAO Executive Director.

(U) Recommendation A.3

(U) We recommend that the Washington Headquarters Services Director ensure that each head of a Washington Headquarters Services-serviced Component has established and resourced a records and information management program within their organization in accordance with DoD policies.

(U) Washington Headquarters Services Comments

(U) The WHS Director disagreed, stating that requiring the WHS Director to ensure that records management programs are established and resourced is not executable or within the Director's authorities. The Director stated that WHS has the authority to assess if WHS-serviced Components have a records management program, and whether the program is resourced and compliant with AI 15 requirements, DoD regulations, and Federal law. However, the Director stated that they cannot "force" WHS-serviced Components to establish and resource a program. The Director requested that we revise the recommendation to direct it to the OSD Principal Staff Assistants and DoD Component Heads supported by the WHS and that the WHS could then assess and report on their compliance status.

(U) Our Response

(U) Comments from the WHS Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. The WHS Director acknowledged that the WHS has the authority to assess whether a WHS-serviced Component has established and resourced a records management program that complies with Federal and DoD policies; however, WHS had not assessed whether DDS had established and resourced a program. AI 15 requires that the WHS Chief, RDD, ESD, "institutes and oversees a records management evaluation program to **ensure** [emphasis added] the WHS-serviced Components' compliance with [AI 15] and the OSD Records and Information Management Program Primer."[22] The Instruction requires the Chief, RDD to provide a written report of compliance or non-compliance, including results, finding, and recommendations to the WHS-serviced Component within 60-days of the evaluation. Any WHS-serviced Component found non-compliant is required to develop a plan of actions and milestones and submit quarterly reports to the Chief, RDD, ESD, until all findings and recommendations are closed.

(U) Therefore, the WHS Director's statement that the WHS cannot ensure the WHS-serviced Components have established and resourced a records management program is inconsistent with the responsibilities assigned to the WHS in AI 15. We request that the WHS Director provide comments within 30 days of the final report that include actions to address the recommendation.

[22] (U) AI 15, "OSD Records and Information Management Program," November 27, 2023, and OSD, "Records and Information Management Primer," December 14, 2023. The primer provides in-depth guidance to WHS-serviced Components on the implementation and compliance of Federal law, regulations, and DoD Records and Information Management directives and issuances.

(U) Finding B

(U) DDS Directors Exceeded the Authorities Granted in the DDS Charter

~~(CUI)~~ We substantiated the January 2023 allegation to the DoD Hotline that DDS officials relied on waivers they granted themselves in violation of the DDS Charter and used unauthorized information technology tools and services in violation of DoD policy. Specifically, two former DDS Directors exceeded their authority and granted waivers of multiple DoD policies to enable the DDS to use unauthorized digital service tools, including cloud-based software development platforms and collaboration software, to store, process, and transmit controlled unclassified information (CUI).[23] Although the DDS Charter authorizes the DDS Director to request waivers to DoD policies that would otherwise impede DDS engagements, the DDS Charter requires the DDS Director to request and receive approval for the waivers from the DoD Components that issued the policies. Instead of requesting waivers from the DoD Components, the former DDS Directors drafted and signed their own waivers without seeking the required approval. Furthermore, we determined that one of the former DDS Directors exceeded their authority and violated DoD policies when they improperly approved an Authority to Operate (ATO) that authorized the use of [redacted] a text messaging application, for discussions including CUI and the storage and processing of CUI on systems and environments in support of the [redacted][24] The DDS Directors violated DoD policy because, in granting authorities to the DDS Director, the OSD did not establish effective internal controls to ensure that the DDS Director exercised the authorities as intended. As a result, DDS and other DoD officials were able to disregard the cybersecurity requirements of seven DoD policies and use multiple unauthorized digital service tools to store, process, and transmit CUI, putting DoD information at additional risk of compromise.

[23] (U) Digital service tools are services provided by third-party companies for digital services such as Internet hosting, software development, and data storage. CUI is information the U.S. Government creates or possesses, or that an entity creates or possesses for or on behalf of the U.S. Government, that a law, regulation, or U.S. Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

[24] (U) The authorizing official is a senior official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations. An ATO is the written authorization from the authorizing official accepting risk to organizational operations, assets, individuals, other organizations, or the Nation and allowing operation of the information system. To obtain an ATO, DoD Components must conduct a risk assessment, identify risks to the system, and implement security controls for identifying and mitigating those risks.

(U) DDS Directors Waived DoD Policies Without DoD Component Approval

(U) Two former DDS Directors exceeded their authority and granted themselves waivers to DoD policy, instead of requesting and receiving approval for the waivers from the DoD Component that issued the policy. The DDS Charter grants the DDS Director the authority to request waivers of DoD regulations, directives, instructions, or other policies from the OSD Principal Staff Assistant or DoD Component head who issued the policy.[25] DDS officials provided copies of three waivers on DDS letterhead, dated between 2017 and 2020, and signed by former DDS Directors. However, the waivers were not approved or countersigned by any of the OSD Principal Staff Assistants or DoD Component heads responsible for the policies waived. The DDS Directors improperly granted themselves waivers to the following versions of DoD policies to enable the DDS to use unauthorized digital tools and services.[26]

- (U) DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019. The Instruction prohibits the use of non–DoD-controlled electronic messaging services to process non-public DoD information and the use of personal, non-official electronic messaging accounts to conduct official DoD business.[27]
- (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (Incorporating Change 1, October 7, 2019). The Instruction establishes cybersecurity programs to protect and defend DoD information and information technology and discusses key positions such as authorizing officials and senior information security officers.
- (U) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014 (Incorporating Change 2, July 28, 2017). The Instruction establishes the decision structure for cybersecurity risk management (the RMF) for DoD information technology systems, assigns responsibilities, and sets out procedures for executing and maintaining the RMF.

[25] (U) If the OSD Principal Staff Assistant or DoD Component head denies a waiver request, they must submit documentation for the basis of the denial to the Secretary of Defense or Deputy Secretary of Defense for a final decision. On February 1, 2022, after the realignment of the DDS under the CDAO, the Deputy Secretary of Defense extended the authorization to request waivers to the CDAO in the "Initial Operating Capability of the Chief Digital and Artificial Intelligence Officer" memorandum.

[26] (U) The versions of the policies listed are the versions included on the waivers.

[27] (U) DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 1993 (Incorporating Change 7, November 17, 2011), defines non-public information as information generally not available to the public, obtained during one's official DoD duties or position, which would normally not be releasable under the Freedom of Information Act, section 552, title 5, United States Code (2020). The term "non-public information" includes "inside information," "proprietary information," and "source selection information."

- ~~(CUI)~~ [redacted][28]
- (U) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016 (Incorporating Change 1, July 25, 2017). The Instruction establishes policy and assigns responsibilities to protect the Department of Defense Information Network against unauthorized activity, vulnerabilities, or threats.
- ~~(CUI)~~ [redacted]
- (U) "DoD Cloud Computing Security Requirements Guide," Version 1, Release 2, March 25, 2016, and Release 3, March 6, 2017. The Guide defines the security requirements for use and implementation of DoD or commercial cloud services by DoD mission owners.

(U) When we asked why the former DDS Directors did not follow the waiver-request process as required in the DDS Charter, the DDS legal counsel stated that the DDS' waiver authority was essentially established by precedent when the first DDS Director issued the first waiver and then continued when the next DDS Director issued two similar waivers. We make a recommendation to address this matter in the section titled, "The Office of the Secretary of Defense Did Not Establish Controls Over the DDS."

(U) By self-granting waivers of DoD policies, such as the cybersecurity requirements of the "DoD Cloud Computing Security Requirements Guide," the DDS Directors authorized the DDS to use digital and cloud service tools that were not authorized for use in the DoD. The waivers they granted themselves included lists of digital and cloud service tools that the DDS used to process and host CUI for engagements. However, some of the tools and services listed were not authorized for use in the DoD or were not authorized to store, process, and transmit CUI. For example, as of January 2022, to protect the CUI that is stored, processed,

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

(U) or transmitted in a cloud service, the DoD Cloud Computing Security Requirements Guide requires the cloud service to be authorized at Defense Information Systems Agency (DISA) Impact Level 4 (IL-4)/Federal Risk and Authorization Management Program (FedRAMP) High.[29] DDS officials acknowledged in the waivers that CUI must be minimally stored in cloud service offerings that meet DISA and FedRAMP security requirements, yet they used digital and cloud services that were not authorized for CUI. Table 2 illustrates the DoD's authorization level and the DDS' stated use of some of their most used digital and cloud services tools.

(U) Table 2. DoD Authorized Use and DDS' Use of Digital Service Tools

~~(CUI)~~ Cloud Service	DoD Authorized Use	DDS Use	DoD Approved Exception
[redacted]	Unclassified Information	CUI	No
[redacted]	Not Authorized	CUI	No
[redacted]	Not Authorized	CUI	No
[redacted]	CUI	CUI	N/A
[redacted]	Not Authorized	CUI	No
[redacted]	Unclassified Information	CUI	No ~~(CUI)~~

(U) Source: The DoD OIG.

(U) On September 28, 2023, the CDAO appointed a Chief Information Officer and Authorizing Official to assess and determine cybersecurity risk using a risk-based authorization process that addresses all applicable Federal, DoD, cybersecurity, and resiliency policies and requirements. Since their appointment, the CDAO Chief Information Officer and Authorizing Official has initiated an audit of all CDAO information technology assets, including hardware, software, digital service tools, and capabilities, used by the CDAO. Therefore, the CDAO Chief Information Officer and Authorizing Official, in coordination with the DISA Chief Information Officer, should conduct assessments to determine:

[29] (U) DISA is responsible for granting the DoD's authorizations for commercial cloud service offerings at four information impact levels based on the criticality and sensitivity of the data stored, processed, or transmitted within a cloud. The four impact levels are IL-2 (lowest), IL-4, IL-5, and IL-6 (highest). DISA's impact levels are similar but not identical to the FedRAMP authorization levels. FedRAMP provides security authorizations for cloud service offerings for the U.S. Government. A commercial cloud service offering must be both DISA and FedRAMP authorized to be used with the DoD.

- (U) whether the hardware, software, cloud services, and other tools used by the DDS are necessary to meet their mission, approved for use by the DoD, comply with DoD policies, and were acquired under terms to ensure that DoD retains ownership of its data;
- (U) the DoD Component owner, the nature, and classification of the data stored, processed, or transmitted by the digital tools and cloud services used by the DDS;
- (U) whether the DoD data were and are properly protected in accordance with DoD cybersecurity and cloud security policies; and
- (U) whether any DoD data were spilled, compromised, or potentially compromised, and if so, immediately initiate mitigating and remedial actions to protect DoD information, including personally identifiable information, in accordance with DoD policies.

(U) In addition, the CDAO should develop and implement a plan of actions and milestones to bring any out of compliance hardware, software, cloud services, networks, and other tools used by the DDS and other CDAO Components into compliance with DoD policies.

(U) The DDS Director Granted an Authority to Operate for Another DoD Component

~~(CUI)~~ We determined that one of the former DDS Directors exceeded their authority and violated DoD policies when they approved an ATO that authorized the use of [redacted][30] DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," March 12, 2014 (Incorporating Change 3, December 29, 2020) states that all DoD information technology systems must go through the RMF process, which indicates that the authorizing official has determined that the risk of operating the system is acceptable before granting an ATO.[31] The Instruction states that DoD and OSD Component heads must ensure that a trained and qualified authorizing official is appointed, in writing, for all DoD information systems operating on behalf of the DoD Component. The Instruction also states that the authorizing official accepts the system-related security risks that may impact organizational operations and assets, individuals, other organizations, or the Nation. In addition, DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, (Incorporating Change 1, October 7, 2019) states

[30] ~~(CUI)~~ The nature of these systems is classified. [redacted] is a text messaging, video, and voice-calling application for use on mobile devices.

[31] (U) On July 19, 2022, the Office of the DoD Chief Information Officer issued a revised version of DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," with the same requirements.

~~(CUI)~~ that the authorizing official renders authorization decisions for DoD information systems under the authorizing official's purview as they formally assume responsibility for operating DoD information systems, hardware, or software at an acceptable level of risk to organizational operations and assets.

~~(CUI)~~ The former DDS Director violated the requirements prescribed in DoD Instructions 8510.01 and 8500.01 by issuing an ATO when they had not been appointed in writing as an authorizing official for the [redacted].[32] In addition, the former DDS Director and Chief of Staff were not aware of the ATO, and the former DDS Chief of Staff stated that they believed that DDS officials had provided only technical support to [redacted] and that the DDS' role did not require an ATO. DDS officials were unaware of the existence of the ATO because the former DDS Director who granted the ATO did not maintain records regarding the ATO.

~~(CUI)~~ Furthermore, the former DDS Director who granted the ATO included in it an authorization for DoD personnel to use the unauthorized messaging application, [redacted] to discuss CUI information in violation of DoD electronic messaging policy. The ATO also required that users configure the messaging application to delete messages automatically [redacted] in violation the Federal and DoD records retention policy requirements to retain official DoD business for a minimum of 7 years. On November 21, 2022, in response to a recommendation we made in the "Management Advisory: The DoD's Use of Mobile Applications," the successor DDS Director issued a memorandum immediately withdrawing the ATO issued by the former DDS Director and provided documentation showing that [redacted] and [redacted] officials were informed of the withdrawal.[33]

(U) The Office of the Secretary of Defense Did Not Establish Controls Over the DDS

(U) DDS officials exceeded their authority because, in granting the authorities to the DDS Director, the OSD did not establish effective internal controls to ensure that the DDS Director exercised the authorities as intended. Due to this lack of oversight, the precedent of using unauthorized digital services by improperly waiving DoD policies continued when the DDS was incorporated into the CDAO. At the time of this report, the DDS continues to use software and cloud services in violation of DoD cybersecurity and cloud security policies. Therefore, the CDAO should develop a clear, formal process for all CDAO directorates to follow when requesting waivers of DoD policies and guidance that, at a minimum, documents

[32] ~~(CUI)~~ The [redacted] is the authorizing official for the [redacted].

[33] (U) See Appendix B for additional information on the management advisory issued during this audit.

(U) the request, the justification for the request, and the approval or denial from the DoD Component that issued the policy. In addition, the process should include steps to ensure that if the waiver request is denied by the DoD Component head who issued the policy, but the OSD overrides the denial and approves the waiver, the DDS Director informs the issuing DoD Component of the approved waiver in writing. Finally, the CDAO should implement Recommendations B.1, B.2, and B.3 for all the CDAO directorates.

(U) The DDS Exposed DoD Information to Additional Cybersecurity Risk and Risk of Compromise

(U) The DoD establishes cybersecurity policies and procedures to protect U.S. interests and the DoD's operational capabilities, individuals, organizations, and assets. By improperly waiving cybersecurity and cloud security requirements and protections, the DDS Directors exposed DoD information to additional cybersecurity risk and increased the risk of compromise.

(U) The DDS has used unauthorized digital and cloud service tools to store, process, and transmit CUI since 2015, with no oversight or official assessment and acceptance of risk. Without a cybersecurity risk assessment of the digital and cloud service tools, the DoD cannot properly mitigate the risks and protect DoD information from compromise, corruption, or theft. Furthermore, by allowing additional CDAO Components to use the unauthorized tools and services, there is an increased risk that DoD information may be compromised or exposed.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation B.1

(U) We recommend that the Chief Digital and Artificial Intelligence Office Chief Information Officer and Authorizing Official, in coordination with the Defense Information Systems Agency Chief Information Officer, assess the hardware, software, cloud services, networks, and any other tools used by the Defense Digital Service since 2015 to determine whether the hardware, software, cloud services, and other tools:

a. **(U) are necessary to meet the mission requirements of the Defense Digital Service;**

b. **(U) are approved for use by the DoD;**

c. **(U) comply with the DoD policy requirements, including, but not limited to:**

   i. **(U) DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019 (Incorporating Change 1, August 24, 2021);**

   ii. **(U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (Incorporating Change 1, October 7, 2019);**

   iii. **(U) DoD Instruction 8510.01, "Risk Management Framework," (July 19, 2022);**

   iv. **~~(CUI)~~** [redacted]

   v. **(U) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016 (Incorporating Change 1, July 25, 2017);**

   vi. **~~(CUI)~~** [redacted] **and**

   vii. **(U) "DoD Cloud Computing Security Requirements Guide," Version 1, Release 4, January 14, 2022.**

d. **(U) were acquired under terms that ensure that the DoD retains ownership of DoD data.**

(U) Chief Digital and Artificial Intelligence Office Comments

(U) The CDAO, responding for the CDAO Chief Information Officer and Authorizing Official, agreed, stating that they had directed the CDAO Authorizing Official to conduct a review of the tools currently in use and advise which tools may be deprecated, restricted, or removed from use.

(U) Defense Information Systems Agency Comments

(U) Although not required to comment, the DISA Chief Information Officer stated that DISA will support the CDAO in their efforts to determine if hardware, software, cloud services, networks, and any other tools used by the DDS were approved or provisionally authorized by DISA for DOD use. The DISA Chief Information Officer stated that DISA cannot be responsible for performing analysis of all tools identified by the CDAO to determine their compliance with the identified policies, determining whether any of identified tools were necessary to meet DDS mission requirements, or verifying that any terms or conditions in DDS acquisitions ensured that DOD retained ownership of its data. DISA further recommends that the OSD Chief Information Officer, as the Department's Chief Information Officer with organizational oversight for CDAO, provide support to the CDAO in their efforts to address the recommendation.

(U) Our Response

(U) Comments from the CDAO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. The CDAO should assess all the digital service tools it has used since 2015 to determine if DoD data was properly protected, if any DoD data remains on the servers of the tools, and if any DoD data is now owned by the tools under the terms of the contract. We request that the CDAO provide comments within 30 days of the final report that include actions to address the recommendation.

(U) Recommendation B.2

(U) We recommend that the Chief Digital and Artificial Intelligence Office Chief Information Officer and Authorizing Official, in coordination with the Defense Information Systems Agency Chief Information Officer, conduct a risk assessment of the DoD data stored, processed, or transmitted by the hardware, software, cloud services, networks, and any other tools used by the Defense Digital Service to determine:

a. **(U) the DoD Component owner, the nature, and classification of the data;**

b. **(U) whether the DoD data were and are appropriately protected in accordance with DoD cybersecurity and cloud security policies; and**

c. **(U) whether any DoD data were spilled, compromised, or potentially compromised, and if so, immediately initiate mitigating and remedial actions to protect DoD information, including personally identifiable information, in accordance with DoD policies.**

(U) Chief Digital and Artificial Intelligence Office Comments

(U) The CDAO, responding for the CDAO Chief Information Officer and Authorizing Official, agreed, stating that the recommendations will be considered when the hardware, software, cloud services, networks, and any other tools used by DDS undergo the ATO process. The CDAO directed the CDAO Director of Cyber Assurance, who also serves as the CDAO Authorizing Official, to review all new hardware, software, cloud services, networks, and any other tools used by the DDS prior to their use.

(U) Defense Information Systems Agency Comments

(U) Although not required to comment, the DISA Chief Information Officer stated that DISA cannot perform any of the analysis outlined in the recommendation, but DISA will, at the request of the CDAO, provide advice and assistance to the extent it is able. The DISA Chief Information Officer further recommended that the OSD Chief Information Officer, as the Department's Chief Information Officer with organizational oversight for the CDAO, provide support to the CDAO in their efforts to address the recommendation.

(U) Our Response

(U) Comments from the CDAO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. It is important that the CDAO conducts the risk assessment for DoD data stored in any digital service tool immediately to ensure the protection of DoD data, rather than wait for the ATO process, which is generally reauthorized every 3 years after the initial ATO is granted. Therefore, we request that the CDAO provide comments within 30 days of the final report that include actions to address the recommendation.

(U) Recommendation B.3

(U) We recommend that after completion of Recommendations B.1 and B.2, the Chief Digital and Artificial Intelligence Officer develop and implement a plan of actions and milestones to bring any out-of-compliance hardware, software, cloud services, networks, and other tools used by the Defense Digital Service and other Office of the Chief Digital and Artificial Intelligence Office Components into compliance with DoD policies.

(U) Chief Digital and Artificial Intelligence Office Comments

(U) The CDAO agreed and directed the DDS Director to work with the Deputy CDAO for Acquisition and the CDAO Director for Cyber Assurance to provide the CDAO with a plan of action and milestones to bring non-compliant hardware, software, cloud services, networks, and other tools used by all CDAO Components, including the DDS, into compliance with DoD policies by September 2024.

(U) Our Response

(U) Comments from the CDAO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation when the CDAO provides documentation of the plan of actions and milestone to bring any out-of-compliance hardware, software, cloud service, networks, or other tools identified as during the assessments conducted as part of B.1 and B.2 were brought into compliance with DoD policies.

(U) Recommendation B.4

(U) We recommend that the Chief Digital and Artificial Intelligence Officer develop and implement a formal process for all Chief Digital and Artificial Intelligence Office directorates to follow when requesting waivers of DoD policies and guidance that, at a minimum, requires:

a. **(U) documentation of the request, justification for the request, and the approval or denial from the policy's issuing DoD Component;**

b. **(U) documentation of the Office of the Secretary of Defense's approval and notification in writing to the policy's issuing DoD Component of the approval of the waiver, if the Office of the Secretary of Defense overrides the denial of the waiver by the Office of the Secretary of Defense Principal Staff Assistant or DoD Component head who issued the policy; and**

c. **(U) maintenance of the documentation created as a result of the implementation of Recommendations B.1.a and B.1.b in accordance with Federal and DoD records management requirements.**

(U) Chief Digital and Artificial Intelligence Office Comments

(U) The CDAO agreed, stating that when the CDAO was established, the authority for the waiver request process was transitioned from the DDS Director to the CDAO. The CDAO stated that all CDAO Directorates will follow the CDAO's process, which is overseen by the CDAO Authorizing Official, to request, document, and implement any policy waiver requests. The CDAO also directed all CDAO Directorates at the Deputy CDAO- and Principal Deputy Director-level to be briefed on the policy waiver request process to ensure compliance with this guidance by May 31, 2024.

(U) Our Response

(U) Comments from the CDAO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation when the CDAO provides documentation verifying that it has an established waiver requires process.

(U) Recommendation B.5

(U) We recommend that the Chief Digital and Artificial Intelligence Officer implement Recommendations B.1, B.2, and B.3 for all the Chief Digital and Artificial Intelligence Office directorates.

(U) Chief Digital and Artificial Intelligence Office Comments

(U) The CDAO agreed, stating that they will implement the recommendations for the other directorates.

(U) Our Response

(U) Comments from the CDAO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CDAO provides a plan of actions and milestones for implementing Recommendations B.1, B.2, and B3 for all the CDAO directorates.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from August 2021 through February 2024 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) On July 7, 2022, while conducting this audit, we responded to a congressional inquiry specific to a DDS engagement concerning millions of dormant Internet Protocol version 4 (IPv4) addresses. During the audit, we also identified concerns with the DoD's use of mobile devices and applications and issued a management advisory on February 9, 2023, addressing those concerns. Please see Appendix B for more information on the congressional inquiry and management advisory.

(U) To determine whether the DDS engagements achieved their intended purpose and were executed in accordance with Federal and DoD policies, we interviewed DDS officials to understand the purpose of the engagements and how the DDS measures their success. We also interviewed DDS officials to determine how the DDS planned, executed, and transferred the engagements to DoD Components. We interviewed DoD Component officials who were supported by the DDS to assess their communication with the DDS during the engagements and any reporting requirements. Specifically, we interviewed officials from the following DoD Components and programs.

- (U) Office of the Under Secretary of Defense for Personnel and Readiness
- (U) Office of the Under Secretary of Defense for Intelligence and Security
- (U) U.S. Cyber Command
- (U) U.S. Central Command
- (U) U.S. Africa Command
- (U) U.S. Army – Army Cyber Command
- (U) U.S. Army – Program Executive Office Simulation, Training and Instrumentation
- (U) U.S. Army – Threat Systems Management Office
- (U) U.S Navy – Naval Information Warfare Systems Command

- (U) U.S. Air Force – Office of the Assistant Secretary of the Air Force (Acquisition, Technology, and Logistics)
- (U) Defense Intelligence Agency
- (U) Defense Logistics Agency
- (U) Defense Counterintelligence and Security Agency
- (U) Defense Health Agency
- (U) National Cyber Security Operations Center

(U) We received a list of DDS engagements from the DDS, from November 2015 to July 2021, and conducted a data call with DoD Components to obtain a list of personnel who worked on the DDS engagements.[34] We identified 92 DDS engagements and removed four engagements from the universe.

- (U) One engagement was represented twice for the unclassified and classified components of the project.
- (U) Two engagements were the subject of a prior audit review.
- (U) One engagement was required to be reviewed as part of this audit; therefore, it was removed from the universe before sample selection and then was added to the final sample.

(U) To identify our sample for additional assessments, we grouped the remaining 88 engagements based on the DDS Engagement Category and DDS Strategic Priority and non-statistically selected 12 engagements to review, including the required engagement. We determined that one engagement was too early in the project for us to determine whether it achieved its intended purpose and was executed in accordance with DoD and Federal policies and one project was self-initiated and later abandoned by the DDS; therefore, we removed these projects from the sample. Table 3 details the sample of 10 engagements grouped by DDS Engagement Category and DDS Strategic Priority.

(U) Table 3. Sample Grouped by DDS Engagement Category and DoD Strategic Priority

(U) DDS Engagement Category	DDS Strategic Priority	Universe	Sample
Discovery Sprints	Force Protection	4	1
Discovery Sprints	Secure Systems	19	1
Discover Sprints	Near Peer	1	0
Projects	Force Protection	12	2 (U)

[34] (U) The list of DDS projects and attributes was not pulled from an information system. DDS personnel manually compiled the list into a spreadsheet.

(U) Table 3. Sample Grouped by DDS Engagement Category and DoD Strategic Priority (cont'd)

(U) DDS Engagement Category	DDS Strategic Priority	Universe	Sample
Projects	Near Peer	1	1
Projects	Secure Systems	24	2
Rapid Response	Rapid Response	21	2
Tech Navigators	Secure Systems	6	1
	Total	**88**	**10** **(U)**

(U) Source: The DoD OIG.

(U) The nonstatistical sample is not representative of the population all the DDS engagements; therefore, any findings regarding the sampled engagements cannot be projected to the population of DDS engagements. Table 4 identifies the DDS engagements included within our audit scope.

(U) Table 4. DDS Engagements Reviewed

~~(CUI)~~ Engagement Category	Strategic Priority	DDS Engagement
Discovery Sprint	Force Protection	[redacted]
	Secure Systems	[redacted]
Projects	Force Protection	[redacted]
	Force Protection	[redacted]
	Secure Systems	[redacted]
	Secure Systems	[redacted]
	Near-Peer	[redacted]
Rapid Response	Rapid Response	[redacted]
	Rapid Response	[redacted]
Tech Navigators	Secure Systems	[redacted] **~~(CUI)~~**

(U) Source: The DoD OIG.

(U) In addition, we reviewed DDS and DoD Component documentation about the engagements. Specifically, we requested and reviewed copies of memorandums of agreement or understanding, policy waivers, contracts, and security classification guides related to the DDS engagements.

(U) To determine whether the DDS met DoD records management requirements, we reviewed applicable Federal and DoD policies related to adequate and proper documentation and records management program requirements. In addition, we interviewed officials from the WHS to understand their responsibilities for oversight of DDS records management program.

(U) To determine whether the former DDS Directors exceeded their authority, we reviewed the authorities granted in the DDS Charter. We initially requested the DDS officials' emails for review to determine whether the former Secretary of Defense granted DDS officials additional authorities and responsibilities not outlined in DoD Directive 5105.87. On January 3, 2022, DISA officials informed us that a former DDS Director's unclassified emails were not retained after 120 days after the former DDS Director left the DoD in 2021.[35] As a result, our review of DDS officials' unclassified emails did not include the former Director's emails between January 2020 and November 2021.

(U) We reviewed applicable DoD policies related to the risk management framework and cybersecurity. We also reviewed the DDS policy waivers to identify the DoD regulations, directives, instructions, or other policies that the DDS Directors waived. We analyzed the digital service tools and services listed in the waivers to determine whether they were authorized for use in the DoD.

(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) Internal Control Assessment and Compliance

(U) We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed whether the engagements conducted by the DDS achieved their intended purpose and were executed in accordance with DoD and Federal policies. However, because our

[35] (U) According to DISA officials, the former DDS Director's email account was not designated to be "journaled." DISA recommends establishing journaled email accounts for high-ranking and other designated individuals whose email may contain official records that are subject to legal and regulatory requirements. DISA retains all emails and attachments sent to and from journaled email accounts for 10 years. However, the organization that requests the email account must determine whether the account should be journaled.

(U) 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

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

(U) Use of Technical Assistance

(U) We received assistance from the DoD OIG Quantitative Methods Division to select a nonstatistical sample of DDS engagements for review. We requested an updated list of engagements from the DDS during our meeting on July 29, 2021. The DDS sent a list with 86 unclassified engagements and 6 classified engagements. The DDS broke the engagements into five different categories—Portfolios, Projects, Rapid Response, Discovery Sprints, and Tech Navigators. Quantitative Methods Division personnel selected a nonstatistical sample of engagements.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) and the DoD Office of Inspector General (DoD OIG) have issued one review and one investigation related to the DDS or DDS engagements. Unrestricted GAO reports can be accessed at http://www.gao.gov, and unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

(U) GAO

(U) Report No. GAO-21-319, "Operation Warp Speed: Accelerated COVID-19 Development Status and efforts to Address Manufacturing Challenges," February 2021

> (U) The GAO determined that Operation Warp Speed and vaccine companies adopted several strategies to accelerate vaccine development and mitigate risk. The GAO found that the technology readiness levels of Operation Warp Speed's vaccine candidates showed that COVID-19 vaccine development under Operation Warp Speed entirely followed traditional practices, with some adaptations. Some vaccine companies relied on data from other vaccines using the same platforms, where available, or conducted certain animal studies at the same time as clinical trials. Operation Warp Speed reported that as of January 31, 2021, companies had released 63.7 million doses, which is about 32 percent of the contracted amount companies with Emergency Use Authorization must provide by March 31, 2021.

(U) DoD OIG

(U) Report No. DODIG-2021-092, "Report of Investigation: Mr. Brett J. Goldstein, Defense Digital Service Director," June 21, 2021

> ~~(CUI)~~ The DoD OIG determined that the evidence it found did not support the allegations that Mr. Goldstein failed to treat subordinates with dignity and respect. In addition, the investigative team substantiated allegations that Mr. Goldstein used and condoned the use of [redacted] an unauthorized electronic messaging and voice-calling application.

(U) Appendix B

(U) Response to Congress

(U) On July 7, 2022, we sent a classified letter to Congress in response to concerns regarding the former DDS Director's authority to transfer 174 million DoD IPv4 addresses to a contractor as part of a DDS pilot project. We determined that the former DDS Director's actions did not violate DoD policy because they were granted broad authority to conduct work and initiate projects to identify and evaluate DoD cybersecurity vulnerabilities and deficiencies by DoD Directive 5105.87, "Director, Defense Digital Service."

(U) Management Advisory: The DoD's Use of Mobile Applications

(U) During the audit, we determined that the former DDS Director authorized the use of an unmanaged mobile application for official DoD business, in violation of DoD electronic messaging and records retention policies. The use of unmanaged applications to conduct official business poses operational and cybersecurity risks and could result in users inadvertently revealing sensitive DoD information or introducing malware to DoD information systems. Therefore, we expanded our review beyond the DDS to determine whether the misuse of unmanaged applications for official business on DoD mobile devices is a DoD enterprise-wide concern.

(U) On February 9, 2023, we issued Report No. DODIG-2023-041, "Management Advisory: The DoD's Use of Mobile Applications." We determined that DoD Component personnel used unmanaged electronic messaging applications in violation of Federal and DoD electronic messaging and records retention policies. In addition, DoD Components:

- (U) allowed personnel to have unrestricted access to unauthorized unmanaged applications through public application stores that could pose operational and cybersecurity risks;
- (U) offered authorized unmanaged mobile applications through application stores that pose known operational and cybersecurity risks to DoD information and systems; and
- (U) lacked controls to ensure that personal use of DoD devices was limited and did not pose operational and cybersecurity risks to the DoD.

(U) The management advisory provided 16 recommendations for corrective action, that when complete, should limit the unjustified use of unmanaged applications on DoD mobile devices and reduce the associated risks. As of May 2024, 4 recommendations are closed; 10 recommendations are resolved but will remain open; and 2 are unresolved.[36]

[36] (U) The following categories are used to describe agency management's comments to individual recommendations:
Closed – The DoD OIG verified that the agreed upon corrective actions were implemented,

Resolved – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation, and

Unresolved – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.

(U) Appendix C

(U) DDS Engagement Categories

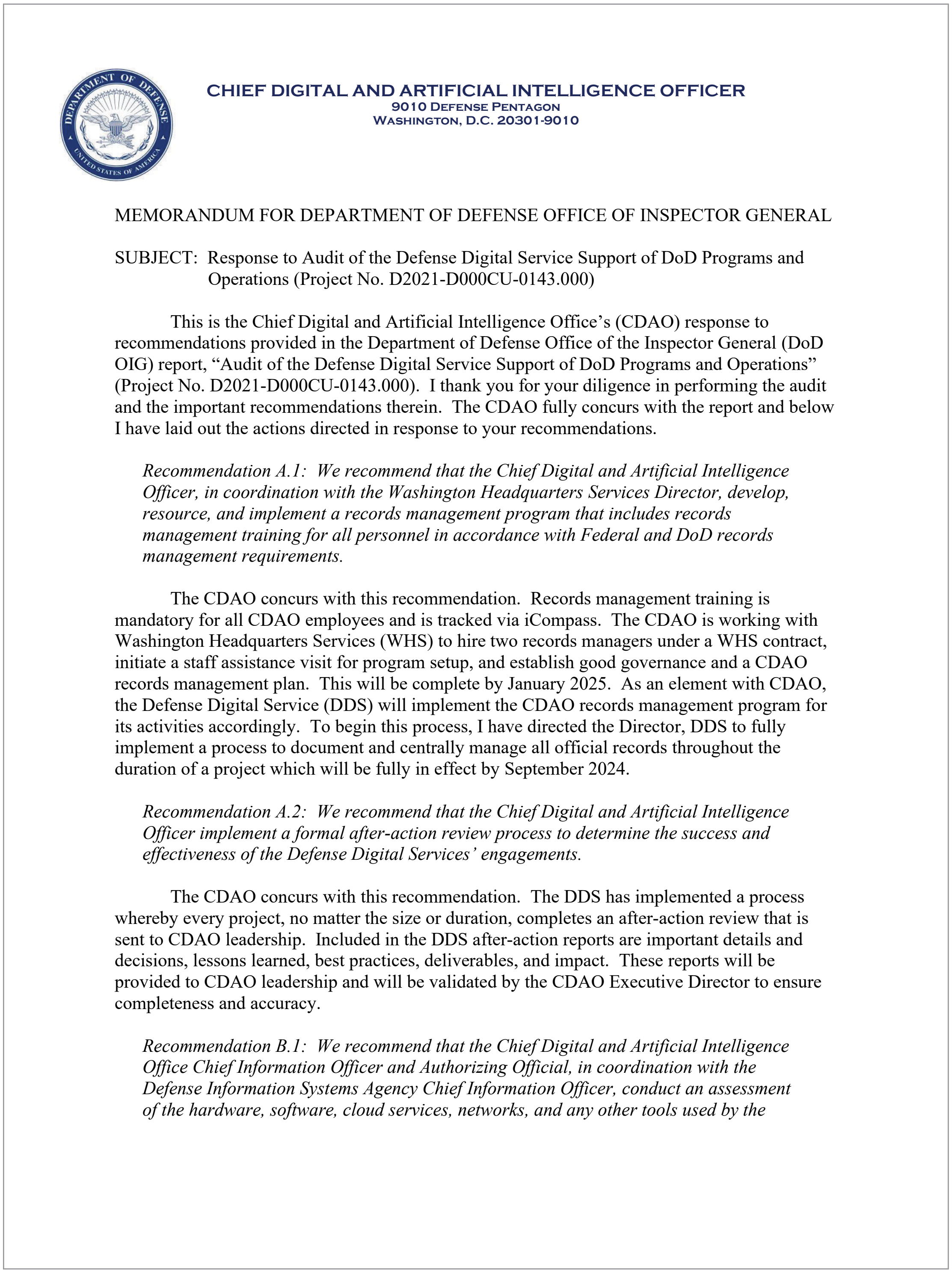
(U) After selection, the DDS placed engagements in five different categories.

- (U) Portfolios: The DDS has several long-term engagements that include Service-specific partnerships and efforts that the DDS is working on for program offices.[37]
- (U) Projects: The majority of engagements that the DDS takes on are discrete scopes of work to develop and deliver technology to solve a problem in the DoD. Project teams are staffed according to technical needs. Projects can span 6 months to a year to successfully transition technology back to the host organization.
- (U) Discovery Sprints: DoD organizations invite the DDS to send roughly four to six team members to spend up to a month observing their organizational and technical challenges. Discovery sprints end with an in-depth report outlining paths forward for the organization and can potentially lead to a DDS project.
- (U) Rapid Response: When a DoD organization faces a technical issue that cannot wait, the DDS issues an immediate response. These engagements end with a quick technical fix or a report that outlines the team's finding and presents possible paths forward.
- (U) Tech Navigators: DDS experts sometimes serve in advisory capacities to a DoD organization addressing a technology challenge. DDS roles can range from design sprint facilitation to best practice advocacy to technical engagement during a complex procurement, ensuring that high-caliber technical advice is available across the DoD.

[37] (U) Portfolios are groups of engagements that the DDS linked together; therefore, we did not consider them a separate group for the purposes of our sample.

(U) Management Comments

(U) Chief Digital and Artificial Intelligence Office



CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-9010

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

SUBJECT: Response to Audit of the Defense Digital Service Support of DoD Programs and Operations (Project No. D2021-D000CU-0143.000)

This is the Chief Digital and Artificial Intelligence Office's (CDAO) response to recommendations provided in the Department of Defense Office of the Inspector General (DoD OIG) report, "Audit of the Defense Digital Service Support of DoD Programs and Operations" (Project No. D2021-D000CU-0143.000). I thank you for your diligence in performing the audit and the important recommendations therein. The CDAO fully concurs with the report and below I have laid out the actions directed in response to your recommendations.

Recommendation A.1: We recommend that the Chief Digital and Artificial Intelligence Officer, in coordination with the Washington Headquarters Services Director, develop, resource, and implement a records management program that includes records management training for all personnel in accordance with Federal and DoD records management requirements.

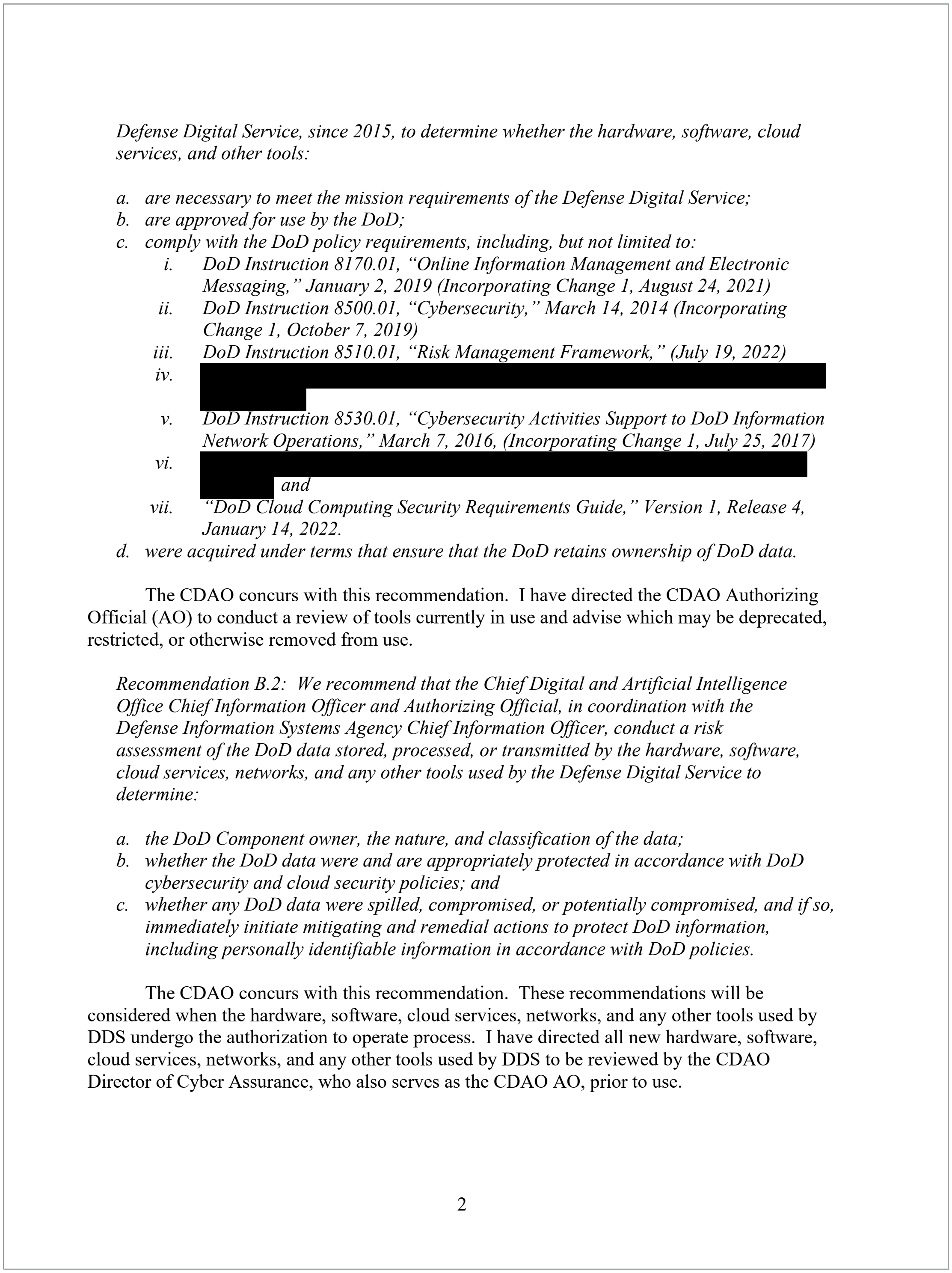
The CDAO concurs with this recommendation. Records management training is mandatory for all CDAO employees and is tracked via iCompass. The CDAO is working with Washington Headquarters Services (WHS) to hire two records managers under a WHS contract, initiate a staff assistance visit for program setup, and establish good governance and a CDAO records management plan. This will be complete by January 2025. As an element with CDAO, the Defense Digital Service (DDS) will implement the CDAO records management program for its activities accordingly. To begin this process, I have directed the Director, DDS to fully implement a process to document and centrally manage all official records throughout the duration of a project which will be fully in effect by September 2024.

Recommendation A.2: We recommend that the Chief Digital and Artificial Intelligence Officer implement a formal after-action review process to determine the success and effectiveness of the Defense Digital Services' engagements.

The CDAO concurs with this recommendation. The DDS has implemented a process whereby every project, no matter the size or duration, completes an after-action review that is sent to CDAO leadership. Included in the DDS after-action reports are important details and decisions, lessons learned, best practices, deliverables, and impact. These reports will be provided to CDAO leadership and will be validated by the CDAO Executive Director to ensure completeness and accuracy.

Recommendation B.1: We recommend that the Chief Digital and Artificial Intelligence Office Chief Information Officer and Authorizing Official, in coordination with the Defense Information Systems Agency Chief Information Officer, conduct an assessment of the hardware, software, cloud services, networks, and any other tools used by the

(U) Chief Digital and Artificial Intelligence Office (cont'd)



Defense Digital Service, since 2015, to determine whether the hardware, software, cloud services, and other tools:

a. are necessary to meet the mission requirements of the Defense Digital Service;
b. are approved for use by the DoD;
c. comply with the DoD policy requirements, including, but not limited to:
i. DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019 (Incorporating Change 1, August 24, 2021)
ii. DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (Incorporating Change 1, October 7, 2019)
iii. DoD Instruction 8510.01, "Risk Management Framework," (July 19, 2022)
iv. [redacted]
v. DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, (Incorporating Change 1, July 25, 2017)
vi. [redacted] *and*
vii. "DoD Cloud Computing Security Requirements Guide," Version 1, Release 4, January 14, 2022.
d. were acquired under terms that ensure that the DoD retains ownership of DoD data.

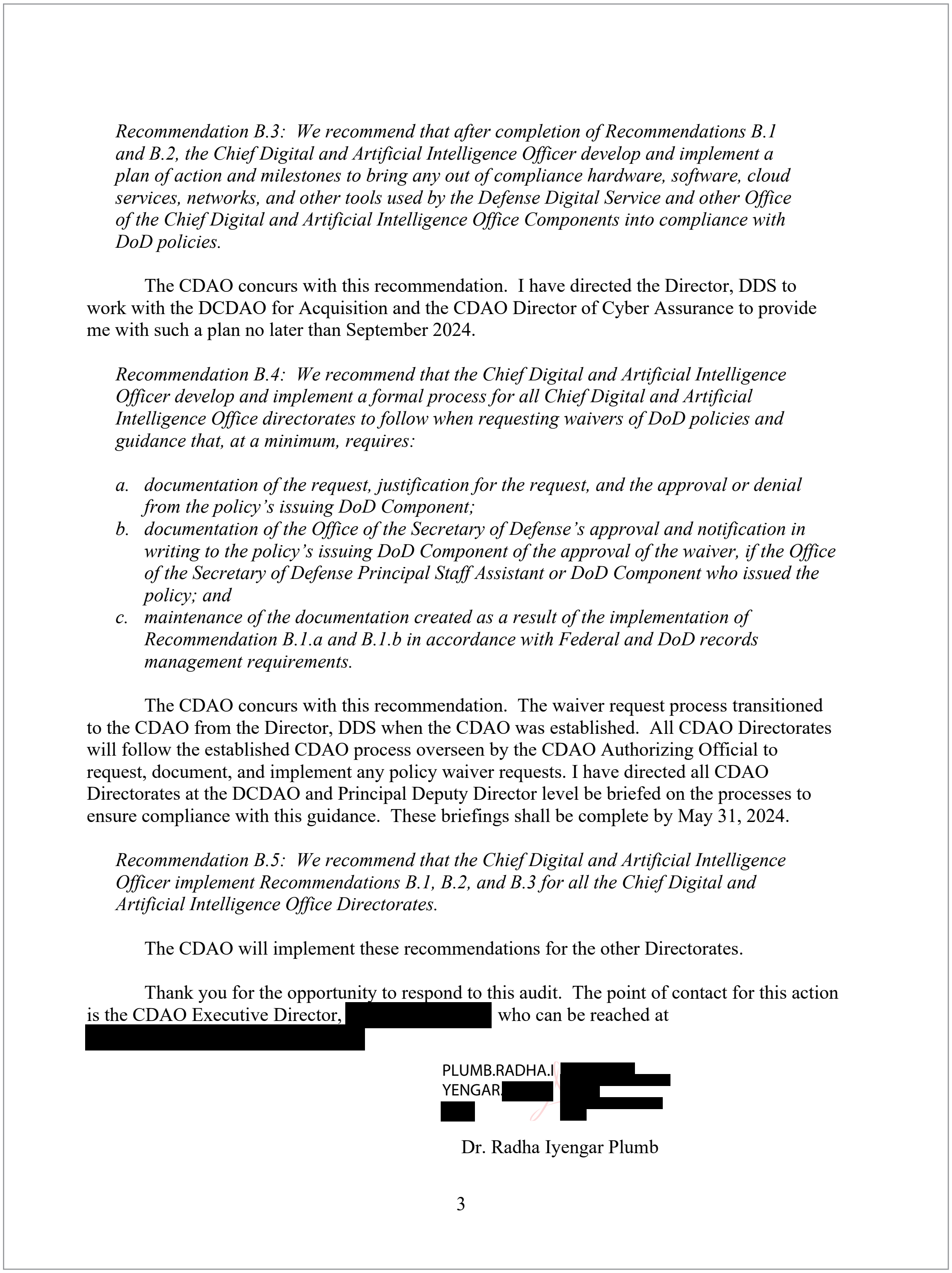
The CDAO concurs with this recommendation. I have directed the CDAO Authorizing Official (AO) to conduct a review of tools currently in use and advise which may be deprecated, restricted, or otherwise removed from use.

Recommendation B.2: We recommend that the Chief Digital and Artificial Intelligence Office Chief Information Officer and Authorizing Official, in coordination with the Defense Information Systems Agency Chief Information Officer, conduct a risk assessment of the DoD data stored, processed, or transmitted by the hardware, software, cloud services, networks, and any other tools used by the Defense Digital Service to determine:

a. the DoD Component owner, the nature, and classification of the data;
b. whether the DoD data were and are appropriately protected in accordance with DoD cybersecurity and cloud security policies; and
c. whether any DoD data were spilled, compromised, or potentially compromised, and if so, immediately initiate mitigating and remedial actions to protect DoD information, including personally identifiable information in accordance with DoD policies.

The CDAO concurs with this recommendation. These recommendations will be considered when the hardware, software, cloud services, networks, and any other tools used by DDS undergo the authorization to operate process. I have directed all new hardware, software, cloud services, networks, and any other tools used by DDS to be reviewed by the CDAO Director of Cyber Assurance, who also serves as the CDAO AO, prior to use.

(U) Chief Digital and Artificial Intelligence Office (cont'd)



Recommendation B.3: We recommend that after completion of Recommendations B.1 and B.2, the Chief Digital and Artificial Intelligence Officer develop and implement a plan of action and milestones to bring any out of compliance hardware, software, cloud services, networks, and other tools used by the Defense Digital Service and other Office of the Chief Digital and Artificial Intelligence Office Components into compliance with DoD policies.

The CDAO concurs with this recommendation. I have directed the Director, DDS to work with the DCDAO for Acquisition and the CDAO Director of Cyber Assurance to provide me with such a plan no later than September 2024.

Recommendation B.4: We recommend that the Chief Digital and Artificial Intelligence Officer develop and implement a formal process for all Chief Digital and Artificial Intelligence Office directorates to follow when requesting waivers of DoD policies and guidance that, at a minimum, requires:

a. documentation of the request, justification for the request, and the approval or denial from the policy's issuing DoD Component;
b. documentation of the Office of the Secretary of Defense's approval and notification in writing to the policy's issuing DoD Component of the approval of the waiver, if the Office of the Secretary of Defense Principal Staff Assistant or DoD Component who issued the policy; and
c. maintenance of the documentation created as a result of the implementation of Recommendation B.1.a and B.1.b in accordance with Federal and DoD records management requirements.

The CDAO concurs with this recommendation. The waiver request process transitioned to the CDAO from the Director, DDS when the CDAO was established. All CDAO Directorates will follow the established CDAO process overseen by the CDAO Authorizing Official to request, document, and implement any policy waiver requests. I have directed all CDAO Directorates at the DCDAO and Principal Deputy Director level be briefed on the processes to ensure compliance with this guidance. These briefings shall be complete by May 31, 2024.

Recommendation B.5: We recommend that the Chief Digital and Artificial Intelligence Officer implement Recommendations B.1, B.2, and B.3 for all the Chief Digital and Artificial Intelligence Office Directorates.

The CDAO will implement these recommendations for the other Directorates.

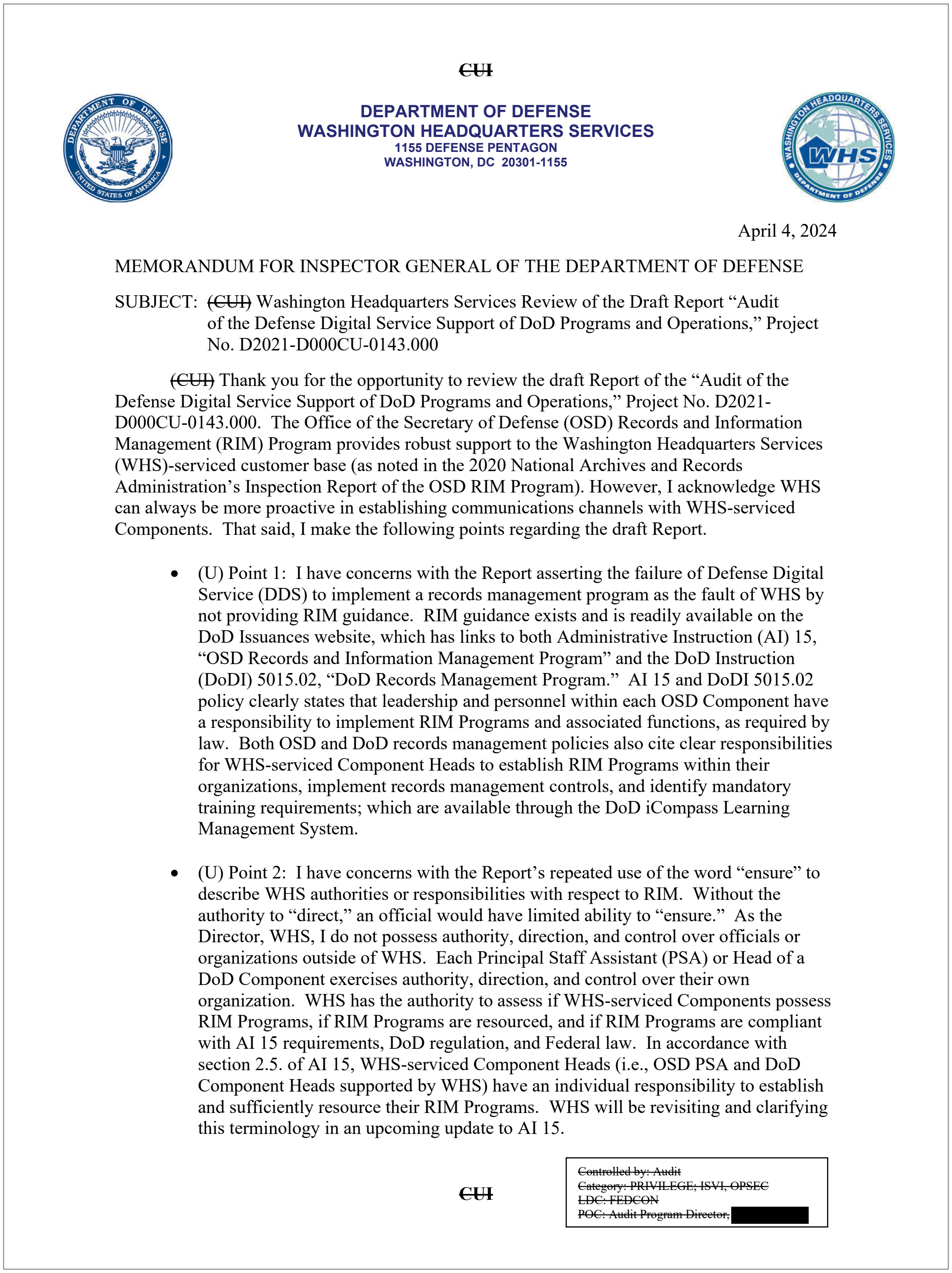
Thank you for the opportunity to respond to this audit. The point of contact for this action is the CDAO Executive Director, [redacted] who can be reached at [redacted]

PLUMB.RADHA.I[redacted]
YENGAR[redacted]
[redacted]

Dr. Radha Iyengar Plumb

3

(U) Washington Headquarters Services



~~CUI~~

DEPARTMENT OF DEFENSE
WASHINGTON HEADQUARTERS SERVICES
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

April 4, 2024

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: ~~(CUI)~~ Washington Headquarters Services Review of the Draft Report "Audit of the Defense Digital Service Support of DoD Programs and Operations," Project No. D2021-D000CU-0143.000

~~(CUI)~~ Thank you for the opportunity to review the draft Report of the "Audit of the Defense Digital Service Support of DoD Programs and Operations," Project No. D2021-D000CU-0143.000. The Office of the Secretary of Defense (OSD) Records and Information Management (RIM) Program provides robust support to the Washington Headquarters Services (WHS)-serviced customer base (as noted in the 2020 National Archives and Records Administration's Inspection Report of the OSD RIM Program). However, I acknowledge WHS can always be more proactive in establishing communications channels with WHS-serviced Components. That said, I make the following points regarding the draft Report.

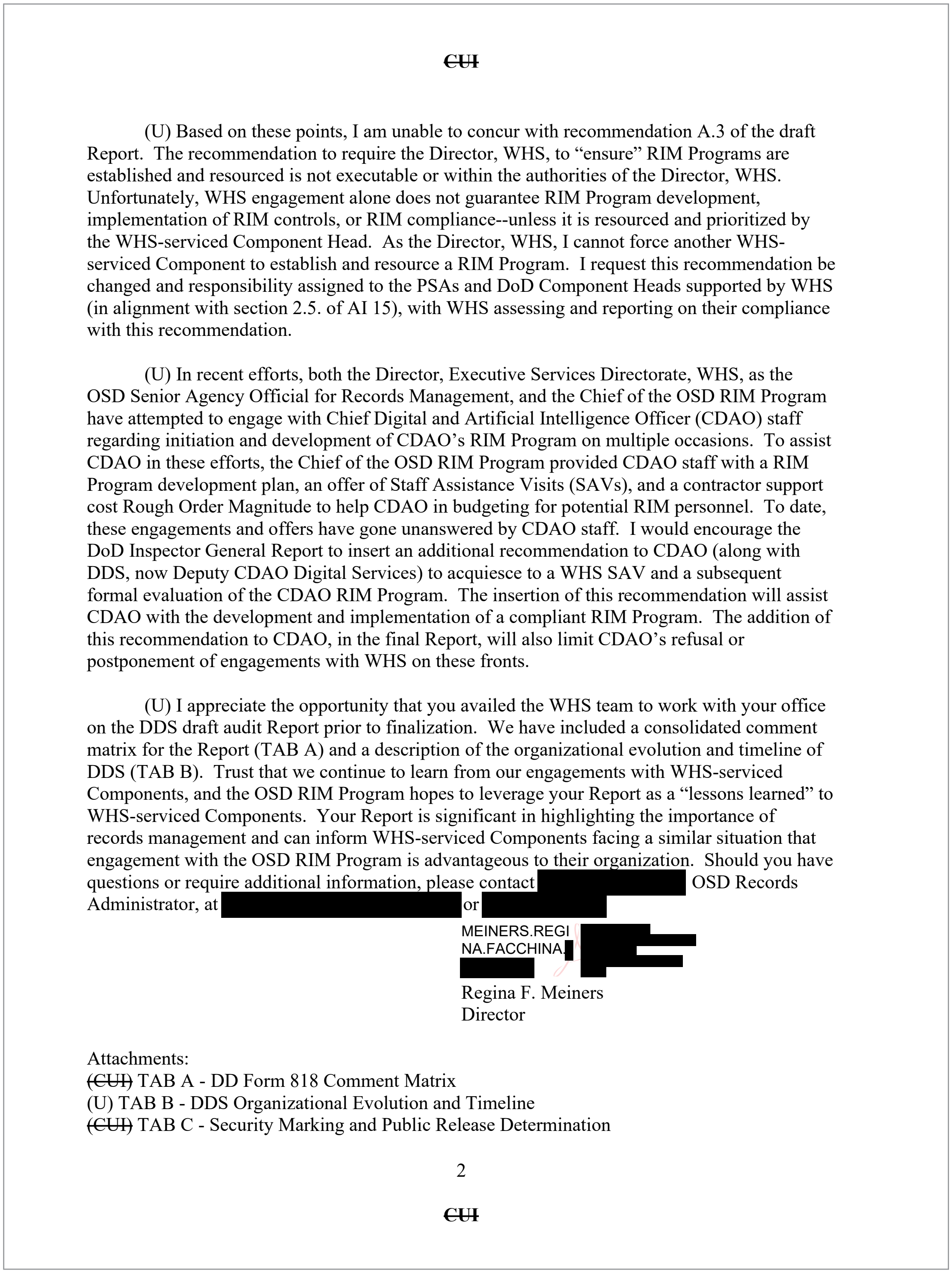
- (U) Point 1: I have concerns with the Report asserting the failure of Defense Digital Service (DDS) to implement a records management program as the fault of WHS by not providing RIM guidance. RIM guidance exists and is readily available on the DoD Issuances website, which has links to both Administrative Instruction (AI) 15, "OSD Records and Information Management Program" and the DoD Instruction (DoDI) 5015.02, "DoD Records Management Program." AI 15 and DoDI 5015.02 policy clearly states that leadership and personnel within each OSD Component have a responsibility to implement RIM Programs and associated functions, as required by law. Both OSD and DoD records management policies also cite clear responsibilities for WHS-serviced Component Heads to establish RIM Programs within their organizations, implement records management controls, and identify mandatory training requirements; which are available through the DoD iCompass Learning Management System.

- (U) Point 2: I have concerns with the Report's repeated use of the word "ensure" to describe WHS authorities or responsibilities with respect to RIM. Without the authority to "direct," an official would have limited ability to "ensure." As the Director, WHS, I do not possess authority, direction, and control over officials or organizations outside of WHS. Each Principal Staff Assistant (PSA) or Head of a DoD Component exercises authority, direction, and control over their own organization. WHS has the authority to assess if WHS-serviced Components possess RIM Programs, if RIM Programs are resourced, and if RIM Programs are compliant with AI 15 requirements, DoD regulation, and Federal law. In accordance with section 2.5. of AI 15, WHS-serviced Component Heads (i.e., OSD PSA and DoD Component Heads supported by WHS) have an individual responsibility to establish and sufficiently resource their RIM Programs. WHS will be revisiting and clarifying this terminology in an upcoming update to AI 15.

~~Controlled by: Audit~~
~~Category: PRIVILEGE; ISVI, OPSEC~~
~~LDC: FEDCON~~
~~POC: Audit Program Director,~~ [redacted]

~~CUI~~

(U) Washington Headquarters Services (cont'd)



~~CUI~~

(U) Based on these points, I am unable to concur with recommendation A.3 of the draft Report. The recommendation to require the Director, WHS, to "ensure" RIM Programs are established and resourced is not executable or within the authorities of the Director, WHS. Unfortunately, WHS engagement alone does not guarantee RIM Program development, implementation of RIM controls, or RIM compliance--unless it is resourced and prioritized by the WHS-serviced Component Head. As the Director, WHS, I cannot force another WHS-serviced Component to establish and resource a RIM Program. I request this recommendation be changed and responsibility assigned to the PSAs and DoD Component Heads supported by WHS (in alignment with section 2.5. of AI 15), with WHS assessing and reporting on their compliance with this recommendation.

(U) In recent efforts, both the Director, Executive Services Directorate, WHS, as the OSD Senior Agency Official for Records Management, and the Chief of the OSD RIM Program have attempted to engage with Chief Digital and Artificial Intelligence Officer (CDAO) staff regarding initiation and development of CDAO's RIM Program on multiple occasions. To assist CDAO in these efforts, the Chief of the OSD RIM Program provided CDAO staff with a RIM Program development plan, an offer of Staff Assistance Visits (SAVs), and a contractor support cost Rough Order Magnitude to help CDAO in budgeting for potential RIM personnel. To date, these engagements and offers have gone unanswered by CDAO staff. I would encourage the DoD Inspector General Report to insert an additional recommendation to CDAO (along with DDS, now Deputy CDAO Digital Services) to acquiesce to a WHS SAV and a subsequent formal evaluation of the CDAO RIM Program. The insertion of this recommendation will assist CDAO with the development and implementation of a compliant RIM Program. The addition of this recommendation to CDAO, in the final Report, will also limit CDAO's refusal or postponement of engagements with WHS on these fronts.

(U) I appreciate the opportunity that you availed the WHS team to work with your office on the DDS draft audit Report prior to finalization. We have included a consolidated comment matrix for the Report (TAB A) and a description of the organizational evolution and timeline of DDS (TAB B). Trust that we continue to learn from our engagements with WHS-serviced Components, and the OSD RIM Program hopes to leverage your Report as a "lessons learned" to WHS-serviced Components. Your Report is significant in highlighting the importance of records management and can inform WHS-serviced Components facing a similar situation that engagement with the OSD RIM Program is advantageous to their organization. Should you have questions or require additional information, please contact [redacted] OSD Records Administrator, at [redacted] or [redacted]

MEINERS.REGI
NA.FACCHINA.[redacted]
[redacted] [redacted]

Regina F. Meiners
Director

Attachments:
~~(CUI)~~ TAB A - DD Form 818 Comment Matrix
(U) TAB B - DDS Organizational Evolution and Timeline
~~(CUI)~~ TAB C - Security Marking and Public Release Determination

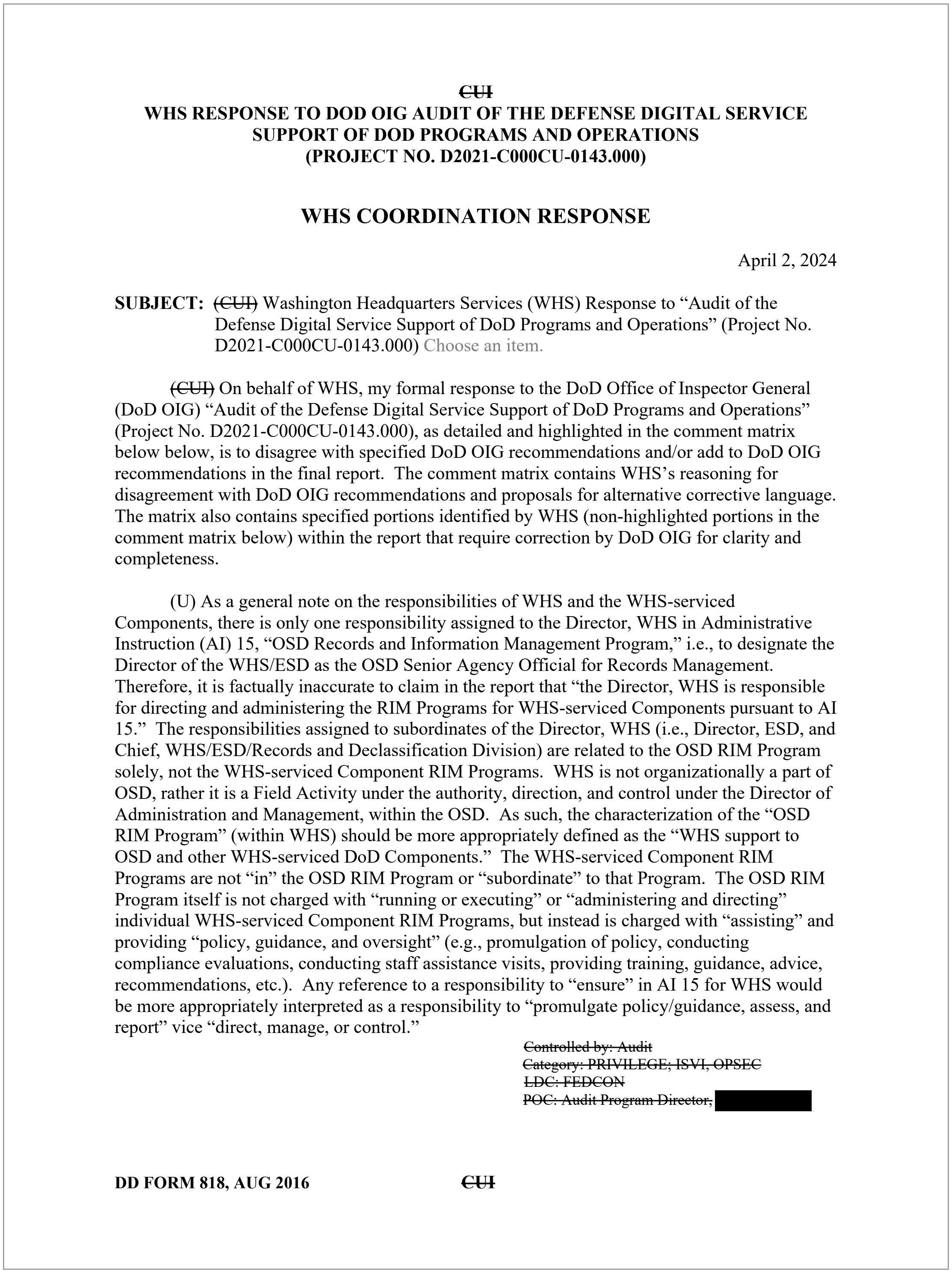
2

~~CUI~~

Omitted Tab A and B because of length.

Copies provided upon request.

(U) Washington Headquarters Services (cont'd)



~~CUI~~
WHS RESPONSE TO DOD OIG AUDIT OF THE DEFENSE DIGITAL SERVICE SUPPORT OF DOD PROGRAMS AND OPERATIONS (PROJECT NO. D2021-C000CU-0143.000)

WHS COORDINATION RESPONSE

April 2, 2024

SUBJECT: ~~(CUI)~~ Washington Headquarters Services (WHS) Response to "Audit of the Defense Digital Service Support of DoD Programs and Operations" (Project No. D2021-C000CU-0143.000) Choose an item.

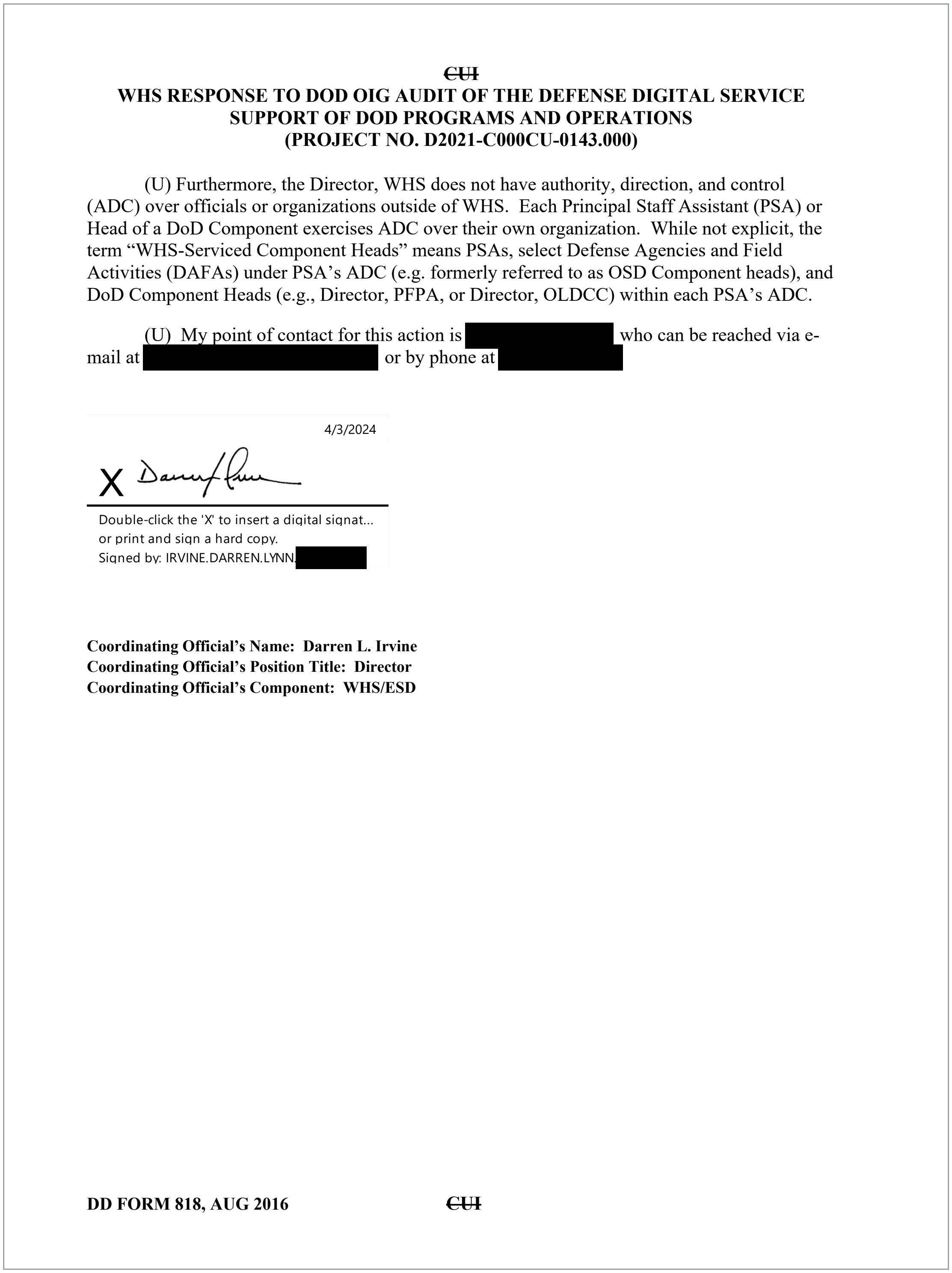
~~(CUI)~~ On behalf of WHS, my formal response to the DoD Office of Inspector General (DoD OIG) "Audit of the Defense Digital Service Support of DoD Programs and Operations" (Project No. D2021-C000CU-0143.000), as detailed and highlighted in the comment matrix below below, is to disagree with specified DoD OIG recommendations and/or add to DoD OIG recommendations in the final report. The comment matrix contains WHS's reasoning for disagreement with DoD OIG recommendations and proposals for alternative corrective language. The matrix also contains specified portions identified by WHS (non-highlighted portions in the comment matrix below) within the report that require correction by DoD OIG for clarity and completeness.

(U) As a general note on the responsibilities of WHS and the WHS-serviced Components, there is only one responsibility assigned to the Director, WHS in Administrative Instruction (AI) 15, "OSD Records and Information Management Program," i.e., to designate the Director of the WHS/ESD as the OSD Senior Agency Official for Records Management. Therefore, it is factually inaccurate to claim in the report that "the Director, WHS is responsible for directing and administering the RIM Programs for WHS-serviced Components pursuant to AI 15." The responsibilities assigned to subordinates of the Director, WHS (i.e., Director, ESD, and Chief, WHS/ESD/Records and Declassification Division) are related to the OSD RIM Program solely, not the WHS-serviced Component RIM Programs. WHS is not organizationally a part of OSD, rather it is a Field Activity under the authority, direction, and control under the Director of Administration and Management, within the OSD. As such, the characterization of the "OSD RIM Program" (within WHS) should be more appropriately defined as the "WHS support to OSD and other WHS-serviced DoD Components." The WHS-serviced Component RIM Programs are not "in" the OSD RIM Program or "subordinate" to that Program. The OSD RIM Program itself is not charged with "running or executing" or "administering and directing" individual WHS-serviced Component RIM Programs, but instead is charged with "assisting" and providing "policy, guidance, and oversight" (e.g., promulgation of policy, conducting compliance evaluations, conducting staff assistance visits, providing training, guidance, advice, recommendations, etc.). Any reference to a responsibility to "ensure" in AI 15 for WHS would be more appropriately interpreted as a responsibility to "promulgate policy/guidance, assess, and report" vice "direct, manage, or control."

~~Controlled by: Audit~~
~~Category: PRIVILEGE; ISVI, OPSEC~~
~~LDC: FEDCON~~
~~POC: Audit Program Director,~~ [redacted]

DD FORM 818, AUG 2016 ~~CUI~~

(U) Washington Headquarters Services (cont'd)



~~CUI~~

WHS RESPONSE TO DOD OIG AUDIT OF THE DEFENSE DIGITAL SERVICE SUPPORT OF DOD PROGRAMS AND OPERATIONS (PROJECT NO. D2021-C000CU-0143.000)

(U) Furthermore, the Director, WHS does not have authority, direction, and control (ADC) over officials or organizations outside of WHS. Each Principal Staff Assistant (PSA) or Head of a DoD Component exercises ADC over their own organization. While not explicit, the term "WHS-Serviced Component Heads" means PSAs, select Defense Agencies and Field Activities (DAFAs) under PSA's ADC (e.g. formerly referred to as OSD Component heads), and DoD Component Heads (e.g., Director, PFPA, or Director, OLDCC) within each PSA's ADC.

(U) My point of contact for this action is [redacted] who can be reached via e-mail at [redacted] or by phone at [redacted]

4/3/2024

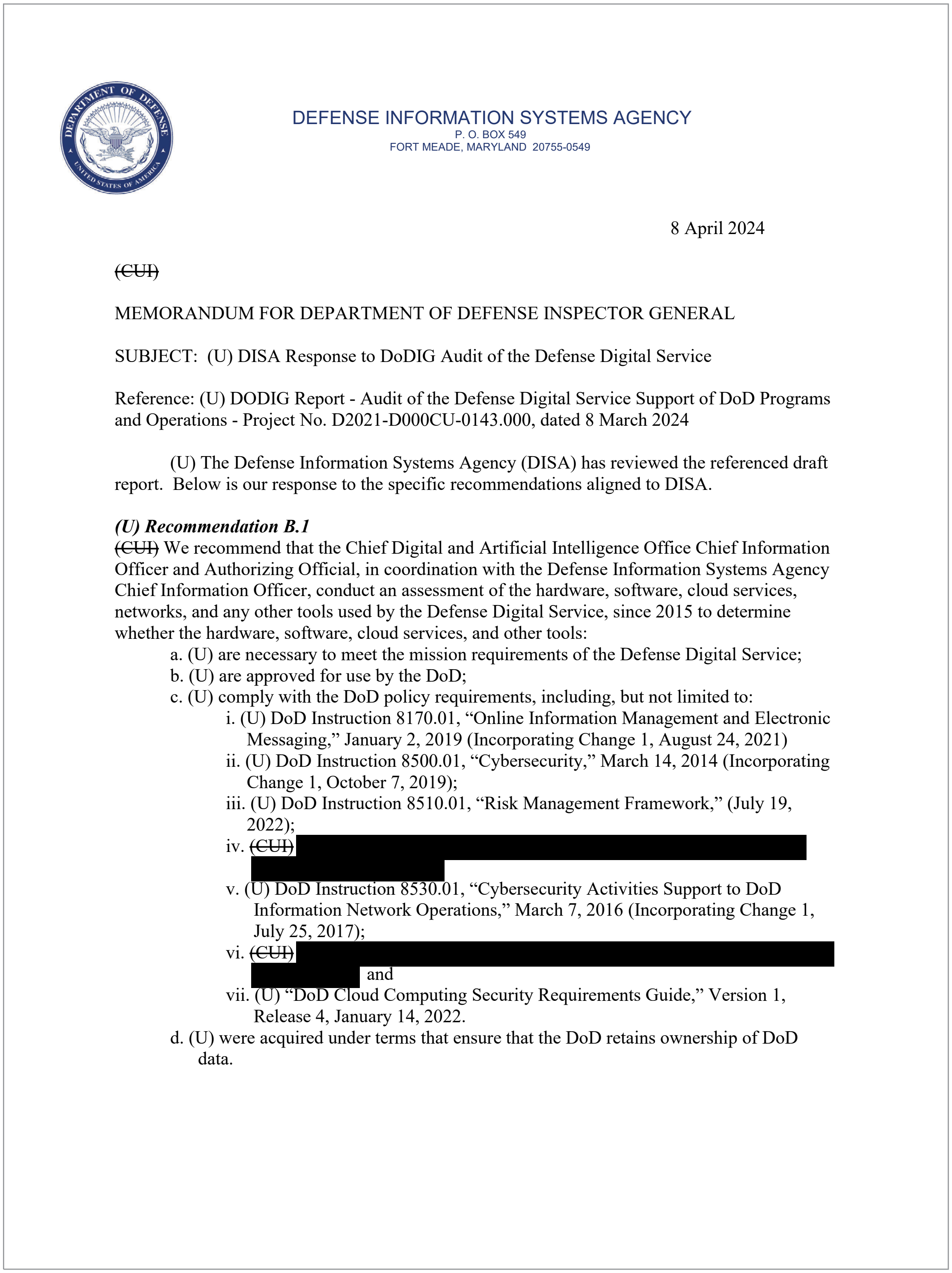
X

Double-click the 'X' to insert a digital signat...
or print and sign a hard copy.
Signed by: IRVINE.DARREN.LYNN.[redacted]

Coordinating Official's Name: Darren L. Irvine
Coordinating Official's Position Title: Director
Coordinating Official's Component: WHS/ESD

DD FORM 818, AUG 2016 ~~CUI~~

(U) Defense Information Systems Agency



DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

8 April 2024

~~(CUI)~~

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: (U) DISA Response to DoDIG Audit of the Defense Digital Service

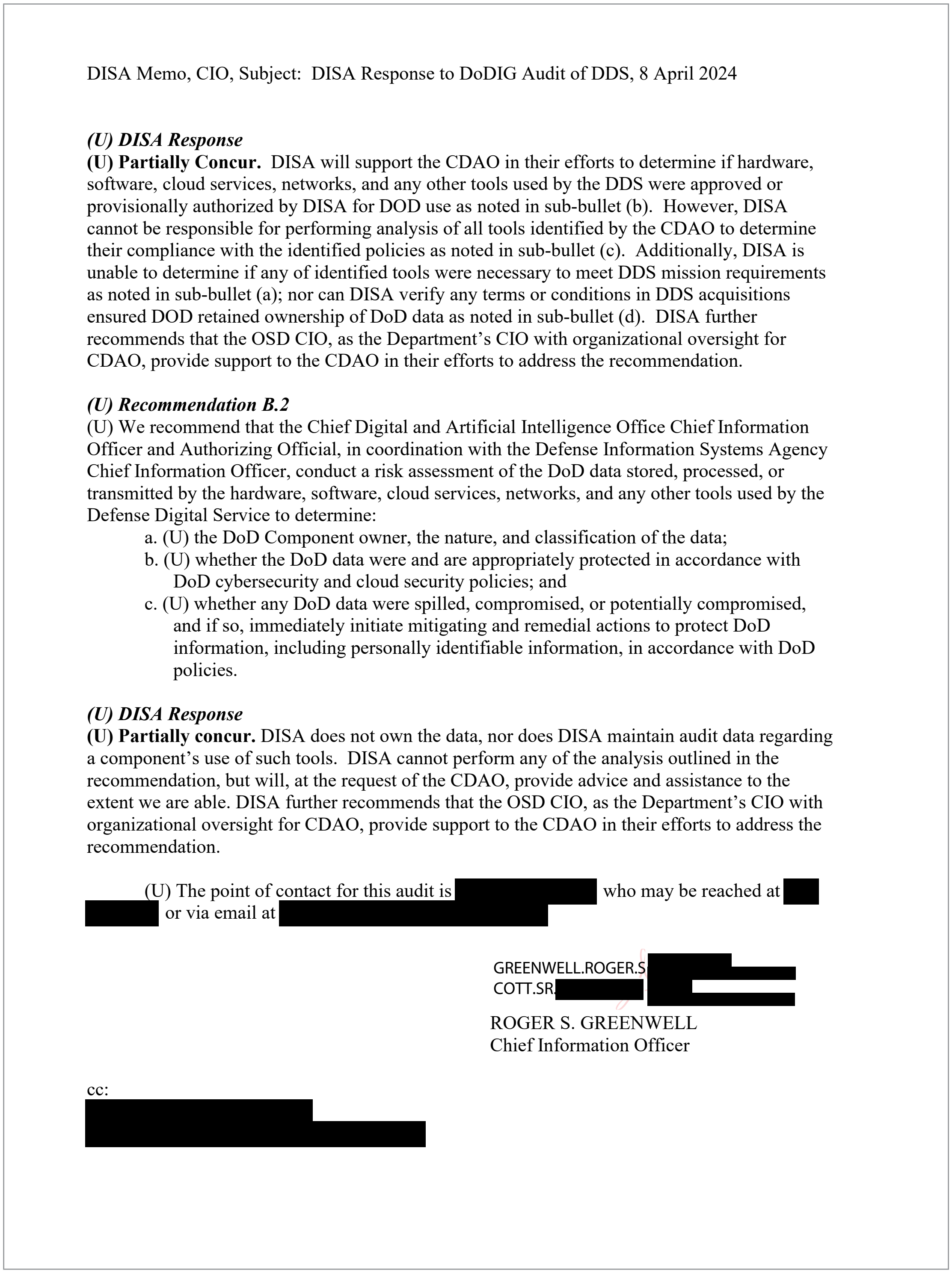
Reference: (U) DODIG Report - Audit of the Defense Digital Service Support of DoD Programs and Operations - Project No. D2021-D000CU-0143.000, dated 8 March 2024

(U) The Defense Information Systems Agency (DISA) has reviewed the referenced draft report. Below is our response to the specific recommendations aligned to DISA.

(U) Recommendation B.1
~~(CUI)~~ We recommend that the Chief Digital and Artificial Intelligence Office Chief Information Officer and Authorizing Official, in coordination with the Defense Information Systems Agency Chief Information Officer, conduct an assessment of the hardware, software, cloud services, networks, and any other tools used by the Defense Digital Service, since 2015 to determine whether the hardware, software, cloud services, and other tools:

a. (U) are necessary to meet the mission requirements of the Defense Digital Service;
b. (U) are approved for use by the DoD;
c. (U) comply with the DoD policy requirements, including, but not limited to:
  i. (U) DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019 (Incorporating Change 1, August 24, 2021)
  ii. (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (Incorporating Change 1, October 7, 2019);
  iii. (U) DoD Instruction 8510.01, "Risk Management Framework," (July 19, 2022);
  iv. ~~(CUI)~~ [redacted]
  v. (U) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016 (Incorporating Change 1, July 25, 2017);
  vi. ~~(CUI)~~ [redacted] and
  vii. (U) "DoD Cloud Computing Security Requirements Guide," Version 1, Release 4, January 14, 2022.
d. (U) were acquired under terms that ensure that the DoD retains ownership of DoD data.

(U) Defense Information Systems Agency (cont'd)



DISA Memo, CIO, Subject: DISA Response to DoDIG Audit of DDS, 8 April 2024

(U) DISA Response
(U) Partially Concur. DISA will support the CDAO in their efforts to determine if hardware, software, cloud services, networks, and any other tools used by the DDS were approved or provisionally authorized by DISA for DOD use as noted in sub-bullet (b). However, DISA cannot be responsible for performing analysis of all tools identified by the CDAO to determine their compliance with the identified policies as noted in sub-bullet (c). Additionally, DISA is unable to determine if any of identified tools were necessary to meet DDS mission requirements as noted in sub-bullet (a); nor can DISA verify any terms or conditions in DDS acquisitions ensured DOD retained ownership of DoD data as noted in sub-bullet (d). DISA further recommends that the OSD CIO, as the Department's CIO with organizational oversight for CDAO, provide support to the CDAO in their efforts to address the recommendation.

(U) Recommendation B.2
(U) We recommend that the Chief Digital and Artificial Intelligence Office Chief Information Officer and Authorizing Official, in coordination with the Defense Information Systems Agency Chief Information Officer, conduct a risk assessment of the DoD data stored, processed, or transmitted by the hardware, software, cloud services, networks, and any other tools used by the Defense Digital Service to determine:

a. (U) the DoD Component owner, the nature, and classification of the data;
b. (U) whether the DoD data were and are appropriately protected in accordance with DoD cybersecurity and cloud security policies; and
c. (U) whether any DoD data were spilled, compromised, or potentially compromised, and if so, immediately initiate mitigating and remedial actions to protect DoD information, including personally identifiable information, in accordance with DoD policies.

(U) DISA Response
(U) Partially concur. DISA does not own the data, nor does DISA maintain audit data regarding a component's use of such tools. DISA cannot perform any of the analysis outlined in the recommendation, but will, at the request of the CDAO, provide advice and assistance to the extent we are able. DISA further recommends that the OSD CIO, as the Department's CIO with organizational oversight for CDAO, provide support to the CDAO in their efforts to address the recommendation.

(U) The point of contact for this audit is [redacted] who may be reached at [redacted] [redacted] or via email at [redacted]

GREENWELL.ROGER.S[redacted]
COTT.SR[redacted]

ROGER S. GREENWELL
Chief Information Officer

cc:
[redacted]

(U) Acronyms and Abbreviations

~~(CUI)~~

AI	Administrative Instruction
ATO	Authority to Operate
CDAO	Chief Digital and Artificial Intelligence Office or Officer
COVID-19	Coronavirus Disease–2019
CUI	Controlled Unclassified Information
DDS	Defense Digital Service
DISA	Defense Information Systems Agency
[redacted]	[redacted]
ESD	Executive Services Directorate
FedRAMP	Federal Risk and Authorization Management Program
GAO	Government Accountability Office
IL	Impact Level
IPv4	Internet Protocol version 4
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
OSD	Office of the Secretary of Defense
RDD	Records and Privacy and Declassification Division
RMF	Risk Management Framework
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
WHS	Washington Headquarters Services

~~(CUI)~~

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

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 http://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:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

𝕏
www.twitter.com/DoD_IG

LinkedIn
https://www.linkedin.com/company/dod-inspector-general/

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