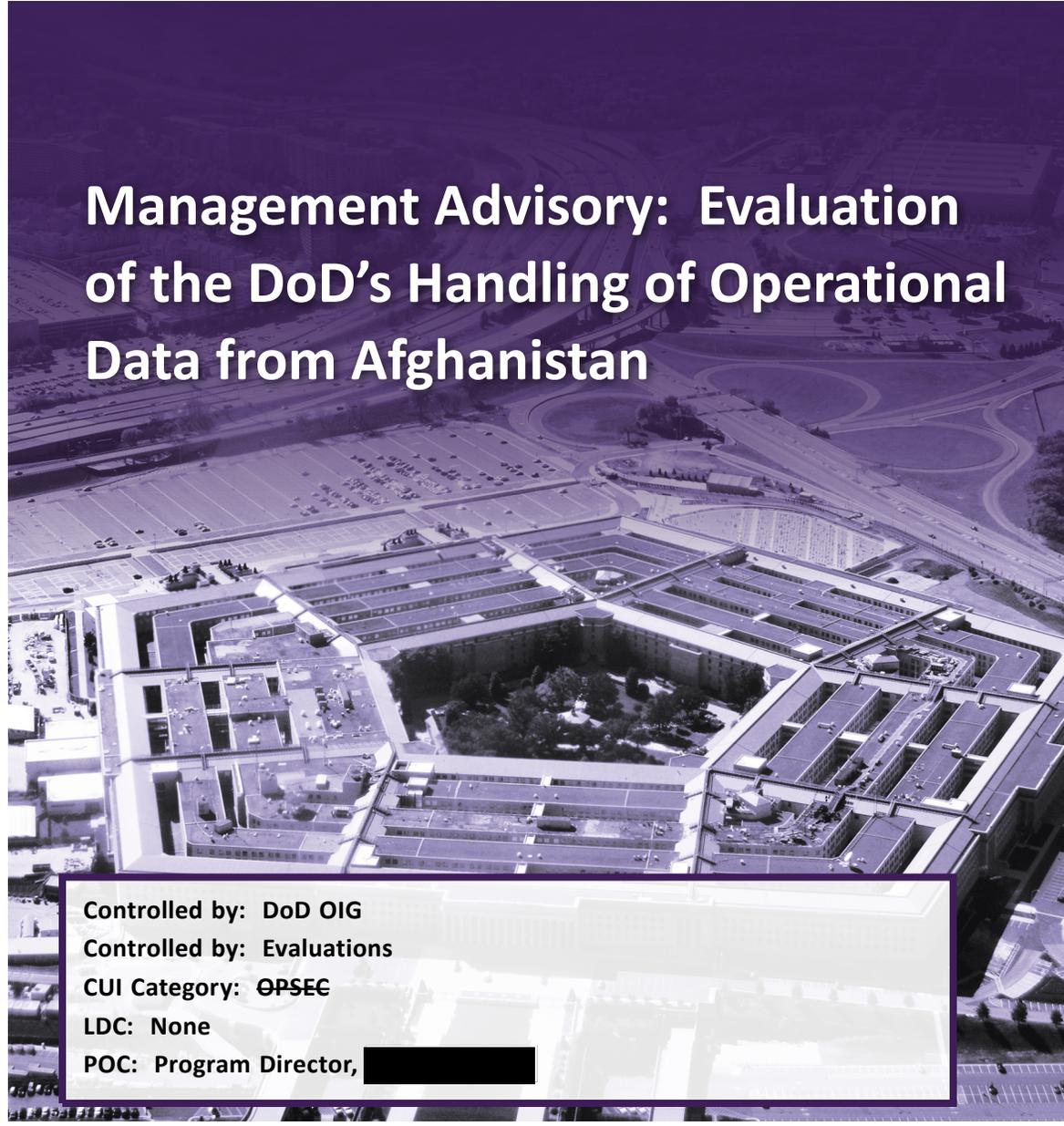


CUI

INSPECTOR GENERAL

U.S. Department of Defense

MAY 6, 2024



Management Advisory: Evaluation of the DoD's Handling of Operational Data from Afghanistan

Controlled by: DoD OIG
Controlled by: Evaluations
CUI Category: OPSEC
LDC: None
POC: Program Director, [REDACTED]

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

CUI





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

May 6, 2024

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR POLICY
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
AND SECURITY
CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE
COMMANDER, U.S. CENTRAL COMMAND
COMMANDER, U.S. SPECIAL OPERATIONS COMMAND

SUBJECT: Management Advisory: Evaluation of the DoD's Handling of Operational Data
from Afghanistan (Report No. DODIG-2024-079)

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

(U) The Deputy Secretary of Defense agreed with the recommendation presented in the report; therefore, we consider the recommendation resolved and open. We will close the recommendation when management officials provide documentation showing that all agreed-upon actions to implement the recommendation are completed. Therefore, please provide us within 90 days your response concerning specific actions in process or completed on the recommendations. Send your response to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET.

FOR THE INSPECTOR GENERAL:

A handwritten signature in black ink that reads "Bryan Clark".

Bryan Clark
Assistant Inspector General for Evaluations Programs,
Combatant Commands, and Operations

(U) Executive Summary

(U) The United States and its coalition partners began a campaign in Afghanistan following the September 11, 2001, terrorist attacks on the United States. U.S. forces departed Afghanistan on August 30, 2021. According to section 1088 of the FY 2022 National Defense Authorization Act (NDAA), a large amount of operational and intelligence data was generated during the war in Afghanistan.¹ Section 1088 directed the Secretary of Defense to archive and standardize operational data from Afghanistan across defense information systems and ensure that the operational data is structured, searchable, and usable across the joint force. Additionally, section 1088 directed the Under Secretary of Defense for Intelligence and Security to provide a congressional briefing on how the DoD has handled the operational data from Afghanistan.

~~(CUI)~~ On December 7, 2022, the Office of the Under Secretary of Defense for Intelligence and Security (OUSD[I&S]) conducted a congressional briefing to address section 1088 of the FY 2022 NDAA. However, the DoD has not fully archived, standardized, and made available for use operational data from operations in Afghanistan as required by the FY 2022 NDAA. Instead of the DoD ensuring that the operational data is structured, searchable, and usable across the joint force, the Joint Staff, the U.S. Central Command (USCENTCOM), and the U.S. Special Operations Command (USSOCOM) are compiling and organizing operational data from Afghanistan by following standard DoD records management policies. Additionally, both USCENTCOM and USSOCOM are only working to make the data accessible and searchable within their respective components. [REDACTED]

[REDACTED] This occurred because the DoD did not designate a lead component or determine the resources necessary to satisfy the section 1088 requirements. As a result, [REDACTED]

(U) For the DoD to satisfy the requirements of section 1088 of the FY 2022 NDAA, we recommend that the Deputy Secretary of Defense (DepSecDef) designate a DoD Component to lead the compliance effort. We also recommend that the lead component coordinate with Congress to determine the actions necessary to satisfy the law’s requirements and develop and implement a plan of action, with milestones, for achieving compliance. The DepSecDef agreed with the recommendations; therefore, the recommendations are resolved but will remain open until the Office of the Under Secretary of Defense for Policy (OUSD[P]) and DoD Chief Information Officer (CIO) provide the documentation necessary for closure.

¹ (U) Public Law 117-81, “The National Defense Authorization Act for Fiscal Year 2022,” section 1088, “Treatment of Operational Data from Afghanistan,” December 27, 2021.

(U) Objective

(U) The objective of this evaluation was to determine whether the DoD comprehensively, effectively, and efficiently archived, standardized, and made available for use operational data from Afghanistan, as required by law.²

(U) We focused our evaluation on the actions of the Under Secretary of Defense for Intelligence and Security, USCENTCOM, USSOCOM, and the Joint Staff to process operational and intelligence data from the Afghanistan War. This analysis included determining whether the congressional briefing required by the FY 2022 NDAA occurred and how effectively and efficiently the operational data was obtained, processed, and made searchable.

(U) Background

(U) Following the September 11, 2001, terrorist attacks on the United States, the United States and its coalition partners began a military campaign in Afghanistan. The conflict continued for almost 20 years, with the last U.S. forces departing Afghanistan on August 30, 2021.

(U) Laws and Guidance Related to the Retention of Operational Data from Afghanistan

(U) The FY 2022 NDAA outlines the legal requirements for the DoD to archive and standardize operational data from Afghanistan. In addition, the 2020 DoD Data Strategy highlights the importance of data and the need for the DoD to become a more data-centric organization.³

(U) National Defense Authorization Act for FY 2022

(U) According to section 1088 of the FY 2022 NDAA, an immense amount of operational and intelligence data was generated over the 2 decades-long Afghanistan War; this data is valuable, and it must be appropriately retained. Section 1088 has two primary elements. First, it directs the Secretary of Defense to archive and standardize operational data from Afghanistan across the myriad of defense information systems, and ensure that the operational data are structured, searchable, and usable across the joint force.⁴ Second, section 1088 directs the Under Secretary of Defense for Intelligence and Security to provide the House Armed Services Committee with a briefing by March 4, 2022, on how the DoD removed, retained, and assured long-term access to operational data from Afghanistan across each Military Department and command.⁵

² (U) This report contains information that has been redacted because it was identified by the DoD as Controlled Unclassified Information (CUI) that is not releasable to the public. CUI is Government-created, or owned, unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies.

³ (U) DoD, "Executive Summary: DoD Data Strategy, Unleashing Data to Advance the National Defense," September 30, 2020.

⁴ (U) Section 1088 of the FY 2022 NDAA does not define "standardize" or what standardizing should entail.

⁵ (U) On October 19, 2022, Representative Michael Waltz sent a letter to the Secretary of Defense stating that the OUSD(I&S)'s briefing to the House Armed Services Committee was not conducted as required by section 1088 of the FY 2022 NDAA. Representative Waltz also stated the importance of the operational and intelligence data from Afghanistan for understanding the war and that the data must be accessible if future campaigns occur in the area.

(U) On December 7, 2022, the OUSD(I&S) conducted a congressional briefing on the treatment of intelligence and operational data from Afghanistan. The purpose of the briefing was to explain how the DoD removed, retained, and assured long-term access to intelligence and operational data from Afghanistan across each Military Department and command. The scope of the briefing included how the DoD standardized and archived operational data from Afghanistan across the myriad of defense information systems and ensured access across the joint force. Additionally, the briefing included responses that the Joint Staff, USCENTCOM, and USSOCOM, sent to the OUSD(I&S) describing how each organization is handling operational data from Afghanistan. An OUSD(P) official told us that they believed the OUSD(I&S) conducted this briefing to satisfy section 1088's briefing requirement.

(U) 2020 DoD Data Strategy

(U) The 2020 DoD Data Strategy emphasizes the importance of data. The Strategy states that all DoD leaders are responsible for treating data as a weapon system and managing, securing, and using data for operational effect. The Strategy also states that the DoD needs to accelerate its transition to a data-centric organization that uses data at speed and scale for operational advantage and increased efficiency.

(U) Roles and Responsibilities for Records Management

(U) Section 3102, title 44, United States Code (U.S.C.), directs the heads of each Federal agency to establish and maintain an active, continuing program for economical and efficient management of agency records.⁶ The following individuals and entities have responsibilities related to general DoD records management and management of operational data specifically from Afghanistan.

(U) Office of the Under Secretary of Defense for Policy

(U) According to DoD Instruction (DoDI) 8320.02, the Under Secretary of Defense for Policy, in collaboration with the DoD CIO and the Under Secretary of Defense for Intelligence and Security, is responsible for developing policies and procedures for protecting data, information, and information technology services.⁷ The instruction also states that these three organizations are also responsible for enabling secure sharing of information across DoD security domains with the intelligence community and mission partners, in accordance with law, policy, and security classifications.

⁶ (U) Section 3102, title 44, U.S.C., "Establishment of Program of Management."

⁷ (U) DoDI 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013 (Incorporating Change 1, June 24, 2020).

(U) Joint Chiefs of Staff

(U) According to DoDI 5015.02, the Chairman of the Joint Chiefs of Staff is responsible for developing, implementing, evaluating, and refining records management policies and procedures for programs and organizations for which the Office of the Chairman of the Joint Chiefs of Staff has oversight, including joint operation planning.⁸ Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5760.01A, volume I, sets forth records management administrative instructions and procedural guidance for the Joint Staff and combatant commands, and CJCSM 5760.01A, volume II, implements a generic disposition schedule for records.⁹

(U) Combatant Commanders

(U) According to DoDI 5015.02, all combatant commanders are responsible for ensuring proper management of operational records throughout their life cycle. Furthermore, all combatant commands must abide by the administrative instructions, procedural guidance, and disposition schedules outlined in CJCSM 5760.01A volumes I and II. Combatant commanders can task any subordinate unit or command, including Service Component commands and theater special operations commands, to fulfill this responsibility in accordance with the combatant command's established priorities, operational guidance, and combatant commander's intent.

(U) U.S. Central Command

(U) According to Central Command Regulation 25-50, the USCENTCOM Command and Control, Communications, and Computer Systems (CCJ6) Director/Chief Information Officer functions as the USCENTCOM senior agency official for records management with oversight of the USCENTCOM records management program and delegates authority for program execution to the command records manager.¹⁰ Central Command Regulation 25-50 outlines USCENTCOM requirements to meet the records management requirements outlined in DoDI 5015.02 and CJCSM 5706.01A volumes I and II.

(U) U.S. Special Operations Command

(U) According to USSOCOM Directive 25-51, the USSOCOM Chief of Staff has oversight of the USSOCOM records management program and delegates authority through the USSOCOM Support Directorate Knowledge Management Division Chief to the command records manager for program execution.¹¹ The knowledge management officer also functions as the USSOCOM senior agency official for records management. USSOCOM Directive 25-51 outlines USSOCOM's responsibilities to meet the records management requirements outlined in DoDI 5015.02 and CJCSM 5706.01A volumes I and II.

⁸ (U) DoDI 5015.02, "DoD Records Management Program," February 24, 2014 (Incorporating Change 1, August 17, 2017).

⁹ (U) CSJCSM 5760.01A, "Joint Staff and Combatant Command Records Management Manual: Volume I—Procedures," February 7, 2008.

(U) CJCSM 5706.01, "Volume II—Disposition Schedule," July 13, 2013.

¹⁰ (U) Central Command Regulation 25-50, "Records Management Program," August 26, 2021.

¹¹ (U) USSOCOM Directive 25-51, "Information Management – Records Management: Records Management Program," September 27, 2023.

(U) Finding

(U) The DoD Has Not Fully Complied with Section 1088 of the FY 2022 NDAA for Archiving and Standardizing Operational Data from Afghanistan

~~(CUI)~~ The DoD has not fully archived, standardized, and made available for use operational data from operations in Afghanistan as required by the FY 2022 NDAA. Specifically, section 1088 states that the operational data from Afghanistan should be archived and standardized across the myriad of defense information systems and structured, searchable, and usable across the joint force. Instead of the DoD ensuring that operational data are structured, searchable, and usable across the joint force, the Joint Staff, USCENTCOM, and USSOCOM are compiling and organizing operational data from Afghanistan by following standard DoD records management policies. Accordingly, both USCENTCOM and USSOCOM are only working to make the data accessible and searchable within their respective components.

[REDACTED]

[REDACTED] This occurred because the DoD did not assign a DoD Component with the overall responsibility to lead the effort or develop a plan to archive and standardize operational data from Afghanistan in accordance with the FY 2022 NDAA requirements.

~~(CUI)~~ As a result, without the DoD appointing a component to lead this effort and develop a plan, the data will not be organized or readily available. According to the OUSD(I&S)'s December 2022 congressional briefing, [REDACTED]

[REDACTED]

(U) The DoD Has Not Archived, Standardized, or Made Available for Use Operational Data from Afghanistan as Required

~~(CUI)~~ The DoD has not fully archived, standardized, and made available for use operational data from operations in Afghanistan as required by the FY 2022 NDAA. Specifically, section 1088 of the FY 2022 NDAA states that the operational data from Afghanistan should be archived and standardized across the myriad of defense information systems and structured, searchable, and usable across the joint force. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) The U.S. Special Operations Command’s Handling of Operational Data from Afghanistan

~~(CUI)~~ USSOCOM, like USCENTCOM, also has large amounts of unstructured operational data from Afghanistan and is using standard DoD records management policies as guidance to archive the data. [REDACTED]

[REDACTED] However, not all of this data has been put into a fully indexed and searchable database.

~~(CUI)~~ USSOCOM faces similar barriers to records management as USCENTCOM. [REDACTED]

[REDACTED] A USSOCOM records manager told us that USSOCOM records managers must assist in any search through these networks for desired data. In addition, USSOCOM records management personnel have not created a standardized database for operational data from Afghanistan. According to a USSOCOM knowledge management official, this is due, in part, to USSOCOM having only one records manager. In addition, the evaluation team learned that the different classification levels of operational data and common over- and misclassification of data also contributed to records management personnel not creating a standardized database for operational data from Afghanistan. [REDACTED]

(U) The Joint Staff’s Handling of Operational Data from Afghanistan

~~(CUI)~~ A Joint Staff representative stated that operational data (archived or unstructured) from Afghanistan in their Content Manager applications is the responsibility of the combatant commands. However, the Joint Staff does have archived operational records from Afghanistan stored in the Joint Staff Archives, with digital copies on unclassified, SECRET, and Top Secret networks, as appropriate. [REDACTED]

(U) USCENTCOM, USSOCOM, and the Joint Staff’s Use of DoD Records Management Policy Will Not Fully Address FY 2022 NDAA Section 1088 Requirements

~~(CUI)~~ [REDACTED]

(CUI) [REDACTED]

[REDACTED] Therefore, the DoD’s compliance with records management policies does not ensure that section 1088 requirements will be met.

(CUI) [REDACTED]

(CUI) [REDACTED]

[REDACTED] Through formal written requests for information and in-person interviews with staff from USCENTCOM, USSOCOM, and the Joint Staff, we found that DoD Components did not receive any tasking directing action regarding section 1088. The only DoD directives related to section 1088 were OUSD(I&S) taskers issued to USCENTCOM, USSOCOM, and the Joint Staff for providing information to support the NDAA-required congressional briefing. However, USCENTCOM and USSOCOM personnel told us that section 1088 did not change how they handled operational data from Afghanistan because processing the data is part of their normal operations.

(U) In an attempt to fulfill section 1088 requirements, the OUSD(I&S) directed the Joint Staff to identify the intelligence products that were retained by the Joint Staff’s J-2 analytic and collection management elements and their respective archived locations through a tasker.¹⁴ The Joint Staff responded to the OUSD(I&S) with an information paper that provided a description of the types of intelligence records the Joint Staff collected and retained related to Afghanistan from 2001 to 2022. An additional tasker from the OUSD(I&S) expanded on the initial request for information to specifically ask for information from USCENTCOM and USSOCOM about the status of their operational records from Afghanistan to support the OUSD(I&S)’s congressional briefing.¹⁵ USCENTCOM and USSOCOM both responded to the OUSD(I&S)’s taskers with the requested information.

(U) Therefore, because the DoD’s current efforts will not fully meet the requirements of section 1088 of the FY 2022 NDAA to standardize, archive, and make available operational data from Afghanistan across the joint force or address the challenges the DoD Components and commands face in fulfilling these requirements, the DepSecDef should designate a DoD Component to lead the effort to coordinate with Congress to determine the actions necessary to satisfy the law and develop and implement a plan, with milestones, for satisfying the requirements of the law.

¹⁴ (U) OUSD(I&S) Memorandum for the Joint Staff, “Treatment of Operational Data from Afghanistan in Support of the National Defense Authorization Act for the Fiscal Year 2022, Section 1088,” undated.

¹⁵ (U) OUSD(I&S) Memorandum for the Joint Staff, USCENTCOM, and USSOCOM, “Treatment of Operational Data from Afghanistan in Support of the National Defense Authorization Act for the Fiscal Year 2022, Section 1088,” October 7, 2022.

(CUI)

~~(CUI)~~ Without higher-level direction and adequate resourcing, the task of organizing and standardizing operational data from Afghanistan will be difficult to complete and, therefore, not readily accessible for future operations or important records requests.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the Deputy Secretary of Defense:

- a. **(U) Designate a DoD Component to lead the DoD effort to satisfy the requirements of section 1088 of the FY 2022 National Defense Authorization Act, including:**
 1. **(U) Coordinating with Congress to determine the actions necessary to satisfy the requirements of section 1088 of the FY 2022 National Defense Authorization Act.**
 2. **(U) Developing and implementing a plan of action with milestones to ensure that the DoD satisfies the requirements of section 1088 of the FY 2022 National Defense Authorization Act.**

(U) Deputy Secretary of Defense Comments

(U) The DepSecDef agreed with the recommendation and designated the OUSD(P) to work with the DoD CIO, the Chief Digital and Artificial Intelligence Officer, and other relevant DoD Components to implement the elements of the recommendation. The DepSecDef stated that the DoD is committed to working with Congress and making information available concerning its operations and activities to congressional members, committees, and staffs. The DoD CIO, in coordination with relevant components, will develop and implement a plan of action as recommended, including evaluating the feasibility of implementing additional measures related to section 1088 of the FY 2022 NDAA. This will include gaining congressional support for resourcing the plan. Additionally, the DepSecDef stated that the DoD is already taking steps to index archived data from Afghanistan to make it more searchable. Specifically, USCENTCOM is working with vendors to develop tools for e-discovery, searching, and automatic metadata tagging.

(U) Our Response

(U) Comments from the DepSecDef addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation when the OUSD(P) and DoD CIO provide documentation showing that the planned actions to address the recommendations are completed.

(U) Appendix

(U) Scope and Methodology

(U) We conducted this evaluation from September 2023 through January 2024 in accordance with the “Quality Standards for Inspection and Evaluation,” published in December 2020 by the Council of Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the evaluation to ensure that objectives are met and that we perform the evaluation to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent, and relevant to lead a reasonable person to sustain the findings, conclusions, and recommendations.

(U) This report was reviewed by 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 DoD Components about the CUI treatment of their information. If 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) We identified and reviewed policies, directives, and DoD guidance. Specifically, we reviewed the following criteria

- (U) Public Law 117–81, “The National Defense Authorization Act for Fiscal Year 2022,” section 1088, “Treatment of Operational Data from Afghanistan,” December 27, 2021
- (U) Section 3102, title 44, U.S.C., “Establishment of Program of Management”
- (U) DoDI 5015.02, “DoD Records Management Program,” August 17, 2017
- (U) DoDI 8320.02, “Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense,” August 5, 2013 (Incorporating Change 1, June 24, 2020)
- (U) CJCSM 5760.01A, “Joint Staff and Combatant Command Records Management Manual: Volume I—Procedures,” February 7, 2008
- (U) CJCSM 5760.01A, “Joint Staff and Combatant Command Records Management Manual: Volume II—Disposition Schedule,” September 15, 2014
- (U) Central Command Regulation 25-50, “Records Management Program,” August 26, 2021
- (U) USSOCOM Directive 25-51, “Information Management – Records Management: Records Management Program,” September 27, 2023

- (U) Department of the Army Pamphlet 25-403, "Army Guide to Recordkeeping," November 10, 2022
- (U) DoD, "Executive Summary: DoD Data Strategy, Unleashing Data to Advance the National Defense," September 30, 2020

(U) We conducted or requested interviews with and reviewed documentation from the following DoD organizations.

- (U) USCENTCOM
- (U) USSOCOM
- (U) Joint Chiefs of Staff
- (U) OUSD(P)
- (U) OUSD(I&S)
- (U) Congressional staff

(U) In November 2023, we conducted a site visit at MacDill Air Force Base in Tampa, Florida, and met with representatives from USCENTCOM and USSOCOM. At both USSOCOM and USCENTCOM, we interviewed representatives from the knowledge management and history offices to determine how they collected and retained data related to USCENTCOM and USSOCOM operations and intelligence during the war in Afghanistan (2001 to 2021) and their efforts to make that data accessible and searchable.

(U) During the evaluation, we obtained the following supporting documentation.

- (U) OUSD(I&S) taskers sent to the Joint Staff and the Joint Staff's response
- (U) OUSD(I&S) taskers issued to USCENTCOM and USSOCOM and USCENTCOM's and USSOCOM's responses
- (U) OUSD(I&S) congressional briefing slides

(U) Management Comments

(U) Deputy Secretary of Defense



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

APR 04 2024

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

Thank you for the opportunity to comment on the Department of Defense Inspector General "Management Advisory: Evaluation of the DoD's Handling of Operational Data from Afghanistan Operations." I also want to thank the members of your team who worked on this report for their collaboration with Department staff and for incorporating many of our comments into the draft.

The draft advisory acknowledges that DoD provided the congressional briefing mandated by section 1088 of the Fiscal Year 2022 National Defense Authorization Act. As conveyed in the briefing, a wide array of operational data, including intelligence data, from the war in Afghanistan has been routinely preserved for future access, is searchable, and is accessible to requestors with a "need to know." On that point, the draft advisory also acknowledges that the Joint Staff, United States Central Command (USCENTCOM), and United States Special Operations Command (USSOCOM) are following standard DoD records management requirements.

The draft advisory explains that USCENTCOM and USSOCOM are "working to make the data accessible and searchable within their respective components." To be clear, both USCENTCOM and USSOCOM also make this data available to other DoD personnel with a bona fide need and the appropriate security clearance.

The draft advisory recommends designation of a DoD Component to lead the effort the DoD to satisfy the requirements of section 1088 to include:

1. Coordinating with Congress to determine the actions necessary to satisfy the requirements of section 1088; and
2. Developing and implementing a plan of action and milestones to ensure the DoD satisfied the requirements of section 1088.

DoD concurs with this recommendation. DoD has designated the Office of the Under Secretary of Defense for Policy to work with the Chief Information Officer of the DoD (CIO), the Chief Digital and Artificial Intelligence Officer (CDAO), and other relevant Components to implement the elements of the recommendation. With respect to item 1, DoD is committed to working closely with Congress and making information available concerning its operations and activities to Members of Congress and relevant congressional committees and their staffs. The Department will respond to any congressional inquiries and requests as responsively and expeditiously as possible, consistent with the constitutional and statutory obligations of the Executive Branch. With respect to item 2, the CIO will, in coordination with relevant Components, develop and implement a plan of action as recommended, to include evaluating the feasibility of implementing additional measures related to section 1088, including gaining

(U) Deputy Secretary of Defense (cont'd)

congressional support for resourcing such a plan. DoD is already taking steps to index archived Afghanistan data to make it more searchable. For example, USCENTCOM is working with vendors to develop tools for e-discovery, searching, and automatic metadata tagging.

As the Department conveyed in the congressional briefing on section 1088, the Department archives and retains hardcopy and digital intelligence and operational data from Afghanistan in compliance with the Federal Records Act and other applicable federal record-keeping requirements. All data retention is being conducted according to appropriate National Archives and Records Administration (NARA) schedules. After the required retention period, the data is accessioned to NARA for permanent archival. Once the data is transferred to NARA, it remains accessible to DoD and intelligence community personnel via formal request.

The draft report refers to Senior Agency Officials for Records Management (SAORM) at both USCENTCOM and USSOCOM. This is incorrect. The SAORM for the joint community, including the Combatant Commands, is in the Joint Staff. This is a NARA program for which the CIO is the overall SAORM for DoD. An official listing of participants in the network of SAORMs in DoD is available at <https://www.archives.gov/records-mgmt/agency/sao-list>.

Thank you for your continued efforts to ensure DoD's responsible management of taxpayers' resources.





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/



www.twitter.com/DoD_IG

LinkedIn

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

DoD Hotline

www.dodig.mil/hotline



CUI



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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



CUI