Report No. DODIG-2026-022

INSPECTOR GENERAL

U.S. Department of Defense

December 2, 2025

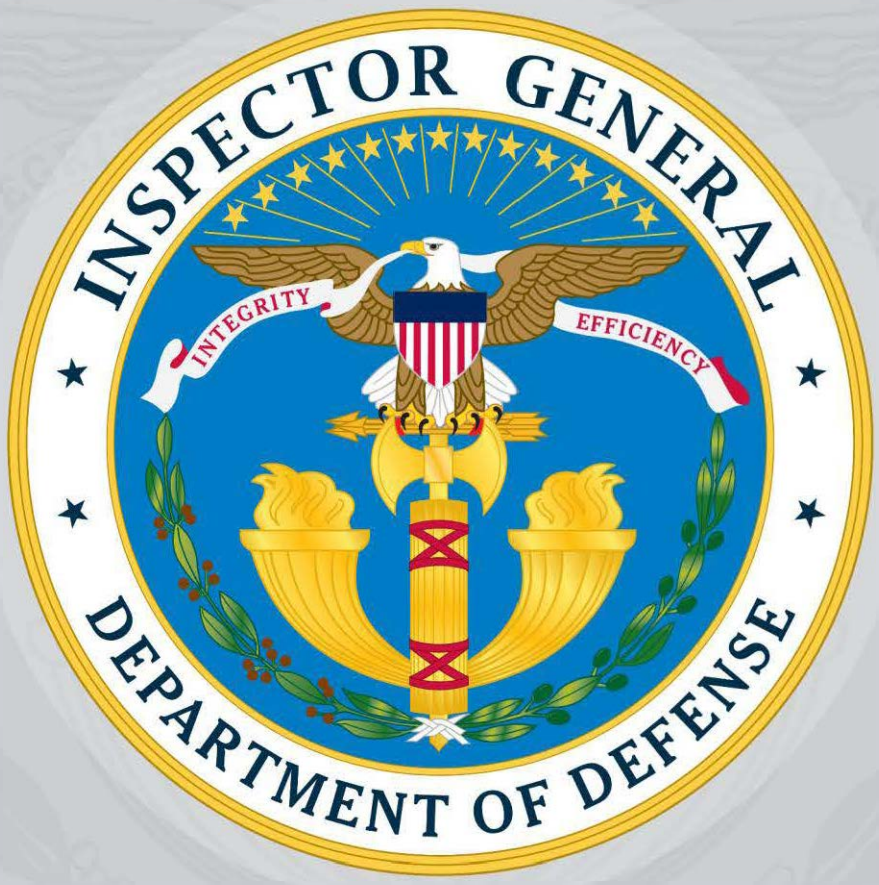
(U) Evaluation of DoD Policy and Oversight Reports Related to Using Non–DoD-Controlled Electronic Messaging Systems to Conduct Official Business

~~Classified By: [redacted]~~
~~Assistant Inspector General for Evaluations~~
~~Programs, Combatant Commands, and Operations~~
~~Derived From: Multiple Sources~~
~~Declassify On: 20490711~~

~~Controlled By: DoD OIG~~
~~Controlled By: Evaluations~~
~~CUI Category: OPSEC, ISVI~~
~~Distribution/Dissemination Control: None~~
~~POC: AIG-PCO, [redacted]~~

~~This content is classified at the SECRET//NOFORN level and may contain elements of controlled unclassified information (CUI), unclassified, or information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to the applicable security classification guides. It must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DoDI 5230.09 prior to public release.~~

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★TRANSPARENCY


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

December 2, 2025

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY
DOD CHIEF INFORMATION OFFICER

SUBJECT: (U) Evaluation of DoD Policy and Oversight Reports Related to Using Non–DoD-Controlled Electronic Messaging Systems to Conduct Official Business (Report No. DODIG-2026-022)

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

(U) This report addresses a March 26, 2025, request from the Chairman and Ranking Member of the Senate Committee on Armed Services to conduct a review of the Secretary's publicly reported use of Signal for official business, including potential use of unclassified networks to discuss sensitive and classified information. Today, the DoD OIG also released a separate report that addresses the facts and circumstances related to the Secretary's use of Signal in the identified incident, "Evaluation of the Secretary of Defense's Reported Use of a Commercially Available Messaging Application for Official Business" (Report No. DODIG-2026-021).

(U) We appreciate the cooperation and assistance received during the evaluation.

Steven A. Stebbins
Acting

(U) Contents

(U) Executive Summary

(U) On March 26, 2025, the Chairman and Ranking Member of the Senate Committee on Armed Services sent a letter to the Acting Inspector General of the DoD requesting: (1) an assessment of DoD policies related to government officers and employees sharing sensitive and classified information on non-government networks and electronic applications, (2) an assessment of DoD classification and declassification policies and processes, and (3) any recommendations to address identified potential issues. This report focuses on the issues we identified during our review of the DoD's information security policies and a summary of seven DoD Office of Inspector General (DoD OIG) reports from 2021 through 2024. This report also provides recommendations to the DoD to address those issues. A separate DoD OIG report, "Evaluation of the Secretary of Defense's Reported Use of a Commercially Available Messaging Application for Official Business" (Report No DODIG-2026-021), provides the facts and circumstances related to the specific events that prompted the request.

(U) As stated in multiple policies and communications, DoD policy:

- (U) requires declassification markings and instructions and identification of who authorized the declassification of classified information;
- (U) prohibits the use of non–DoD-controlled electronic messaging systems, with limited exceptions, and directly prohibits using them for convenience or because of perceived security;
- (U) requires DoD personnel to protect nonpublic DoD information; and
- (U) requires DoD personnel to comply with Federal law to retain official records.

(U) Our review of seven reports issued before the end of 2024 found instances when DoD personnel did not comply with DoD policies for information and operations security, electronic messaging, and records retention. For example, one evaluation found that at the start of maximum telework during the COVID-19 pandemic, some teleworking personnel reported using unauthorized video conferencing applications and personal laptops and cell phones to complete their work because some DoD Components were unprepared for maximum telework. We also found that of the 48 recommendations in the reports we summarize in this report, 22 remain open.

(U) As a result, DoD personnel's use of non–DoD-controlled electronic messaging systems may have jeopardized DoD operations or missions. Furthermore, DoD policy clearly states that DoD personnel who use non–DoD-controlled electronic messaging

(U) systems must still transfer the records to a DoD records system within 20 days of transmission.

(U) Recommendations, Management Comments, and Our Response

(U) We made four recommendations to the DoD Chief Information Officer (CIO). The official Performing the Duties of the DoD CIO provided comments that addressed three recommendations to: (a) provide DoD-controlled capabilities that meet the DoD's needs to share information internally, externally, at various classification levels, on mobile devices, and in compliance with policy and law; (b) require a tailored training for DoD political appointees, general or flag officers, and civilian executives on how to use mobile devices and applications in compliance with DoD policy; and (c) make the waiver process in the DoD's electronic messaging policies more clear and consistent. These recommendations are resolved but will remain open until the DoD CIO provides evidence of implementation.

(U) We also recommended that the DoD CIO include information in the DoD's annual cyber training about the impacts and risks of using non–DoD-controlled electronic messaging services. The official Performing the Duties of the DoD CIO disagreed with this recommendation. Therefore, it is unresolved. We request that the DoD CIO provide additional comments on how they plan to implement the recommendation.

(U) We recommended that the Under Secretary of Defense for Intelligence and Security (USD[I&S]) conduct a DoD-wide assessment to identify the extent of DoD personnel using non–DoD-controlled electronic messaging services to conduct official business and the associated risks and provide the findings and recommendations from the assessment to the DoD CIO. The Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security, responding for the USD(I&S), partially agreed with the assessment recommendation and agreed to conduct a smaller-scoped risk assessment and include two questions in a future data call. This did not meet the intent of the recommendation and is therefore unresolved. Additionally, the Director agreed to our second recommendation to provide their assessment's findings and recommendations, as well as two relevant completed studies, to the DoD CIO. This recommendation is resolved but will remain open until the USD(I&S) provides evidence of implementation.

(U) Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Under Secretary of Defense for Intelligence and Security	2.a	2.b	None
DoD Chief Information Officer	1.d	1.a, 1.b, and 1.c	None (U)

(U) Please provide Management Comments by January 2, 2026.

(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.

(U) Introduction

(U) Objective

(U) The objective of this evaluation was to summarize DoD policies and previous DoD Office of Inspector General (DoD OIG) oversight reports published from March 2021 through October 2024 related to the use of unclassified networks and non–DoD-controlled electronic messaging systems to discuss sensitive and classified information.

(U) In a March 26, 2025 letter, the Chairman and Ranking Member of the Senate Committee on Armed Services requested that the DoD OIG conduct a review of and provide an assessment regarding the publicly reported use of Signal by the Secretary of Defense (SecDef) for official business, including potential use of unclassified networks to discuss sensitive and classified information. Specifically, the Chairman and Ranking Member requested that the following information be included in the review.

1. (U) The facts and circumstances surrounding the above referenced Signal chat incident, including an accounting of what was communicated and any remedial actions taken as a result;
2. (U) DoD policies and adherence to policies relating to government officers and employees sharing sensitive and classified information on non-government networks and electronic applications;
3. (U) An assessment of DoD classification and declassification policies and processes and whether these policies and processes were adhered to;
4. (U) How the policies of the White House, DoD, the intelligence community, and other Departments and agencies represented on the National Security Council of this subject differ, if at all;
5. (U) An assessment of whether any individuals transferred classified information, including operational details, from classified to unclassified systems, and if so, how;
6. (U) Any recommendations to address potential issues identified.

(U) This report addresses parts 2, 3, and 6 of the Chairman and Ranking Member's request. The DoD OIG is releasing a separate report, "Evaluation of the Secretary of Defense's Reported Use of a Commercially Available Messaging Application for Official Business" (Report No. DODIG-2026-021), which will address parts 1, 2, 3, 5, and 6 of the

(U) request. We did not address part 4 of the request because the DoD OIG does not have jurisdiction over non-DoD entities, such as the White House, Intelligence Community, or other government departments.

(U) Finding

(U) Summary of DoD Policies Related to Classification, Declassification, and DoD Personnel Sharing Information on Non–DoD-Controlled Electronic Messaging Systems

(U) We found that DoD policy provides specific processes and procedures for classifying, declassifying, and protecting controlled and classified information. Specifically, DoD policy: (1) requires declassification markings and instructions and identification of who authorized the declassification of classified information; (2) prohibits the use of non–DoD-controlled electronic messaging systems, with limited exceptions, and directly prohibits using them for convenience or because of perceived security; (3) requires DoD personnel to protect nonpublic DoD information; and (4) requires DoD personnel to comply with Federal law to retain official records.[1]

(U) Types of DoD Information

(U) DoD policy defines multiple types of information and standards for how to protect them. According to DoD Instruction (DoDI) 8582.01, DoD information is "any information that is in DoD custody and control; relates to information in DoD custody and control; was acquired by DoD employees as part of their official duties or because of their official status in the DoD, including information that is provided by the DoD to a non-DoD entity; or is developed by a non-DoD entity in support of an official DoD activity."[2] Additionally, public DoD information is "DoD information that has been cleared for public release in accordance with DoDI 5230.09."[3] Similarly, nonpublic DoD information is "any DoD information that has not been cleared for public release" and must be protected. Nonpublic DoD information can also meet the definition of other information types shown in Figure 1 and be subject to additional safeguarding or secrecy standards.

[1] (U) In this report, we use the term "non–DoD-controlled electronic messaging system" to refer to any third-party, commercially available, or non–U.S. Government-controlled electronic messaging or texting system.

[2] (U) DoDI 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," December 9, 2019.

[3] (U) DoDI 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019 (Incorporating Change 1, February 9, 2022).

(U) Figure 1. Spectrum of Nonpublic DoD Information Security and Sensitivity by Type

(U) Unclassified		Classified		
Sensitive Information	**CUI**	**Confidential**	**SECRET**	**TOP SECRET**
Information that, if lost, misused, accessed without authorization, or modified, could adversely affect national interest and the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act but that does not meet the criteria in law or an Executive order to be kept secret in the interest of National defense or foreign policy.[4]	Information that the Government creates or possesses that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls	Information that, if disclosed, could reasonably be expected to cause **damage** to national security	Information that, if disclosed, could reasonably be expected to cause **serious damage** to national security	Information that, if disclosed, could reasonably be expected to cause **exceptionally grave damage** to national security (U)

(U) Source: DoD Manual 5200.01, Volume 1; DoD Manual 5205.02; and 32 C.F.R. § 2002.4.

(U) DoD Policies for Controlling, Classifying, and Declassifying Information

(U) According to DoD Directive 5205.02E, "DoD Operations Security (OPSEC)," DoD personnel must maintain essential secrecy of all information that is useful for adversaries and potential adversaries to plan, prepare, and conduct military and other operations against the United States, as well as safeguard this information from unauthorized access and disclosure.[5] This includes protecting classified information, such as SECRET and TOP SECRET, and controlled unclassified information (CUI) during physical and electronic storage and transmission.[6]

(U) CUI is unclassified information that a law, regulation, or government-wide policy identified as needing safeguarding. DoDI 5200.48, "Controlled Unclassified Information (CUI)," says that DoD CUI is organized into organizational indexes, such as defense, privacy, and proprietary, and is categorized by the DoD according to the specific law,

[4] (U) The full definition of sensitive information in DoD policy is "information that the loss, misuse, unauthorized access, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code, but that has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of National defense or foreign policy."

[5] (U) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012 (Incorporating Change 2, August 20, 2020).

[6] (U) According to 32 C.F.R. § 2002.4, CUI is "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls."

(U) regulation, or government-wide policy requiring control.[7] CUI requires access control, handling, marking, dissemination controls, and other protective measures for safeguarding. Information is designated as CUI when an individual, agency, organization, or group of users permitted to handle CUI determines that a specific item of information falls into a CUI category or subcategory.[8]

(U) According to DoD Manual (DoDM) 5200.01, Volume 1, original classification is the initial decision that information: (1) could reasonably be expected to cause identifiable or describable damage to national security if subjected to unauthorized disclosure and (2) requires protection in the interest of national security.[9] Only senior positions assigned a unique mission with responsibility for one of the eight reasons to classify information may be delegated original classification authority (OCA) by the SecDef or Secretaries of the Military Departments.[10] At the time information is classified, the OCA establishes a specific date or event for declassification based on the duration of the national security sensitivity of the information.

(U) According to DoDM 5200.01 and DoDM 5200.45, "Original Classification Authority and Writing a Security Classification Guide," the responsible OCA will issue security classification guidance for each system, plan, program, project, or mission involving classified information.[11] The required classification guidance may be in the form of a memorandum, plan, order, letter, or security classification or declassification guide. For example, the U.S. Central Command security classification guide establishes the basic policies for properly marking, classifying, downgrading, and declassifying information related to the U.S. Central Command or units operating in its area of responsibility. The guide includes details about the information elements to protect, their level of classification, the reason for classification, declassification information, dissemination controls, and appropriate CUI category. An OCA can also determine that a combination of CUI should be classified.

(U) DoDM 5200.01, Volume 1, states that information will be declassified as soon as it no longer meets the standards for classification. Information is usually declassified using one of four processes described in Appendix C and communicated through

[7] (U) DoDI 5200.48, "Controlled Unclassified Information," March 6, 2020.

[8] (U) Appendix C includes a comprehensive summary of DoD CUI, classification and declassification policy and processes.

[9] (U) DoDM 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012 (Incorporating Change 2, July 28, 2020).

[10] (U) Information must meet one of the following categories to be classified: (1) military plans, weapon systems, or operations; (2) foreign government intelligence; (3) intelligence activities, sources or methods, or cryptology; (4) foreign relations or foreign activities of the United States, including confidential sources; (5) scientific, technological, or economic matters related to national security; (6) U.S. Government programs for safeguarding nuclear materials or facilities; (7) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services related to national security; or (8) the development, production, or use of weapons of mass destruction.

[11] (U) DoDM 5200.45, "Original Classification Authority and Writing a Security Classification Guide," January 17, 2025.

(U) declassification guides or markings. Declassification markings are used to clearly convey the declassified status of the information and who authorized the declassification.

(U) DoD Electronic Messaging Policy

(U) DoDI 8170.01, "Online Information Management and Electronic Messaging," directly states, "do not use non–DoD-controlled electronic messaging services to process nonpublic DoD information, regardless of the service's perceived appearance of security."[12] The instruction gives examples, such as private accounts or groups or encrypted messages. DoDI 8170.01 also states that classified information can only be sent by electronic messaging on classified networks or those encrypted with National Security Agency-approved cryptography.[13]

(U) DoDI 8170.01 also requires compliance with DoD records retention, cybersecurity, and information security policies. This DoDI reiterates the legal requirement for records retention and states that DoD personnel may not create or send a record using a nonofficial electronic messaging account without copying their official electronic messaging account or forwarding a complete copy of the record to their official electronic messaging account within 20 days. The definition of a record is included in the next section of this report, DoD Records Policy. DoDI 8170.01 also states that Office of the Secretary of Defense and DoD Component heads are responsible for ensuring that all nonpublic DoD information is collected, distributed, shared, stored, or otherwise processed on systems that comply with cybersecurity policies, such as DoDIs 8510.01, "Risk Management Framework for DoD Systems," and 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," and the National Industrial Security Program Operating Manual.[14] DoDI 8170.01 also reiterates that DoD personnel must not disclose nonpublic information or unclassified information that aggregates to reveal sensitive or classified information.

(U) Additionally, DoDI 8170.01 states that personnel may not use personal, nonofficial accounts for personal convenience or preference. DoD policy says that "DoD personnel

[12] (U) DoDI 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019 (Incorporating Change, March 12, 2025).

[13] (U) Appendix D includes a more comprehensive summary of how the DoD's electronic messaging and related policies evolved over time.

[14] (U) DoDI 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022.

(U) DoDI 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," December 9, 2019.

(U) Title 32 C.F.R. Part 117, "National Industrial Security Program Operating Manual (NISPOM)."

(U) must not use personal email or other nonofficial accounts to exchange official information." Any exception to policy must meet all three of the following conditions.

- (U) The use is for emergencies and other critical mission needs.
- (U) Other official communication capabilities are unavailable, impractical, or unreliable.
- (U) The use is in the interest of DoD or other U.S. Government missions.

(U) DoDI 8170.01 further states that the Office of the Secretary of Defense and DoD Component heads may approve, as appropriate, official use of non–DoD-controlled electronic messaging services, but the DoDI provides no mechanism or specific parameters for exercising the exception. In October 2023, in response to a DoD OIG audit, the DoD CIO issued a memorandum that created a process for DoD Components to request an exception to policy that requires final exception approval from the DoD CIO Chief Information Security Officer.[15] However, the newest version of DoDI 8170.01, published in March 2025, did not incorporate this exception request process or clarify that a Component head cannot provide final approval for the policy exception.

(U) DoD Records Policy

(U) According to DoDI 5015.02, "DoD Records Management Program," a record is defined as:

> (U) all recorded information, regardless of form or characteristics, made or received by a federal agency under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the U.S. Government or because of the informational value of the data in them. A DoD record also includes operational logistics, analysis, support, and other materials created or received by the DoD Components in training, contingency, and wartime operations, as well as in all routine and peacetime business.[16]

(U) According to DoDI 5015.02, "DoD records will be managed as national assets" in compliance with chapters 29, 31, 33, and 35 of Title 44 U.S. Code. Both DoD policy and Federal law provide specific requirements for maintaining records and include instructions for using non-official electronic messaging accounts. If a non-official electronic messaging account is used, both DoDI 5015.02 and 44 U.S.C. § 2911 require

[15] (U) DoD CIO Memorandum, "Use of Unclassified Mobile Applications in Department of Defense," October 6, 2023.

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

(U) DoD employees to forward a copy of the record to their official account at the time of transmission or within 20 days of its original creation.

(U) The DoD Reiterated Its Policies; However, Personnel Did Not Consistently Comply with Federal Law and DoD Policies for Electronic Messaging and Records Retention

(U) DoD Components repeatedly communicated DoD policy related to the use of non-DoD-controlled devices and messaging applications. For example, DoD senior leaders issued multiple memorandums from 2016 to 2023 to emphasize information security procedures.[17] In 2023, the then-SecDef and DoD CIO separately issued memorandums emphasizing the prohibition of transmitting nonpublic DoD information on non-DoD-controlled electronic messaging services, information systems, and accounts or personal email accounts, regardless of the messaging service's perceived appearance of security.

~~(S)~~ However, our review of seven prior DoD OIG reports identified multiple instances when DoD personnel did not comply with DoD policy and records retention law.[18] For example, one evaluation found that, at the start of maximum telework in response

[17] (U) See Appendix D for a list of DoD memorandums issued from 2016 through 2023 that emphasize information security procedures to DoD personnel.

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

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]

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

~~(CUI)~~ [redacted]

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

(U) DoD OIG Report No. DODIG-2021-065, "Evaluation of Access to Department of Defense Information Technology and Communications During the Coronavirus Disease-2019 Pandemic," March 30, 2021.

(U) The Prior Coverage section in Appendix A includes summaries of each of the seven reports and the status of their recommendations.

(U) DoD OIG Report No. DODIG-2025-058, "Review of Responsibilities and Actions Related to the Secretary of Defense's Hospitalizations and the DoD's Policies and Procedures for Notification and Transfer of Functions and Duties," January 10, 2025, also noted issues with DoD personnel using non-DoD-controlled electronic messaging services and personal devices or accounts for official DoD information. The DoD Inspector General referred these issues back to the DoD for separate consideration. However, this review did not provide enough information for analysis to be included as a relevant oversight report for this evaluation.

~~(S)~~ to the COVID-19 pandemic, some teleworking personnel reported using unauthorized video conferencing applications and personal laptops, printers, and cell phones to complete their work because some DoD Components were unprepared for maximum telework.[19] Other reports identified instances of DoD personnel violating electronic messaging and records retention policies while: (1) teleworking during the COVID-19 pandemic; (2) [redacted] (3) using DoD mobile devices; (4) [redacted]; (5) [redacted]; and (6) performing official duties as the Director of the Defense Digital Service. [redacted][20]

~~(S)~~ DoD personnel used non–DoD-controlled electronic messaging systems for a variety of reasons. For example, some personnel used them because of the systems' perceived appearance of security. [redacted]

(U) As a result, DoD personnel increased the risk of exposing sensitive DoD information to our adversaries and did not comply with the legal obligation to retain and preserve official records.[21]

(U) The DoD Has Not Fully Implemented DoD OIG Recommendations Related to the Use of Non–DoD-Controlled Electronic Messaging Systems

(U) We found that DoD Components have not fully implemented the recommendations from the seven relevant DoD OIG reports we reviewed.[22] Of the 48 recommendations from the seven reports, 26 were closed and 22 remained open as of September 24, 2025. The open recommendations fall into the following categories: (1) addressing and mitigating known vulnerabilities; (2) conducting risk assessments; (3) training; (4) policies, processes, and procedures; and (5) ensuring personnel were properly

[19] (U) DoD OIG Report No. DODIG-2021-065.

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

[21] (U) Chapter 31 of Title 44 U.S. Code requires agencies to make and preserve records. Title 44 U.S.C. § 3106 provides procedures related to the unlawful removal or destruction of records.

[22] (U) Appendix B provides a table of all recommendations and their statuses.

(U) equipped. Some recommendations fit into multiple categories. Additionally, each summary may include multiple recommendations.

(U) We found 10 open recommendations related to addressing and mitigating known vulnerabilities. The DoD did not implement recommendations to:

- (~~CUI~~) [redacted], and
- (U) remove unauthorized applications from and limit future access to unauthorized applications on DoD mobile devices.

(U) We found four open recommendations related to conducting risk assessments. The DoD did not implement recommendations to:

- (U) have all geographic combatant commands establish risk assessment procedures to evaluate the use of different technologies in accordance with DoDI 8170.01,
- (U) assess unmanaged applications for operational and cybersecurity risks and remove those with unacceptable risks from DoD mobile devices,
- (U) assess DoD mobile device users' access to public application stores, and
- (~~CUI~~) [redacted]

(U) We found five open training-related recommendations. The DoD did not implement recommendations to:

- (U) provide training to all DoD mobile device users on the proper use of DoD mobile devices,
- (U) develop OPSEC training requirements that address the risks of using non–DoD-controlled electronic messaging systems,
- (U) have all geographic combatant commands create training criteria addressing proper use of non–DoD-controlled electronic messaging systems, and
- (U) use standardized terminology in policy and training for different types of applications.

(U) We found 14 open recommendations related to policies, procedures, and processes. The DoD did not implement recommendations to:

- (U) develop a comprehensive mobile device and mobile application policy;
- (U) develop tailored, command-level guidance on the use of non–DoD-controlled electronic messaging systems at the U.S. Southern Command; and
- (~~CUI~~) [redacted]

(~~CUI~~) We found two open recommendations related to ensuring personnel had the appropriate equipment to perform their duties in compliance with policy. [redacted]

(U) Noncompliance with DoD Policy and Incomplete Implementation of Report Recommendations Increased Security Risks

(~~S~~) DoD personnel are legally required to protect nonpublic DoD information and maintain all official records. Additionally, failure to comply with law and DoD policies to properly classify, declassify, and protect nonpublic DoD information puts DoD mission success at risk. [redacted] To address the problems identified in prior reports, the DoD must implement open DoD OIG recommendations and the recommendations of this report to:

- (U) mitigate known vulnerabilities;
- (U) conduct risk assessments;
- (U) improve training;
- (U) develop and implement clear policies, processes, and procedures; and
- (U) appropriately equip DoD personnel so they can comply with policy.

(U) Recommendations, Management Comments, and Our Response

(U) Revised Recommendation

(U) As a result of management comments, we revised draft Recommendation 1.b to clarify the nature of the actions needed to complete the recommendation and identify the DoD CIO-suggested offices with coordinating responsibilities.

(U) The original recommendation was to "Develop and implement a tailored training with a knowledge assessment for DoD political appointees, general officers, flag officers, and members of the Senior Executive Service that includes the elements in DODIG-2023-041 Recommendation 2.d and its sub-elements." We accepted the DoD CIO's suggestion to include other offices with coordination responsibilities. We did not adopt the exact proposed language or remove the references to DODIG-2023-041 Recommendation 2.d and its sub-elements because the intent of the recommendation is to provide only who should receive the training and the topic areas it should cover (at least those listed in DODIG-20203-041 Recommendation 2.d), not prescribe the training format. Nothing in this recommendation interferes with closing the open recommendations in DODIG-2023-041. The work done to close those recommendations should create efficiencies in closing this recommendation.

(U) Recommendation 1

(U) We recommend that the DoD Chief Information Officer:

a. **(U) Source and maintain DoD-controlled capabilities that meet the DoD's operational needs to share information across the DoD and U.S. Government and with foreign partners. The capabilities should include the ability to communicate on DoD-approved and non-DoD personnel mobile devices, collaborate in group environments, and share unclassified, controlled, and classified information; have a user-friendly interface; and comply with DoD and government-wide requirements to protect information and preserve official records.**

(U) DoD Chief Information Officer Comments

(U) The official Performing the Duties of the DoD CIO partially agreed and stated that several steps have been taken to develop and maintain comprehensive, layered architecture designed to protect information at all sensitivity levels. The DoD CIO stated that the current capabilities include robust collaboration tools and secure file-transfer mechanisms to exchange data with internal and external partners, as well as mobile capabilities for DoD-approved devices with stringent security controls designed to meet the needs of warfighters and partners. The DoD CIO stated that each DoD Component develops and fields capabilities that meet their specific mission

(U) requirements and that DoD policy enables Components to meet their own needs. The DoD CIO also stated that the current capability does not fully meet the combatant commands' requirements to securely share unclassified messages with coalition partners. Additionally, the DoD CIO stated that the Office of the DoD CIO continues to investigate how to improve the performance of these devices and develop newer and more efficient designs.

(U) Our Response

(U) Although the DoD CIO only partially agreed with the recommendation, their comments addressed the specifics of the recommendation; therefore, it is resolved but will remain open. We will close the recommendation when the DoD CIO provides evidence that DoD-controlled capabilities meet the DoD's operational needs to share information across the DoD and U.S. Government and with foreign partners, including the ability to use mobile devices and electronic messaging applications.

b. (U) Establish and implement, in coordination with the Under Secretary of Defense for Intelligence and Security and Director of Administration and Management, a training requirement in DoD policy for DoD political appointees, general officers, flag officers, and members of the Senior Executive Service to take a tailored training with a knowledge assessment that addresses the unique needs of senior leaders and includes the content areas spelled out in DODIG-2023-041 Recommendation 2.d and its sub-elements.[23]

[23] (U) DODIG-2023-041 Recommendation 2.d states that the DoD CIO should, in coordination with the USD(I&S), develop comprehensive mobile device and mobile application policy for Components and users. The policy should, at a minimum, require DoD Components to provide regularly scheduled training to DoD mobile device users on the responsible and effective use of mobile devices and applications, including electronic messaging services, in accordance with DoD CIO memorandum, "Mobile Application Security Requirements," October 6, 2017, and DoDI 8170.01. The training should address, at a minimum: (1) ethics guidelines to ensure compliance with DoD 5500.07-R, "Joint Ethics Regulation;" (2) definitions of, differences between, and responsible use of managed and unmanaged applications on DoD mobile devices; (3) best practices when using unmanaged applications; (4) operational security concerns, potential threats, and risks associated with using unmanaged applications, which may contain capabilities such as location sharing (GPS tracking) or personal information sharing or may have nefarious characteristics, such as marketing scams and human trafficking; (5) cybersecurity concerns associated with using unmanaged applications, which may contain malware or spyware; (6) privacy-related concerns; (7) records management requirements to ensure compliance with DoD Instruction 5015.02; (8) information review for clearance and release authorization procedures; and (9) accessibility standards to ensure compliance with DoD Manual 8400.01, "Accessibility of Information and Communications Technology."

(U) DoD Chief Information Officer Comments

(U) The official Performing the Duties of the DoD CIO partially agreed and proposed rewriting the recommendation to:

> (U) "The DoD CIO, in coordination with the USD(I&S) and in conjunction with the Director of Administration and Management, establish guidance for the development, implementation, and provision of personalized one-on-one training, with a knowledge assessment, for DoD political appointees, general officers, flag officers, and members of the Senior Executive Service based on current and existing training required to be taken by all DoD civilian, military, and contract employees prior to gaining access to unclassified and classified systems and information. This "Senior Official" training will be provided and given to the respective Senior Officials by the direct supporting Security/Access Control Official/Office for the same officials."

(U) The DoD CIO also recommended removing all references to the open recommendations in DODIG-2023-041 because the DoD CIO staff answered and provided supporting documentation to close the remaining open recommendations for that report.

(U) Our Response

(U) Although the DoD CIO only partially agreed with the recommendation, their comments addressed the intent of the recommendation; therefore, it is resolved but will remain open. We will close this recommendation when the DoD CIO provides evidence that they created and implemented the training requirement for senior leaders that includes a knowledge assessment and the topic areas in DODIG-2023-041 Recommendation 2.d parts 1 through 9.

c. (U) Clearly define the criteria, process, and personnel authorized to grant a waiver to the DoD's prohibition against using non–DoD-controlled electronic messaging services to conduct official business in DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," and related policies.

(U) DoD Chief Information Officer Comments

(U) The official Performing the Duties of the DoD CIO agreed and acknowledged that there is confusion on the criteria, process, and personnel authorized to grant a waiver. They also stated that their office will update all associated policies to ensure that the process and approver for any messaging waivers is consistent.

(U) Our Response

(U) The comments from the official Performing the Duties of the DoD CIO addressed the specifics of the recommendation; therefore, it is resolved but will remain open. We will close the recommendation when the DoD CIO provides documentation showing that all associated policies were updated to ensure that the process and approver for any messaging waivers are consistent.

d. (U) Update the annual DoD-wide cyber training to include information about the impacts of unauthorized disclosures on non-government applications and risks of using non–DoD-controlled electronic messaging services.

(U) DoD Chief Information Officer Comments

(U) The official Performing the Duties of the DoD CIO disagreed and stated that an update to the annual DoD-wide cyber training would be a redundant and non–cost-effective undertaking. They also stated that the topic of unauthorized disclosures on messaging applications is included in the course materials for the annual DoD-wide "Unauthorized Disclosure of Classified Information and CUI" training course, which is currently required for DoD personnel who have access to and use DoD information systems and information at all classified levels.

(U) Our Response

(U) Comments from the official Performing the Duties of the DoD CIO did not address the specifics of the recommendation; therefore, it is unresolved. We acknowledge the DoD CIO's concern that including information about the impacts of unauthorized disclosures on non-government applications and risks of using non–DoD-controlled electronic messaging services in the annual DoD-wide cyber training would be redundant. However, current training is not sufficient because we found that DoD personnel did not consistently comply with policy. Additionally, DD Form 2875, "System Authorization Access Request," asks for requestors only to attest that they completed the annual cyber awareness training and provide the completion date when requesting access to DoD systems and information. We request that the DoD CIO provide comments on how they plan to implement the recommendation.

(U) Recommendation 2

(U) We recommend that the Under Secretary of Defense for Intelligence and Security:

a. **(U) Conduct an Office of the Secretary of Defense- and DoD-wide assessment to identify the extent of DoD personnel using non–DoD-controlled electronic messaging services to conduct official business and associated risks.**

(U) Under Secretary of Defense for Intelligence and Security Comments

(U) The Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security, responding on behalf of the USD(I&S), partially agreed and stated that the Office of the USD(I&S) (OUSD[I&S]) cannot conduct an assessment on the extent of the use of non–DoD-controlled electronic messaging services by DoD personnel for multiple reasons, including authority and privacy concerns. The Director stated that they planned to include the following questions on the next DoD-wide OPSEC data call, tentatively scheduled for 2027.

- (U) Are DoD Component leaders and supervisors aware whether DoD personnel under their supervision are using non–DoD-controlled electronic messaging services to conduct official business?

- (U) Have DoD Component leaders and supervisors taken any actions regarding the use of non–DoD-controlled electronic messaging services to conduct official business, including permitting such use?

(U) The Director also agreed to conduct a risk assessment on the use of non–DoD-controlled electronic messaging services to conduct official business.

(U) Our Response

(U) We acknowledge the OUSD(I&S)'s prior work assessing awareness of DoD policy regarding the use of non–DoD-controlled systems, as well as their concerns for how to gather accurate information on the extent of DoD personnel's use of non–DoD-controlled electronic messaging systems. However, their proposed actions to include two questions in the OPSEC data call, tentatively planned for 2027, is neither timely nor does it gather sufficient information. The Director agreed that DoD personnel's use of non–DoD-controlled electronic messaging services could jeopardize DoD operations or missions. Given that risk, the OUSD(I&S) should not wait until 2027 to gather information and then begin mitigating these risks. Additionally, we disagree that the OUSD(I&S) cannot conduct an assessment that would be accurate or useful. The OUSD(I&S) should look to best practices and prevalence of noncompliance assessment methodologies to

(U) determine: (1) what information is being shared or official business is being conducted on non–DoD-controlled systems; (2) the various non–DoD-controlled electronic messaging systems being used; (3) and the prevalence of noncompliance. Therefore, Recommendation 2.a remains unresolved until the OUSD(I&S) provides a proposed methodology for the DoD-wide risk assessment to determine what information is being shared or official business is being conducted on non–DoD-controlled systems, the systems being used, and the prevalence of use.

b. (U) Provide the findings and any recommendations of the assessment in Recommendation 2.a to the DoD Chief Information Officer to help inform the requirements for the capability described in Recommendation 1.a.

(U) Under Secretary of Defense for Intelligence and Security Comments

(U) The Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security, responding on behalf of the USD(I&S), agreed with Recommendation 2.b. The Director stated that the OUSD(I&S) will provide the findings and recommendations of the risk assessment to the DoD CIO, as well as related research reports they had funded.

(U) Our Response

(U) The Director's comments addressed the specifics of the recommendation; therefore, it is resolved but will remain open. We will close the recommendation when the Director provides evidence showing that the findings and recommendations of the risk assessment were provided to the DoD CIO.

(U) Appendix A

(U) Scope and Methodology

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

(U) This evaluation focused on issues related to the use of non–DoD-controlled electronic messaging systems, assessing DoD policies related to "government officers and employees sharing sensitive and classified information on non-governmental networks and electronic applications," and DoD classification and declassification policies and processes. This evaluation did not assess the extent to which any individuals complied with the reviewed policies or the facts and circumstances related to the events of March 15, 2025, which are assessed in "Evaluation of the Secretary of Defense's Reported Use of a Commercially Available Messaging Application for Official Business" (Report No. DODIG-2026-021), published December 2, 2025.

(U) We searched www.oversight.gov, www.gao.gov, and DoD OIG reports and found seven relevant DoD OIG evaluations, audits, or investigations conducted in the last 5 years. In addition, we:

- (U) identified and analyzed the most relevant DoD policies and summarized them in the report and Appendixes C and D,
- (U) analyzed the seven relevant DoD OIG reports for consistent themes and insights,
- (U) obtained the current status of the 48 recommendations from the DoD OIG reports, and
- (U) analyzed the open recommendations and organized them into various categories based on the themes that we found.

(U) Use of Computer-Processed Data

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

(U) Prior Coverage

(U) During the last 5 years, the DoD OIG issued seven reports discussing the use of DoD electronic messaging systems in violation of DoD policy. Unrestricted DoD OIG reports can be accessed at www.dodig.mil/reports.

(U) Report No. DODIG-2025-006, "Follow-up Evaluation on Management Advisory: The Protection of Sensitive Mission Data by the Security Assistance Group–Ukraine and Its Subordinate Commands," October 11, 2024

(U) The objective of DODIG-2025-006 was to assess the extent to which the Security Assistance Group–Ukraine (SAG-U) and its subordinate commands, in coordination with the U.S. Army Europe and Africa, fully implemented plans and issued guidance to improve compliance with DoD information security policies. DODIG-2025-006 was conducted as a follow-up evaluation to DODIG-2024-002.

~~(CUI)~~ The DoD OIG found that SAG-U and its subordinate commands improved their information security practices. For example, SAG-U and its subordinate Division Tactical Command Post (DTAC) developed information security standard operating procedures (SOPs) that direct personnel to use approved DoD programs of record corresponding to or exceeding the classification of the information being transmitted to ensure information security. The SOPs also directed all personnel under their operational control to not use non–DoD-controlled electronic messaging services, such as communication applications on cellular devices, to process nonpublic DoD information. [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

(U) The follow-up report made five total recommendations. Four are resolved but remain open, and one related to physical security is now closed. The report recommended that the SAG-U Commander direct DTAC to establish a process to regularly remind U.S. personnel to follow applicable DoD information security guidance and conduct and document DTAC SOP training for all movement control personnel. The report also recommended that the SAG-U Commander review and refine SOPs and recurring compliance inspections to include the use of public electronic messaging services.

(U) Report No. DODIG-2024-109, "Management Advisory: U.S. Air Forces in Europe Handling of Sensitive Information at Logistics Enabling Node–Romania," July 11, 2024

(U) The objective of DODIG-2024-109 was to address urgent security concerns discovered with operational and information security of documents and communications used to manage, track, and coordinate the movement of U.S. defense items to Ukraine through Logistics Enabling Node–Romania (LEN-R).

~~(S)~~ The DoD OIG found that U.S. Air Forces in Europe (USAFE) personnel at LEN-R mishandled classified and sensitive mission data. Specifically, USAFE personnel violated DoDI 8170.01, DoD Manual 5200.01, and Secretary of Defense (SecDef) guidance by transmitting official DoD information over public networks using personal electronic devices and non–DoD-controlled electronic messaging systems. This occurred because USAFE did not provide LEN-R personnel with mission-specific classification guidance on the appropriate classification of mission-related information or the equipment necessary to conduct their mission through approved communication platforms. The DoD risked operational security and the success of the DoD's mission to provide Ukraine with defense items through Romania. [redacted]

(U) The report made three recommendations that are considered closed. The report recommended that the USAFE Commander:

- (U) review security classification guidance to determine whether existing guidance is sufficient for personnel to properly mark, store, and disseminate information related to USAFE missions in support of Ukraine;

- (U) provide necessary communications equipment for personnel to perform their mission in accordance with DoD policy; and

- (U) develop guidance and lessons learned on the improper use of non–DoD-controlled electronic messaging systems into USAFE annual trainings and security refreshers on derivative classification and operational security.

(U) Report No. DODIG-2024-002, "Management Advisory: The Protection of Sensitive Mission Data by the Security Assistance Group–Ukraine and Its Subordinate Commands," November 2, 2023

(U) The objective of DODIG-2024-002 was to address discovered issues concerning information security of communications used to manage, track, and coordinate the movement of U.S. defense articles to Ukraine in LEN-P and between LEN-P and external organizations.

~~(CUI)~~ [redacted]

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

~~(CUI)~~ [redacted]

~~(CUI)~~ The report made seven total recommendations—six that are open and one that is closed. [redacted]

~~(CUI)~~ [redacted]

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

(U) The purpose of this management advisory was to provide DoD officials responsible for approving and managing the use of mobile applications with concerns identified during the "Audit of the Defense Digital Service Support of DoD Programs and Operations."[24]

(U) The DoD OIG found that DoD Component personnel used non–DoD-controlled electronic messaging systems 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, non–DoD-controlled electronic messaging systems through public application stores that could pose operational and cybersecurity risks;
- (U) offered non–DoD-controlled electronic messaging system mobile applications through application stores that pose known operational and cybersecurity risks to DoD information and systems; and
- (U) lacked controls to ensure personal use of DoD devices was limited and did not pose operational and cybersecurity risks to the DoD.

(U) The DoD OIG also found that DoD personnel violated policy and misused mobile applications because the DoD does not have a comprehensive mobile device and application policy that addresses the operational and cybersecurity risks associated with the use of mobile devices and applications. In addition, the Defense Information

[24] (U) DoD OIG Report No. DODIG-2024-087, "Audit of the Defense Digital Service Support of DoD Programs and Operations," May 29, 2024.

(U) Systems Agency and other DoD Components did not provide adequate training on the acceptable use of DoD mobile devices or applications.

(U) As a result, the DoD Components' mobile device programs vary widely in the features and applications that users are permitted to access and use. DoD officials may not be aware of the operational and cybersecurity risks that unmanaged applications pose to the DoD. DoD personnel may inadvertently lose or intentionally delete important DoD communications on unmanaged messaging applications. Additionally, mobile applications that are misused by DoD personnel or compromised by malicious actors can expose DoD information or introduce malware into DoD systems.

(U) The report made 16 recommendations, of which 7 are closed and 9 remain open. These included a recommendation to the DoD CIO to direct the DoD Components to immediately require users to forward a complete copy of all official DoD messages generated over unmanaged electronic messaging applications to an official electronic messaging account. The report also recommended that the DoD CIO, in coordination with the USD(I&S), develop comprehensive mobile device and mobile application policy for Components and users that must, at a minimum:

- (U) define the acceptable use of DoD mobile devices and mobile applications for official DoD business and personal use;
- (U) address the cybersecurity and operational security risks of unmanaged applications and mobile device features;
- (U) address the DoD records management requirements of DoD Instruction (DoDI) 5015.02 and the Deputy Secretary of Defense memorandum, "Records Management Responsibilities for Text Messages;"[25]
- (U) require DoD Components to provide regularly scheduled training to DoD mobile device users on the responsible and effective use of mobile devices and applications, including electronic messaging services, in accordance with DoD CIO memorandum, "Mobile Application Security Requirements," and DoDI 8170.01;[26] and
- (U) require DoD Components to justify and approve the mission requirements for all managed and unmanaged applications and limit access to only applications with a justified and approved need.

[25] (U) Deputy Secretary of Defense Memorandum, "Records Management Responsibilities for Text Messages," August 3, 2022.

[26] (U) DoD CIO Memorandum, "Mobile Application Security Requirements," October 6, 2017.

~~(CUI)~~ [redacted]

(U) Report No. DODIG-2022-076, "Evaluation of Combatant Commands' Communication Challenges with Foreign Partner Nations During Coronavirus Disease-2019 Pandemic and Mitigation Efforts," March 28, 2022

(U) The objective of this evaluation was to determine how the U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Indo-Pacific Command, U.S. Southern Command, and their Component commands mitigated communication problems with partner nations during the COVID-19 pandemic and how these mitigation strategies should be employed in future operations when face-to-face interaction is not possible.

~~(S//NF)~~ [redacted]

(U) This occurred because the available DoD tools did not meet all of the needs of combatant command personnel, and foreign partners had technological, cultural, and computer literacy challenges that limited their ability to use DoD-controlled systems.

(U) The report made 13 recommendations, of which 3 remain open. These included recommendations that:

- (U) the DoD CIO conduct a needs assessment to better understand the technological limitations of U.S. foreign partners and how the limitations impact the combatant commands' abilities to communicate and collaborate with foreign partners. This recommendation is closed.

- (U) the USD(I&S) develop policy to strengthen the DoD OPSEC program. This recommendation is closed.

- (U) the USD(I&S) develop OPSEC training requirements on the risks of sharing DoD information on non–DoD-controlled systems and add these requirements to DoD policy. This recommendation remains open.

- (U) the Commanders of the U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Indo-Pacific Command, and U.S. Southern Command: (1) issue command-level guidance tailored to their operational environments that details how personnel in their areas of operations could mitigate risks and comply with DoD policy when using non–DoD-controlled electronic messaging systems and (2) establish risk assessment procedures to evaluate and monitor their personnel's use of current and emerging technologies. The recommendations are closed for the U.S. Africa Command, U.S. Central Command, U.S. European Command, and U.S. Indo-Pacific Command, but remain open for the U.S. Southern Command.

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

(U) This investigation was conducted in response to DoD Hotline complaints against the Director of the Defense Digital Service from March 22, 2020, through June 18, 2020. During the investigation, the DoD OIG concluded that the Director used and condoned his subordinates' use of an unauthorized electronic messaging and voice-calling application to discuss official DoD information.

(U) The Director was found to have used the application regularly to communicate with Defense Digital Service employees and other DoD officials to discuss official information. Of his 11 subordinates, 5 stated that a perception existed that the Director and Defense Digital Service employees used the application to discuss classified or sensitive information. Additionally, 4 of the 11 subordinates stated that a perception existed that the application was used to avoid complying with the Freedom of Information Act (FOIA) and the DoD's record retention policies.

(U) The report recommended that the then SecDef take appropriate action regarding the Director's use of the unauthorized electronic messaging and voice-calling application. The recommendation is now closed.

(U) Report No. DODIG-2021-065, "Evaluation of Access to Department of Defense Information Technology and Communications During the Coronavirus Disease-2019 Pandemic," March 30, 2021

(U) The objective of this evaluation was to determine the extent to which DoD Components provided access to DoD information technology and communications during the COVID-19 pandemic.

(U) The DoD OIG found that some DoD Components did not fully test whether their information systems could support government-wide, mandated telework and did not conduct telework exercises with their personnel, as required by the DoD Implementation Plan and DoD Telework Policy. Some teleworking personnel reported that they found their own alternative solutions, including the use of unauthorized video conferencing applications and personal laptops, printers, and cell phones, to complete their work because some DoD Components were unprepared for maximum telework. However, using unauthorized applications or sharing DoD information over improperly secured devices, even temporarily, increases the risk of exposing sensitive DoD information that could impact national security and DoD missions.

(U) This evaluation made three recommendations, all of which are closed. The recommendations were related to updating and exercising the DoD Implementation Plan for Pandemic Influenza and DoD Components' Pandemic Plans, including updating and including revised planning assumptions regarding DoD telework for personnel and the resources required to support the teleworking workforce. The report also recommended that the Under Secretary of Defense for Policy establish management oversight procedures to verify that DoD Components performed the testing, training, and exercise requirements of the DoD Implementation Plan for Pandemic Influenza and DoD Telework Policy to assess the ability of DoD Components to support government-wide, mandated telework.

(U) Appendix B

(U) Status of Report Recommendations

(U) The seven relevant reports included in this summary report contain 48 combined recommendations. As of September 24, 2025, 26 recommendations were closed and 22 remained open. The table provides the report number, recommendation language, and status of the recommendation.

(U) Table. Recommendations and Implementation Status from Relevant Reports

(U) 48 Total Recommendations

(U) 26 Closed ✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅✅

(U) 22 Open ○○○○○○○○○○○○○○○○○○○○○○

(U) Report	(U) Recommendation		(U) Status
(U) DODIG-2025-006 **1 of 5 Closed**	1	(U) We recommend that the Commander of the Security Assistance Group–Ukraine (SAG-U) direct the Division Tactical Command Post (DTAC) to:	
	1.a	(U) Establish a process to regularly remind U.S. and partner nation personnel to follow applicable DoD information security guidance.	○
	1.b	(U) Develop and implement incident reporting procedures for security violations and establish sanctions for repeated violations.	○
	1.c	(U) Ensure that physical access to the SIPRNet terminal is appropriately controlled.	✅
	1.d	(U) Conduct and document DTAC standard operating procedures training for all movement control personnel.	○
	2	(U) We recommend that the SAG-U Commander review and refine standard operating procedures and recurring compliance inspections to include SIPRNet equipment security, the use of public electronic messaging services, and the presence of personal electronic devices in secure spaces at logistical nodes and Logistics Support Area Eagle.	○

(U) Report	(U) Recommendation		(U) Status
(U) DODIG-2024-109 **3 of 3 Closed**	1	(U) We recommend that the Commander of the U.S. Air Forces in Europe (USAFE):	
	1.a	(U) Conduct a review of USAFE security classification guidance and determine whether existing guidance is sufficient for USAFE personnel to properly mark, store, and disseminate information related to USAFE missions in support of Ukraine, such as those at Logistics Enabling Node–Romania.	✓
	1.a.1	(U) If the Commander determines that existing guidance is insufficient, the Commander should update the USAFE security classification guide and provide notification to squadron information protection officers informing them of the new guidance.	
	1.a.2	(U) If the Commander determines that existing guidance is sufficient, the Commander should issue coordinating instructions to squadron information protection officers on how to apply existing guidance for USAFE missions in support of Ukraine.	
	1.b	(U) Provide necessary communication equipment and gear to the Logistics Enabling Node–Romania team to allow the squadron to perform its security assistance mission in accordance with DoDI 8170.01, DoDM 5200.01, and the SecDef memorandum on DoD information security procedures, April 17, 2023.	✓
	1.c	(U) Develop guidance and lessons learned from the improper classification and use of third-party electronic messaging services identified in this management advisory into USAFE annual trainings and security refreshers on proper derivative classification and OPSEC.	✓
(U) DODIG-2024-002 **1 of 7 Closed**	1	~~(CUI)~~ [redacted]	
	1.a	~~(CUI)~~ [redacted]	○

(U) Report	(U) Recommendation	(U) Status
(U) DODIG-2024-002 (cont'd) **1 of 7 Closed**	1.b ~~(CUI)~~ [redacted]	
	2 ~~(CUI)~~ [redacted]	
	2.a ~~(CUI)~~ [redacted]	
	2.b ~~(CUI)~~ [redacted]	
	2.c ~~(CUI)~~ [redacted]	
	2.d ~~(CUI)~~ [redacted]	
	3 ~~(CUI)~~ [redacted]	

(U) Report	(U) Recommendation		(U) Status
(U) DODIG-2023-041 **7 of 16 Closed**	1	(U) We recommend that the DoD CIO direct the DoD Components to immediately:	
	1.a	(U) Require users to forward a complete copy of all official DoD messages generated over unmanaged electronic messaging applications to an official electronic messaging account.	✓
	1.b	(U) After completion of Recommendation 1.a, remove all unauthorized, unmanaged applications from all DoD mobile devices.	○
	1.c	(U) After completion of Recommendation 1.a, assess all unmanaged applications for operational and cybersecurity risks and remove those with unacceptable risks or without a justifiable need from users' mobile devices and Component application stores.	○
	1.d	(U) Assess mobile device users' access to public application stores and remove access of those without a justifiable need. If unable to remove mobile device users' access, require Components to develop and implement policy that defines the acceptable use of public application stores and requires periodic assessments of mobile device users downloads to determine that all applications have a justifiable need.	○
	2	(U) We recommend that the DoD CIO, in coordination with the Under Secretary of Defense for Intelligence and Security, develop comprehensive mobile device and mobile application policy for Components and users. The policy should, at a minimum:	
	2.a	(U) Define the acceptable use of DoD mobile devices and mobile applications for official DoD business and personal use.	○
	2.b	(U) Address the cybersecurity and operational security risks of: 2.b.1 (U) User access to unmanaged applications without cybersecurity assessments through Component application stores or public application stores. 2.b.2 (U) Mobile device features, including geolocation, screen capture, copy and paste, and camera, among others.	○

(U) Report	(U) Recommendation		(U) Status
(U) DODIG-2023-041 (cont'd) **7 of 16 Closed**	2.c	(U) Address the DoD records management requirements of DoD Instruction 5015.02, and the Deputy Secretary of Defense memorandum "Records Management Responsibilities for Text Messages."	
	2.d	(U) Require DoD Components to provide regularly scheduled training to DoD mobile device users on the responsible and effective use of mobile devices and applications, including electronic messaging services, in accordance with DoD CIO memorandum, "Mobile Application Security Requirements," and DoD Instruction 8170.01. The training should address, at a minimum: 2.d.1 (U) Ethics guidelines to ensure compliance with DoD 5500.07-R, "Joint Ethics Regulation," August 30, 1993 (Incorporating Change 7, November 17, 2011). 2.d.2 (U) Definitions of, difference between, and responsible use of managed and unmanaged applications on DoD mobile devices. 2.d.3 (U) Best practices when using unmanaged applications. 2.d.4 (U) Operational security concerns, potential threats, and risks associated with using unmanaged applications, which may contain capabilities such as location sharing (GPS tracking), personal information sharing, or may have nefarious characteristics (for example, marketing scams, and human trafficking). 2.d.5 (U) Cybersecurity concerns associated with using unmanaged applications, which may contain malware or spyware. 2.d.6 (U) Privacy-related concerns. 2.d.7 (U) Records management requirements to ensure compliance with DoD Instruction 5015.02. 2.d.8 (U) Information review for clearance and release authorization procedures. 2.d.9 (U) Accessibility standards to ensure compliance with DoD Manual 8400.01, "Accessibility of Information and Communications Technology," November 14, 2017.	

(U) Report	(U) Recommendation		(U) Status
(U) DODIG-2023-041 (cont'd) **7 of 16 Closed**	2.e	(U) Require DoD Components to justify and approve the mission requirements for all managed and unmanaged applications and limit access to only those applications with a justified and approved need.	○
	3	(U) We recommend that the DoD CIO, in coordination with the Defense Information Systems Agency CIO, revise DoD policy and memorandums and Defense Information Systems Agency mobile application documentation and training to ensure the use of common terminology when referring to approved, managed, DoD-controlled, authorized, and official applications and unmanaged, non–DoD-controlled, unauthorized, nonofficial, and personal-use applications.	○
	4	(U) We recommend that the Defense Information Systems Agency CIO:	
	4.a	(U) Update the DoD Mobility Unclassified Capability service to provide Component mobile device managers reports and data regularly, at least quarterly, of the mobile applications downloaded to the mobile devices within the manager's area of responsibility.	✓
	4.b	(U) Publish a clear list of applications approved for official DoD business and make the list easily accessible from DoD mobile devices.	✓
	4.c	(U) Develop and implement policy to conduct periodic reviews, at least annually, of the list of authorized unmanaged applications and remove those without a justifiable need or with known cybersecurity risks.	✓
	4.d	(U) Remove or hide any unauthorized, unmanaged applications from the mobile devices of users who cannot demonstrate a justifiable need for the application.	✓
	4.e	(U) Revise the "New Application Request" form to ask whether the Component intends to use the application to conduct official DoD business and process requests that have the answer "Yes" to this question as managed applications.	✓

(U) Report	(U) Recommendation		(U) Status
(U) DODIG-2023-041 (cont'd) **7 of 16 Closed**	5	~~(CUI)~~ [redacted]	✓
(U) DODIG-2022-076 **10 of 13 Closed**	1	(U) We recommend that the DoD CIO, in coordination with the Under Secretary of Defense for Intelligence and Security, conduct a needs assessment to better understand the technological limitations of U.S. foreign partners and how they impact the combatant command's ability to communicate and collaborate with these partners. This assessment should inform recommendations for DoD enterprise technology solutions to improve communications interoperability with foreign partners.	✓
	2	(U) We recommend that the Under Secretary of Defense for Intelligence and Security:	
		2.a (U) Develop policy to strengthen the DoD OPSEC program and promote integration of OPSEC into future DoD operations and activities to mitigate the risks of using non–DoD-controlled electronic messaging systems.	✓
		2.b (U) Develop OPSEC training requirements on the risks of sharing DoD information on non–DoD-controlled systems and add these requirements to the existing training requirements described in DoD Instruction 8170.01 and DoD Directive 5205.02E.	○
	3	(U) We recommend that the Commanders of the U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Indo-Pacific Command, and U.S. Southern Command:	

(U) Report	(U) Recommendation		(U) Status
(U) DODIG-2022-076 (cont'd) **10 of 13 Closed**	3.a	(U) Issue command-level guidance clarifying the use of non–DoD-controlled electronic messaging systems. This guidance should include: 3.a.1 (U) Any area of responsibility-specific conditions that permit personnel to use non--DoD-controlled messaging systems. 3.a.2 (U) What information can be shared over the electronic messaging system. 3.a.3 (U) How personnel are to maintain records generated on non-DoD systems in accordance with records management regulations. 3.a.4 (U) How to report any security violations or misuse of a system. 3.a.5 (U) A process to ensure that any use of non--DoD-controlled electronic messaging systems meets the exception criteria in DoD Instruction 8170.01. 3.a.6 (U) Additional training criteria for personnel that address the risks of using non-DoD electronic messaging systems, violating OPSEC regulations, and consequences of noncompliance.	(U) U.S. Africa Command/ U.S. Central Command/ U.S. European Command/ U.S. Indo-Pacific Command ✓ U.S. Southern Command ○
	3.b	(U) Establish risk assessment procedures to evaluate and monitor combatant command use of current and emerging information technologies to identify opportunities for use and to assess risks in accordance with DoD Instruction 8170.01.	(U) U.S. Africa Command/ U.S. Central Command/ U.S. European Command/ U.S. Indo-Pacific Command ✓ U.S. Southern Command ○
(U) DODIG-2021-092 **1 of 1 Closed**	1	(U) We recommend that the Secretary of Defense take appropriate action regarding Mr. Goldstein's use of an unauthorized electronic messaging and voice-calling application.	✓
(U) DODIG-2021-065 **3 of 3 Closed**	1	(U) We recommend that the Assistant Secretary of Defense (Homeland Defense and Global Security) revise the DoD Implementation Plan for Pandemic Influenza to:	

(U) Report	(U) Recommendation		(U) Status
(U) DODIG-2021-065 (cont'd) **3 of 3 Closed**	1.a	(U) Update the planning assumptions in the DoD Implementation Plan for Pandemic Influenza to include the use of telework for essential and nonessential personnel and to align the DoD Implementation Plan for Pandemic Influenza with the DoD Telework Policy, Enclosure 3, section 3(i)(2).	✓
	1.b	(U) Require DoD Components to update their Pandemic Plans to include the revised assumptions regarding telework for essential and nonessential personnel and the resources required to support the teleworking workforce.	✓
	2	(U) We recommend that the Under Secretary of Defense for Policy, in coordination with the Under Secretary of Defense for Personnel and Readiness, establish management oversight procedures to verify that DoD Components performed the testing, training, and exercise requirements of the DoD Implementation Plan for Pandemic Influenza and the DoD Telework Policy. The oversight procedures should assess the ability of DoD Components to support Government-wide mandated telework, including the results from tests of network and communications systems and telework exercises with personnel.	✓

Source: The DoD OIG.

(U) Appendix C

(U) Summary of DoD CUI, Classification, and Declassification Policy and Processes

(U) This appendix summarizes parts of DoD CUI policy and DoD policies and procedures for classifying and declassifying classified information.

(U) The DoD protects all nonpublic DoD information, but it has special policies and procedures for controlled unclassified and classified information. According to 32 C.F.R. § 2002.4, CUI is "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls." CUI is not classified.

(U) According to Executive Order 13526, "Classified National Security Information," information can be classified at either the TOP SECRET, SECRET, or CONFIDENTIAL levels.[27] TOP SECRET is applied to information that, if disclosed without authorization, could reasonably be expected to cause *exceptionally grave damage* to national security. SECRET is applied to information that, if disclosed without authorization, could reasonably be expected to cause *serious damage* to national security. CONFIDENTIAL is applied to information that, if disclosed without authorization, could reasonably be expected to cause *damage* to national security.

(U) Controlled Unclassified Information Policy

(U) DoD Instruction (DoDI) 5200.48 establishes policy, assigns responsibilities, and prescribes procedures for CUI throughout the DoD in accordance with Executive Order 13556, "Controlled Unclassified Information."[28] The DoDI states that all DoD CUI must be protected until authorized for public release, including by limiting access and using handling, marking, and dissemination controls and other protective measures for safeguarding the information. For example, DoD information systems that process, store, or transmit CUI have to meet specific cybersecurity and risk management requirements.

(U) The authorized holder of a document or material is responsible for determining, at the time of creation, whether information in a document or material falls into a CUI category. The DoD CUI Registry, which mirrors the National CUI Registry, provides an official list of the indexes and categories used to identify the various types of DoD CUI.

[27] (U) Executive Order 13526, "Classified National Security Information," December 29, 2009.

[28] (U) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010.

(U) If information falls into a CUI category, the authorized holder is responsible for applying CUI markings and dissemination instructions accordingly. Information will not be designated CUI to:

- (U) conceal violation of law, inefficiency, or administrative error;
- (U) prevent embarrassment to a person, organization, or agency;
- (U) prevent open competition; or
- (U) control information not requiring protection under a law, regulation, or government-wide policy, unless by the CUI Executive Agent at the National Archives and Records Administration through the USD(I&S).

(U) Original classification authorities will determine if aggregated CUI under their control should be classified in accordance with DoD Manual (DoDM) 5200.01, Volume 1, and will confirm that the relevant security classification guides address the compilation.

(U) The originator of information, original classification authority (OCA), or designated offices for decontrolling CUI will decontrol and release CUI records. Decontrol of CUI occurs when the CUI no longer requires safeguarding and follows DoD records management procedures, unless specifically required by a law, regulation, or government-wide policy. Additionally, the DoD originator or authorized CUI holder must ensure a prepublication and security policy review is conducted before CUI is approved for public release.

(U) Classification Process for CONFIDENTIAL, SECRET, and TOP SECRET Information

(U) DoDM 5200.01, Volume 1, provides guidance for classifying and declassifying DoD information that requires protection in the interest of national security. DoD policy states to classify and declassify national security information in accordance with Executive Order 13526 and 32 C.F.R. parts 2001 and 2002.

(U) DoDM 5200.01 says that information will be classified only to protect national security. If significant doubt exists about the need to classify information, it will not be classified. Unnecessary or higher than necessary classification is prohibited by Executive Order 13526. Information will be declassified as soon as it no longer qualifies for classification.

(U) According to DoDM 5200.01, Volume 1, Enclosure 4, classification may be applied only to information that is owned by, produced by or for, or is under the control of the U.S. Government. Information may be considered for classification only if its

(U) unauthorized disclosure: (1) could reasonably be expected to cause identifiable or describable damage to national security and (2) concerns one of the categories specified in Executive Order 13526.[29]

(U) Enclosure 4 also describes the original classification process. In making a decision to originally classify information, an OCA will determine or document that the information:

- (U) is owned by, produced by or for, or is under the control of the U.S. Government;
- (U) falls in one or more of the categories of classifiable information;
- (U) was not already classified by another OCA;
- (U) is not covered by already available classification guidance;[30]
- (U) has a reasonable possibility that it can be protected from unauthorized disclosure;[31] and
- (U) is assigned the appropriate level of classification (TOP SECRET, SECRET, or CONFIDENTIAL) based on reasoned judgment as to the degree of damage, which the OCA can describe, that could be caused by unauthorized disclosure. If significant doubt exists about the appropriate level of classification, it will be classified at the lower level.

(U) If an OCA must make their decision verbally because of exigencies of an ongoing operation or other emergency, they must issue written confirmation within 7 calendar days of the decision and provide the required declassification and marking instructions.

[29] (U) The categories of classifiable information include: (1) military plans, weapon systems, or operations; (2) foreign government intelligence; (3) intelligence activities, sources or methods, or cryptology; (4) foreign relations or foreign activities of the United States, including confidential sources; (5) scientific, technological, or economic matters relating to national security; (6) U.S. Government programs for safeguarding nuclear materials or facilities; (7) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security; or (8) the development, production, or use of weapons of mass destruction.

[30] (U) In the DoD, the majority of existing classification guidance is indexed and promulgated through the Defense Technical Information Center, available at www.dtic.mil.

[31] (U) OCAs will balance the cost to protect the information against the risks associated with its disclosure. The advantages must outweigh the disadvantages of classification.

(U) OCAs must also:

- (U) be prepared to produce a written description of the damage, as necessary, for a classification challenge, security classification review, damage assessment, request for mandatory review for declassification, or request for release when pertinent to judicial proceedings or as statutes or regulations may require;
- (U) determine the appropriate duration of classification to be applied to the information; and
- (U) document the classification decision and clearly and concisely communicate it in writing to people who will possess the information by issuing classification guidance or by ensuring documents containing the information are properly marked to reflect the decision.[32]

(U) Declassification Process

(U) According to DoDM 5200.01, Volume 1, Enclosure 5, information will be declassified as soon as it no longer meets the standards for classification. Executive Order 13526 establishes the following four separate and parallel processes for declassifying information.

- (U) At the time of classification, the OCA will establish a specific date or event for declassification based on the duration of the information's national security sensitivity.
- (U) Automatic declassification is a system for declassifying information in permanently valuable historical records. Information is automatically set to declassify 25 years after the time of classification because of its permanent historical value unless action is taken to keep it classified longer.
- (U) Any individual or organization can request the mandatory declassification review process. The heads of DoD Components are required to have established processes for responding to these requests.
- (U) A systematic review is a process to review information in a DoD Component's custody for possible declassification.

(U) According to DoDM 5200.01, information may be declassified or downgraded by the responsible OCA, the OCA's supervisory official if they have OCA, or the officials with delegated declassification authority. The authority to declassify information

[32] (U) Classification guidance may be communicated by issuing a security classification or declassification guide or in the form of a memorandum, plan, order, or letter. If issued by anything other than a classification or declassification guide, the guidance should be incorporated in a guide in a timely fashion.

(U) extends only to information for which the specific official has classification, program, or functional responsibility.

(U) DoDM 5200.01 states that classified information will be marked as declassified before it is handled as unclassified. Declassification markings are used to clearly convey the declassified status of the information and who authorized the declassification. DoDM 5200.01 further states that "Persons with declassification authority shall develop and issue declassification guidance to facilitate effective review and declassification of information." It adds that guidance may be in the form of declassification guides, sections of security classification guides, or memorandums.

(U) Appendix D

(U) Chronological Summary of DoD Policy and Guidance for Electronic Messaging Systems

(U) The DoD issued at least 10 policies and memorandums since 2015 that discuss: (1) the prohibited use of non–DoD-controlled electronic messaging systems, with limited exceptions; (2) the requirement to protect nonpublic DoD information; and (3) records retention. We listed these policies and memorandums in chronological order to demonstrate how the DoD continuously informed personnel of their responsibilities for protecting and preserving DoD information.

(U) February 2015: DoDI 5015.02, "DoD Records Management Program"

(U) DoDI 5015.02 establishes policy and assigns responsibilities for managing DoD records in all media, including electronic. DoDI 5015.02 states that nonofficial electronic messaging accounts, with very few exceptions, must not be used to conduct official DoD communications in accordance with DoDI 8550.01, "DoD Internet Services and Internet-Based Capabilities."[33] It also states that if a DoD employee uses a nonofficial electronic messaging account, the employee must copy the message to their official electronic messaging account when the record is first transmitted or forward a complete copy of the record to their official electronic messaging account within 20 days of the record's original creation or transmission, pursuant to Title 44 U.S. Code.

(U) April 2016: DoD CIO Memorandum, "Use of Non-Official Electronic Messaging Accounts and Records Management"

(U) The DoD CIO sent this memorandum to senior DoD officials to provide clarifying guidance about using non–DoD-controlled electronic messaging systems and existing DoD records management policies.[34] In the memorandum, the DoD CIO provided the following examples that might warrant the use of nonofficial electronic messaging accounts.

- (U) Official messaging accounts are not available and mission requirements require the use of a nonofficial messaging account to communicate.

[33] (U) DoDI 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012, was incorporated into and cancelled by DoDI 8170.01. DoDI 8550.01 states that, "barring absence of official communication channels, personal accounts shall not be used to conduct official DoD communication."

[34] (U) DoD CIO Memorandum, "Use of Non-Official Electronic Messaging Accounts and Records Management," April 6, 2016.

- (U) Technological difficulties make the use of available messaging accounts impractical or unreliable.

- (U) Use of an official messaging account would substantially delay or hinder the transmission of purely administrative communications or would be inconsistent with the individual's ability to conduct work efficiently.

(U) The DoD CIO's memorandum also stated that, if circumstances exist that would warrant use of a nonofficial electronic messaging account, DoD personnel: (1) must never transmit classified information on that account and (2) should use good judgment regarding the transmission of other potentially sensitive information. Finally, the DoD CIO reiterated that DoD personnel who use any nonofficial electronic messaging account to conduct official business must copy the message to their official electronic messaging account at the time of creation or within 20 days after transmitting the original message.

(U) January 2018: Deputy Secretary of Defense Memorandum, "Conducting Official Business on Electronic Messaging Accounts"

(U) Deputy Secretary of Defense (DepSecDef) Patrick Shanahan sent this memorandum to all DoD personnel to remind them to use their official DoD email or other official DoD electronic messaging accounts when conducting DoD business.[35] In this memorandum for all DoD personnel, the DepSecDef stated that law and DoD policy are clear: "non-official electronic messaging accounts," including personal email accounts, "must not be used to conduct official DoD communications, with very few exceptions, and intentional violations of this may be the basis for disciplinary actions." The DepSecDef clarified that a DoD official being out of the office, without access to official communication channels, and needing to send an urgent, DoD, mission-related email is an example of an extraordinary circumstance when a personal or other nonofficial email account may be used for official business. The DepSecDef also referred DoD personnel to the DoD CIO's April 6, 2016 memorandum for examples of exceptions to this policy.

(U) January 2019: DoDI 8170.01, "Online Information Management and Electronic Messaging"

(U) DoDI 8170.01 establishes policy, assigns responsibilities, and prescribes procedures for conducting, establishing, operating, and maintaining electronic messaging services to collect, distribute, store, and otherwise process unclassified and classified official

[35] (U) DepSecDef Memorandum, "Conducting Official Business on Electronic Messaging Accounts," January 16, 2018.

(U) DoD information.[36] According to DoDI 8170.01, DoD policy states that DoD personnel must:

- (U) "continue to innovate through electronic messaging services to achieve capabilities that are faster, better, and less expensive, while simultaneously ensuring implementation of cybersecurity appropriate for the risks and the magnitude of harm that could result from the loss, compromise, or corruption of the information;"

- (U) "not use personal email or other nonofficial accounts to exchange official information and must not auto-forward official messages to nonofficial accounts or corporate accounts;" and

- (U) "conduct online information management and electronic messaging, regardless of the information technology or format used, in compliance with applicable laws, regulations, this issuance, and the references cited throughout."

(U) DoDI 8170.01 clearly states, "Do not use non–DoD-controlled electronic messaging services to process nonpublic DoD information, regardless of the service's perceived appearance of security." It continues by saying that the Office of the Secretary of Defense and DoD Component heads "may approve the establishment of non–DoD-controlled electronic messaging services accounts by authorized users for public communication related to assigned duties ... or any other purpose deemed necessary and in the interest of the U.S. Government."

(U) DoDI 8170.01 states that DoD personnel may not use their personal, nonofficial accounts to conduct official DoD communications unless: (1) the use is an emergency or other critical mission need; (2) official communication capabilities are unavailable, impractical, or unreliable; and (3) the use is in the DoD's or U.S. Government's interest. Personal, nonofficial accounts may not be used for personal convenience or preferences.

[36] (U) DoDI 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019 (Incorporating Change 2, March 12, 2025).

(U) DoDI 8170.01 also states that, consistent with 44 U.S.C. § 2911:

> (U) an officer or employee of an executive agency may not create or send a record using a nonofficial electronic messaging account unless the officer or employee:
>
> (U) (1) copies an official electronic messaging account of the officer or employee in the original creation or transmission of the record; or
>
> (U) (2) forwards a complete copy of the record to an official electronic messaging account of the officer or employee no later than 20 days after the original creation or transmission of the record.

(U) March 2020: DoDI 5200.48, "Controlled Unclassified Information (CUI)"

(U) DoDI 5200.48 establishes policy and the official DoD CUI Registry, assigns responsibilities, and prescribes procedures for CUI throughout the DoD. DoDI 5200.48 also discusses the prohibited use of non–DoD-controlled electronic messaging systems, with limited exceptions; the requirement to protect nonpublic DoD information; and records retention. DoDI 5200.48 states that:

> (U) DoD personnel will not use unofficial or personal e-mail accounts, messaging systems, or other non-DoD information systems, except approved or authorized government contractor systems, to conduct official business involving CUI. This is necessary to ensure proper records retention and to help remediate data spillage in accordance with the Presidential and Federal Records Act Amendments of 2014 and the January 16, 2018 Deputy SecDef memorandum.[37]

(U) Appendix C includes a comprehensive summary of CUI policy.

(U) March 2020: DoD CIO Memorandum, "COVID-19 Response: Remote Work Capability"

(U) The DoD CIO sent this memorandum to DoD senior officials to remind DoD personnel to use the same discipline, awareness, and security measures when working remotely as required for on-site work.[38] In this memorandum, the DoD CIO's Chief of Staff distributed refresher guidance on defending the DoD information network with "do's" and "don'ts" to DoD senior officials for dissemination to their components. One of the don'ts listed under the cybersecurity guidance on defending the DoD

[37] (U) Presidential and Federal Records Act Amendments of 2014, Pub. L. No. 113-187, November 26, 2014.

[38] (U) DoD CIO Memorandum, "COVID-19 Response: Remote Work Capability," March 19, 2020.

(U) information network stated, "[Do not] use any non-DoD instant messaging applications to share DoD information."

(U) July 2020: Secretary of Defense Memorandum, "Strengthening Operations Security and Preventing Unauthorized Disclosures"

(U) Secretary of Defense (SecDef) Mark Esper sent this memorandum to senior DoD officials to inform DoD personnel of their responsibilities for protecting information.[39] In this memorandum, the SecDef stated that protecting information, a key part of operations security (OPSEC), is crucial to maintaining our advantage against adversaries who seek to degrade our operations, put the safety of our personnel at risk, or prevent our mission success. In addition, poor OPSEC practices may result in unauthorized disclosures of nonpublic information, including classified national security information and CUI. Furthermore, the SecDef stated that all DoD personnel must accept responsibility and accountability for their actions, fully commit to improving their OPSEC practices, prevent unauthorized disclosures, and increase awareness and application of safeguards to reduce the loss and misuse of information.

(U) June 2021: Office of the Under Secretary of Defense for Intelligence and Security Memorandum, "Information and Operations Security Risks Posed by Non-Government Websites and Applications"

(U) The Office of the Under Secretary of Defense for Intelligence and Security sent this memorandum to senior Pentagon leadership, the commanders of the combatant commands, and Defense agency and DoD field activity directors.[40] It requested their assistance to ensure that their information security and OPSEC programs had safeguards to prevent unauthorized disclosures, such as posting nonpublic information to a closed group on a commercial social media platform even if all members of the group are otherwise authorized to receive the information. The memorandum stated that these platforms can often be breached, and the use of privacy or other security settings does not change the fact that the information is stored on non-government servers that may not provide a level of protection that meets Government standards.

(U) August 2022: DoDI 5400.17, "Official Use of Social Media for Public Affairs Purposes"

(U) DoDI 5400.17 provides core principles regarding social media use in the DoD, guidance regarding records management procedures for social media accounts, and

[39] (U) SecDef Memorandum, "Strengthening Operations Security and Preventing Unauthorized Disclosures," July 20, 2020.

[40] (U) Office of the Under Secretary of Defense for Intelligence and Security Memorandum, "Information and Operations Security Risks Posed by Non-Government Websites and Applications," June 22, 2021.

(U) guidance on personal social media use by DoD personnel.[41] The DoDI says that "release of unauthorized content through any means, including social media, may unnecessarily hazard individuals, units, and the mission." Furthermore, it says not to conduct official business on personal social media accounts, in accordance with DoDI 8170.01 and 44 U.S.C. § 2911, and that "a personal social media account must not be an avenue for friends, followers, or private contacts to gain access to DoD programs or seek action from DoD officials in a manner not available to the general public."

(U) April 2023: SecDef Memorandum, "Immediate Review and Assessment of Department of Defense Information Security Procedures"

(U) SecDef Lloyd Austin sent this memorandum to all DoD personnel as a reminder of the importance of adhering to required security procedures, including the requirement to transmit classified national security information only over secure communications networks approved for the transmission of information at the specified level of classification.[42] The memorandum also reminds DoD personnel that, in accordance with DoDI 8170.01, non–DoD-controlled electronic messaging systems are not authorized to process nonpublic DoD information.

(U) October 2023: DoD CIO Memorandum, "Use of Unclassified Mobile Applications in Department of Defense"

(U) The DoD CIO sent this memorandum to senior Pentagon leadership, the commanders of the combatant commands, and Defense agency and DoD field activity directors to provide guidance on the use of mobile applications on unclassified, DoD, government-owned, -leased, or -issued mobile devices. This memorandum states that the misuse and mismanagement of mobile applications poses a cybersecurity and OPSEC risk and may result in the unauthorized disclosure of CUI and unclassified DoD information that was not approved for public release. In addition, the memorandum emphasizes that unmanaged applications are prohibited from accessing, transmitting, storing, or processing nonpublic DoD information, including CUI, in accordance with DoDI 5200.48. All applications that access, transmit, store, or process nonpublic DoD information must comply with the DoD Records Management Program. Any record created or received and not captured in a DoD records system must be transferred to a DoD records system within 20 days of creation or receipt.

[41] (U) DoDI 5400.17, "Official Use of Social Media for Public Affairs Purposes," August 12, 2022 (Incorporating Change 2, February 14, 2025)

[42] (U) SecDef Memorandum, "Immediate Review and Assessment of Department of Defense Information Security Procedures," April 17, 2023.

(U) Management Comments

(U) Office of the Under Secretary of Defense for Intelligence and Security

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE
AND SECURITY

SEP 3 2025

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR EVALUATIONS PROGRAMS, COMBATANT COMMANDS AND OPERATIONS

SUBJECT: Management Comments on Inspector General Project No. D2025-DEV0OC-0094.000

On behalf of the Under Secretary of Defense for Intelligence and Security (USD(I&S)), I appreciate your team evaluating DoD policies related to government employees sharing sensitive and classified information on non-governmental networks and electronic applications. I concur with your assessment that DoD personnel's unauthorized use of non-DoD-controlled electronic messaging systems could jeopardize DoD operations or missions. I also appreciate your recognition that DoD has already issued policy related to the use of non-DoD controlled devices and messaging applications and has issued a series of memorandums from 2016 to 2023 to emphasize information security procedures.

The attachment contains specific responses for each of the report's recommendations directed to the USD(I&S). We take the protection of critical, sensitive, and classified information very seriously. My point of contact for this effort is [redacted]

John P. Dixson
Director for Defense Intelligence
Counterintelligence, Law Enforcement,
& Security

Attachment

(U) Office of the Under Secretary of Defense for Intelligence and Security (cont'd)

Attachment

Recommendation 2.: We recommend that the Under Secretary of Defense for Intelligence and Security:

a. Conduct an Office of the Secretary of Defense- and DoD-wide assessment to identify the extent of DoD personnel using non-DoD-controlled electronic messaging services to conduct official business and associated risks.

Partially Agree. The Office of the USD(I&S) (OUSD(I&S) disagrees with conducting an assessment on the extent of DoD personnel using non-DoD-controlled electronic messaging services to conduct official business, but agrees with conducting a risk assessment of such use.

OUSD(I&S) has previously assessed whether the DoD and OSD Components are aware of the policy regarding the use of non–DoD-controlled messaging applications. The Fiscal Year 2023-2024 Operations Security (OPSEC) Data Call, tasked to all OSD and DoD Component OPSEC-representatives, asked if "*Component leaders, supervisors, and subordinates are aware of, and trained to understand the risk to DoD personnel, on and off duty, and to our military operations from using non-government websites and applications to post information or communicate DoD information that was not approved for public release?*" Ninety-six percent (96%) of responding DoD Components responded "yes," indicating that the ongoing issue is not a lack of policy or awareness, but of compliance. As your report—and prior IG reports —found, there is likely widespread use of non-DoD controlled messaging services by OSD and DoD personnel to conduct official business, negating the benefit of an OSD- and DoD-wide assessment to guide policy development.

OUSD(I&S) cannot conduct an assessment of the extent of the use by DoD-personnel of non-DoD-controlled electronic messaging services in any manner that would be accurate or useful. The USD(I&S) does not have the authority to broadly access Office of the Secretary of Defense (OSD) and DoD personnel's government-issued devices for such purposes. Moreover, it is presumed that DoD IG is not requesting a direct assessment of personally-owned devices. With regard to such an assessment on DoD-owned devices, any such assessment should be conducted by the DoD Chief Information Officer (CIO) through the DoD components that issue and maintain such devices.

- DoD cannot perform a technical assessment of DoD personnel's private phones for such usage without legal process or their consent, which we are unlikely to receive given the significant privacy concerns.
- Although DoD could conduct a technical assessment of DoD personnel's government-issued phones, the mere presence of a non-DoD-controlled electronic messaging service on the phone is not indicative of its use for official business: DoD currently allows the installation and use of such services on government-issued phones for personal use only. To conduct an accurate assessment DoD would need to examine the actual content sent and received using those services on the government-issued phones, which implicates various legal issues and privacy concerns.
- OUSD(I&S) does not expect that a survey asking DoD personnel whether they use non-DoD-controlled electronic messaging services for official business in violation of policy and/or law would be approved or generate results that would be helpful for policy purposes.

(U) Office of the Under Secretary of Defense for Intelligence and Security (cont'd)

Instead, OUSD(I&S) will include questions on the next DoD-wide OPSEC Data Call (tentatively scheduled for 2027) asking:

1. Are DoD Component leaders and supervisors aware whether DoD personnel under their supervision are using non–DoD-controlled electronic messaging services to conduct official business? This would be accompanied by a caveat that leaders and supervisors are not to pose this question directly to their workforce.
2. Have DoD Component leaders and supervisors taken any actions regarding the use of non–DoD-controlled electronic messaging services to conduct official business, including permitting such use?

b. Provide the findings and any recommendations of the assessment in Recommendation 2.a to the DoD Chief Information Officer (CIO) to help inform the requirements for the capability described in Recommendation 1.a.

OUSD(I&S) agrees to provide the findings and recommendations of the risk assessment described in the response to Recommendation 2.a. to the DoD CIO, in lieu of the original assessment recommended.

OUSD(I&S) will also provide DoD CIO with the results of two other OUSD(I&S)-funded efforts related to unauthorized disclosures (UDs) that could be of benefit to the DoD CIO in developing requirements for the capability described in Recommendation 1.a.:

- A 2013 RAND study, "Fixing Leaks: Assessing the Department of Defense's Approach to Preventing and Deterring Unauthorized Disclosures," assessed DoD personnel's motivation to commit intentional UDs as political impetus, ego gratification, cultivating goodwill with the media, whistleblowing, self-interest for personal or professional advantage, and claiming an exercise of free speech.
- A 2022 Applied Research Laboratory for Intelligence and Security (ARLIS) research project on UDs, "Trusted Insiders and the Temptation to Talk: Preventing Unauthorized Disclosures," concluded DoD personnel's motivation to commit UDs stemmed from feelings of demoralization, resentment, and alienation as well as ineffective training and managers who believe they "outrank" the need for training and are impervious to any adverse consequences.

2

(U) DoD Chief Information Officer

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

SEP 18 2025

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: (U) Review and Comment of DoD Inspector General "Evaluation of DoD Policy and Oversight Reports Related to Using Non–DoD-Controlled Electronic Messaging Systems to Conduct Official Business" Draft Report (D2025-DEV0PC-0094.000)

(U) This is the Department of Defense (DoD) Chief Information Officer (CIO) "revised" response to the subject DoD Inspector General draft report:

(U) DoD IG Recommendation 1: We recommend that the DoD Chief Information Officer:

a. (U) Source and maintain DoD-controlled capabilities that meet the DoD's operational needs to share information across the DoD and U.S. Government and with foreign partners. The capabilities should include the ability to communicate on DoD-approved and non-DoD personnel mobile devices, collaborate in group environments, and share unclassified, controlled, and classified information; have a user-friendly interface; and comply with DoD and government-wide requirements to protect information and preserve official records.

b. (U) Develop and implement a tailored training with a knowledge assessment for DoD political appointees, general officers, flag officers, and members of the Senior Executive Service that includes the elements in DoDIG-2023-041 Recommendation 2.d and its sub-elements.23.

c. (U) Clearly define the criteria, process, and personnel authorized to grant a waiver to the DoD's prohibition against using non–DoD-controlled electronic messaging services to conduct official business in DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," and related policies.

d. (U) Update the annual DoD-wide cyber training to include information about the impacts of unauthorized disclosures on non-government applications and risks of using non–DoD-controlled electronic messaging services.

(U) DoD CIO Response:

(U) **Recommendation 1.a.:** The DoD CIO partially agrees with this recommendation. The DoD current suite of controlled capabilities demonstrably reflects the commitment to secure and efficient communication. From dedicated networks for unclassified information to hardened, highly secure systems for classified data, DoD maintains a comprehensive, layered architecture designed to protect information at all sensitivity levels. Complementing these networks are robust collaboration tools for teamwork and secure file transfer mechanisms for safely exchanging data with internal and external partners. Additionally, specialized mobile capabilities are provided for DoD-approved devices, operating under stringent security controls, offering a diverse set of resources specifically designed to meet the needs of warfighters and partners.

(U) DoD Chief Information Officer (cont'd)

(U) The DoD continuously adapts its security measures, upgrades its technological infrastructure, and modernizes its platforms to source and adopt new technology while staying ahead of evolving threats. This includes actively performing regular security audits, enhancing vulnerability management, integrating robust threat intelligence, and maintaining comprehensive user training programs. By staying proactive and building on its existing capabilities framework, the DoD continuously improves the efficiency and security of its operations.

(U) The current capability does not fully meet Combatant Commander's (COCOM) requirements to securely share unclassified messages with coalition partners. The Department continues to investigate, test, and deploy options to communicate faster, more securely, and in a more user-friendly fashion with foreign partners that do not have access to the capabilities used within the Department.

(U) In accordance with Department policy, each DoD Component develops and fields capabilities that meet their specific mission requirements. DoD policies enable Components to meet their information sharing and communications requirements such as Controlled Unclassified Information (CUI), mobile applications security, records management, and the Bring Your Own Devices (BYOD) program. DoD components are permitted to establish BYOD programs in accordance with the 2022 DoD CIO Memorandum, "Use of non-Government owned Mobile Devices." Users of such devices can only process, transmit, or display up to CUI information using managed mobile applications in accordance with the 2023 DoD CIO Memorandum, "Use of Unclassified Mobile Applications in Department of Defense."

(U) The use of unclassified government devices and BYOD devices for classified information sharing and communication (including Confidential, Secret and Top Secret) is prohibited by DoD policy and not viable due to national security systems requirements. There is a small number of government-owned multi-security domain devices that are available to senior leadership for use. DoD CIO continues to investigate how to improve the performance of these devices and develop newer and more efficient designs.

(U) Additionally, all personnel must complete required training and sign a user agreement before being granted mobile device access, understand the risks of data spillage, and comply with both DoD-wide and local security policies to safeguard sensitive and classified information. Violations of the requisite published policies and guidance can result in disciplinary action, security clearance revocation, or legal consequences.

(U) Recommendations 1.b.: DoD CIO partial-agrees with this recommendation. DoD CIO recommends that this recommendation be re-written as follows: Recommendation 1. b. (U) The DoD CIO in coordination with Undersecretary of Defense for Intelligence and Security (USD-I&S) and in conjunction with the Director of Administration and Management (DAM) establish guidance for the development, implementation, and provision of personalized one-on-one training, with a knowledge assessment for DoD political appointees, general officers, flag officers, and members of the Senior Executive Service based on the current and existing training required to be taken by all DoD Civilian, Military and Contract employees prior to gaining

2

(U) DoD Chief Information Officer (cont'd)

access to Unclassified and Classified systems and infonnation. This "Senior Official" training will be provided and given to the respective Senior Officials by the direct supporting Security/Access Control Official/Office for the same officials. The DoD CIO recommends removing in its entirety any/all references (to include footnotes) to the open recommendations contained in DODIG-2023-041, in that the responsible DoD CIO staff have worked tirelessly to answer and provide supporting documentation in support of and have staffed a memo for PTDO DoD CIO signature recommending closure of all remaining open recommendations as actions have been addressed and completed. This memo is currently pending the completion of OGC legal review.

(U) Recommendations 1.c.: DoD CIO agrees with this recommendation. There is confusion between the Secretary of Defense Memo signed 17 Apr 2023, *Immediate Review and Assessment of Department of Defense Information Security Procedures*, DoD Instruction 8170.01, and the 2023 DoD Memorandum, *Use of Unclassified Mobile Applications in Department of Defense*, on the criteria, process, and personal authorized to grant a waiver. DoD CIO will update all associated policies to ensure the process and the approver for any messaging waivers is consistent.

(U) Recommendations 1.d.: DoD CIO disagrees with this recommendation. An update to the annual DoD-wide cyber training to include information about the impacts of unauthorized disclosures on non-government applications and risks of using non–DoD-controlled electronic messaging services would be a redundant and non-cost/resource effective undertaking. The subject matter of unauthorized disclosure while using messaging applications is included in the student guide, online training course, and assessment/examination for the DoD-wide "Unauthorized Disclosure of Classified Information and CUI" training course, which is currently required annual training for all DoD personnel who have access to and use DoD information systems and information at all classification levels.

(U) The draft report has also been reviewed for proper security markings; there are no recommendations for revision or change of them.

(U) The DoD CIO point of contact for this matter in [redacted] DoD CIO Audits Liaison, who may be reached at [redacted]

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

(U) List of Classified Sources

(U) Source 1
(U) DODIG-2022-076, "Evaluation of Combatant Commands' Communication Challenges with Foreign Partner Nations During Coronavirus Disease-2019 Pandemic and Mitigation Efforts," March 28, 2022
~~Source Classification: SECRET//NOFORN~~
~~Declassification Date: March 28, 2047~~

(U) Source 2
(U) DODIG-2024-002, "Management Advisory: The Protection of Sensitive Mission Data by the Security Assistance Group–Ukraine and Its Subordinate Commands," November 2, 2023
~~Source Classification: SECRET~~
~~Declassification Date: November 2, 2033~~

(U) Source 3
(U) DODIG-2024-109, "Management Advisory: U.S. Air Forces in Europe Handling of Sensitive Information at Logistics Enabling Node–Romania," July 11, 2024
~~Source Classification: SECRET~~
~~Declassification Date: July 11, 2049~~

(U) Source 4
(U) DODIG-2025-006, "Follow-up Evaluation on Management Advisory: The Protection of Sensitive Mission Data by the Security Assistance Group–Ukraine and Its Subordinate Commands," October 11, 2024
~~Source Classification: SECRET~~
~~Declassification Date: October 11, 2034~~

(U) Acronyms and Abbreviations

CIO	Chief Information Officer
CUI	Controlled Unclassified Information
DepSecDef	Deputy Secretary of Defense
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
OCA	Original Classification Authority
OPSEC	Operations Security
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
SecDef	Secretary of Defense
USD(I&S)	Under Secretary of Defense for Intelligence and Security

(U) Glossary

(U) Controlled Unclassified Information. A control marking for unclassified 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 government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls in accordance with DoDM 5200.01, Volume 4.

(U) DoD-Controlled. Used only for DoD purposes, dedicated to DoD processing, and effectively under DoD configuration control.

(U) Electronic Messaging Services. Online communications capabilities, including websites, email, texting, chat, and related online communications methods.

(U) Information Security. The system of policies, procedures, and requirements to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to executive order, statute, or regulation.

(U) Nonofficial Electronic Messaging Services. Online communications capabilities that are not intended to be used for official DoD information and are not owned, operated, or controlled by the DoD. Examples include so-called "free services" and "purchased services" that are used for private personal communications, such as for personal electronic messaging.

(U) Nonpublic DoD Information. DoD information that has not been approved for public release.

(U) Original Classification Authority. An individual authorized in writing, either by the President, Vice President, or agency heads or other officials designated by the President, to originally classify information.

(U) Security Classification Guide. A documentary form of classification guidance issued by an original classification authority that: (1) identifies the elements of information regarding a specific subject that must be classified and (2) establishes the level and duration of classification for each such element.

Whistleblower Protection

U.S. Department of Defense

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

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

Legislative Affairs Division
703.604.8324

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

www.dodig.mil

DoD Hotline
www.dodig.mil/hotline

~~SECRET//NOFORN~~

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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

~~SECRET//NOFORN~~