



INSPECTOR GENERAL

U.S. Department of Defense

December 2, 2025



(U) Evaluation of the Secretary of Defense's Reported Use of a Commercially Available Messaging Application for Official Business

Classified By: [REDACTED]
Assistant Inspector General for
Evaluations Programs, Combatant
Commands, and Operations
Derived From: Multiple Sources
Declassify On: 20501231

Controlled By: DoD OIG
Controlled By: Evaluations
CUI Category: OPSEC
Distribution/Dissemination Control:
FEDCON, PRVN
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 U.S. Central Command Regulation 380-14, "USCENTCOM Security Classification Guide." 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





(U) Results in Brief

(U) Evaluation of the Secretary of Defense's Reported Use of a Commercially Available Messaging Application for Official Business

(U) December 2, 2025

(U) Objective

(U) The objective of this evaluation was to determine the extent to which the Secretary of Defense (the Secretary) and other DoD personnel complied with DoD policies and procedures for the use of the Signal commercial messaging application (Signal) for official business. Additionally, we reviewed compliance with classification and record retention requirements.

(U) Background

(U) On March 15, 2025, beginning at approximately 1345 Eastern Daylight Time (EDT), U.S. forces conducted air and missile strikes on Houthi forces in Yemen. Approximately 2 hours before these strikes, information containing specific details of the strike package was included in a group chat on Signal that included 19 members, including the Secretary and a journalist. On March 24 and 26, 2025, the news magazine The Atlantic published two articles that revealed the details of the Signal group chat conversation.

(U) Finding

(U) At 2054 EDT on March 14, 2025, approximately 17 hours before the beginning of the March 15 strikes, the Commander of the U.S. Central Command (USCENTCOM) sent an email classified SECRET and not releasable to foreign nationals (SECRET//NOFORN) to the attention of the Secretary and the Acting Chairman of the Joint Chiefs of Staff. This email provided operational details and updates to senior DoD leadership, including detailed information on the means and timing of the strikes.

(U) We determined that, based on the content of the email, USCENTCOM personnel classified the email consistent with Executive Order 13526 and the USCENTCOM security classification guide. Although this email contained markings at the top and bottom identifying its classification as SECRET//NOFORN, it did not contain

(U) Finding (cont'd)

(U) portion markings on each paragraph, as required by DoD Manual 5200.01, Volume 2.

(U) Based on interviews with four current and former DoD officials, we determined that on Saturday, March 15, 2025, three individuals (the Secretary, his junior military assistant, and his personal communicator) were present in a sensitive compartmented information facility (SCIF) at the Secretary's residence at Fort McNair immediately preceding and during the execution of the strikes.

(U) We requested that the DoD provide a copy of the Secretary's communications on Signal on or about March 15, 2025. The DoD provided a partial copy of messages from the Secretary's personal cell phone, including some messages that The Atlantic previously reported, but other messages had auto-deleted because of chat settings. Therefore, we had to rely in part on the transcript of the chat The Atlantic posted publicly ("Houthi PC Small Group") for a full record.

(U) In a July 25, 2025 statement that the Secretary provided to the DoD Office of Inspector General, he confirmed that he sent a message containing operational information to members of the "Houthi PC Small Group" Signal chat at 1144 EDT on March 15, 2025. We compared The Atlantic Signal chat transcript to the email from the USCENTCOM Commander. Based on our review, we concluded that some information the Secretary sent from his personal cell phone on Signal on March 15, 2025, matched the operational information USCENTCOM sent and classified as SECRET//NOFORN.

(U) The Secretary declined to be interviewed for this evaluation. In his July 25, 2025 statement, he provided the following information.

- (U) He received the email briefing from the USCENTCOM Commander, classified as SECRET//NOFORN, on March 14.



(U) Results in Brief

(U) Evaluation of the Secretary of Defense's Reported Use of a Commercially Available Messaging Application for Official Business

(U) Finding (cont'd)

- (U) As an original classification authority, he has authority to decide whether information should be classified and whether classified materials no longer require protection.
- (U) In his 1144 EDT message, he took "non-specific general details" that he determined, as an original classification authority, were either not classified or that he could safely declassify and use to create an "unclassified summary" to provide to the Signal chat participants.

(U) We concluded that the Secretary sent sensitive, nonpublic, operational information that he determined did not require classification over the Signal chat on his personal cell phone. The Secretary is the head original classification authority in the DoD based on Executive Order 13526 and DoD Manual 5200.45 and holds the authority to determine the required classification level of all DoD information he communicates. However, because the Secretary indicated that he used the Signal application on his personal cell phone to send nonpublic DoD information, we concluded that the Secretary's actions did not comply with DoD Instruction 8170.01, which prohibits using a personal device for official business and using a nonapproved commercially available messaging application to send nonpublic DoD information.

(U) The Secretary sent nonpublic DoD information identifying the quantity and strike times of manned U.S. aircraft over hostile territory over an unapproved, unsecure network approximately 2 to 4 hours before the execution of those strikes. Using a personal cell phone to conduct official business and send nonpublic DoD information through Signal risks potential compromise of sensitive DoD information, which could cause harm to DoD personnel and mission objectives.

(U) Recommendation

(U) We recommend that the Chief of the USCENTCOM Special Security Office review the command's classification

(U) procedures for compliance with DoD Manual 5200.01, Volume 2, and issue additional procedures, as necessary, to ensure proper portion marking of classified information.

(U) We are not making any additional recommendations in this report. Our report, "Evaluation of DoD Policy and Oversight Reports Related to Using Non-DoD-Controlled Electronic Messaging Systems to Conduct Official Business," (DODIG-2026-022) recommended that the DoD improve training for senior DoD officials on the proper use of electronic devices. Once implemented and adhered to, the corrective actions would comply with information security and recordkeeping requirements.

(U) Management Comments and Our Response

(U) Although not required to comment, the DoD's Deputy General Counsel for Legislation, Investigations, and Oversight provided additional context for the DoD OIG to consider. However, the Deputy General Counsel did not provide any documentation to support this additional context. As a result, we could not independently verify the Deputy General Counsel's information. Therefore, in accordance with our evaluation standards and without evidence to support this information, we did not include the recommended language in the body of the report. We included the comments from the Deputy General Counsel in the report's Management Comments section.

(U) The Chief of the USCENTCOM Special Security Office agreed with our recommendation and described how USCENTCOM met its intent. Specifically, the Chief conducted an in-depth review and provided evidence that the command has a comprehensive training program that provides clear guidance on portion marking classified documents. This evidence met the intent of the recommendation; therefore, the recommendation is closed.

(U) Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief, U.S. Central Command Special Security Office	None	None	1 (U)

The following categories are used to describe agency management's comments to individual recommendations.

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



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

December 2, 2025

MEMORANDUM FOR SECRETARY OF DEFENSE
GENERAL COUNSEL, DEPARTMENT OF DEFENSE
CHIEF, U.S. CENTRAL COMMAND SPECIAL SECURITY OFFICE

SUBJECT: (U) Evaluation of the Secretary of Defense's Reported Use of a Commercially Available Messaging Application for Official Business
(Report No. DODIG-2026-021)

(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 report's recommendation. We considered management's comments on the draft report when preparing the final report. These comments are included in the report. The Chief of the U. S. Central Command's Special Security Office took action sufficient to address the recommendation in this report, and we consider the recommendation closed.

(U) This report addresses a March 26, 2025 request from the Chairman and Ranking Member of the Senate Committee on Armed Services to review the Secretary's publicly reported use of Signal for official business, including potential use of unclassified networks to discuss sensitive and classified information. Additionally, we issued a separate report that reviewed our previous oversight work related to DoD personnel using non-approved commercial messaging applications, titled, "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). Together, these two reports address the Chairman's and Ranking Member's request.

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

A handwritten signature in blue ink, appearing to read "Steven A. Stebbins", is located below the text.

Steven A. Stebbins
Acting

(U) Contents

(U) Introduction.....	1
(U) Objective.....	1
(U) Background.....	2
(U) Finding.....	11
(U) The Secretary of Defense Sent Operational Information That He Determined Did Not Require Classification over Signal on His Personal Phone	11
(U) USCENTCOM Provided Classified Strike Details to the Secretary in Advance of and Throughout the March 15 Strikes.....	14
(U) The Secretary Oversaw the March 15, 2025 Strikes from a SCIF at His Fort McNair Residence Alongside Two Aides.....	19
(U) The Secretary Sent Sensitive, Nonpublic Information over Signal, an Application Not Approved for Transmission of Nonpublic DoD Information.....	20
(U) The Secretary and OSD Did Not Retain the Secretary’s Conversations on Signal as Official Records as Required by Federal Law and DoD Policy.....	24
(U) The Secretary’s Communication of Nonpublic DoD Information Created Additional Risks to U.S. Forces and Missions.....	25
(U) Management Comments on the Finding and Our Response.....	26
(U) Recommendation, Management Comments, and Our Response	27
(U) Appendix A	28
(U) Scope and Methodology.....	28
(U) Use of Computer-Processed Data.....	30
(U) Use of Technical Assistance.....	30
(U) Appendix B	31
(U) Prior Coverage	31
(U) Appendix C	39
(U) Additional Information Related to the Secretary’s Use of Signal to Conduct Official Business.....	39
(U) Appendix D	42
(U) Transcript of the Signal Group Chat Published by The Atlantic on March 24 and March 26, 2025.....	42

(U) Partial Transcript of the Signal Group Chat Retained by the DoD on March 27, 2025, from the Secretary of Defense's Personal Cell Phone.....	48
(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 2054 EDT on March 14, 2025.....	52
(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 1255 EDT on March 15, 2025.....	55
(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 1346 EDT on March 15, 2025.....	58
(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 2111 EDT on March 15, 2025.....	61
(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS Included in the Secretary's March 15, 2025 Information Packet	64
(U) Secretary of Defense Statement to the DoD OIG, Received on July 25, 2025.....	66
(U) Appendix E.....	67
(U) Senate Committee on Armed Services Chairman and Ranking Member Letter to the Acting Inspector General on March 26, 2025	67
(U) Management Comments	68
(U) Document Provided by DoD Deputy General Counsel on September 24, 2025, Suggesting Additional Context for the Report Finding	68
(U) Chief, U.S. Central Command Special Security Office	69
(U) List of Classified Sources.....	71
(U) Acronyms and Abbreviations.....	74

(U) Introduction

(U) Objective

(U) The objective of this evaluation was to determine the extent to which the Secretary of Defense (the Secretary) and other DoD personnel complied with DoD policies and procedures for the use of the Signal commercial messaging application (Signal) for official business. Additionally, we reviewed compliance with classification and records retention requirements.

(U) In a March 26, 2025 letter, the Chairman and Ranking Member of the Senate Committee on Armed Services requested that the DoD Office of Inspector General (DoD OIG) 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. 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 the Chairman and Ranking Member's request and answers requests 1, 2, 3, 5, and 6. The DoD OIG released a separate report that also reviewed requests 2, 3, and 6, titled "Evaluation of DoD Policy and Oversight Reports Related to Using Non-DoD-Controlled Electronic Messaging Systems to Conduct Official Business,"

(U) (Report No. DODIG-2026-022) on December 2, 2025. We did not address question 4 of the Chairman and Ranking Member's request because the DoD OIG does not have jurisdiction over non-DoD entities such as the White House, Intelligence Community, or other U.S. Government (USG) departments. The letter from the Chairman and Ranking Member of the Senate Committee on Armed Services is located in Appendix E.

(U) Background

(U) On March 15, 2025, at approximately 1345 Eastern Daylight Time (EDT), U.S. forces conducted air and missile strikes on Houthi forces in Yemen. Approximately 2 hours before these strikes began, information containing specific details of the strike package was included in a group chat on Signal that included 19 members, including the Secretary and a journalist.

(U) Public Disclosure of the Signal Chat Among Senior Government Officials, Including the Secretary of Defense

(U) On March 24, 2025, the news magazine The Atlantic published an article stating that the President's National Security Advisor invited the magazine's editor-in-chief to a group chat on Signal.¹ The article stated that in this chat, the National Security Advisor and others, including the Vice President, Secretary of State, Secretary of Defense, Director of the Central Intelligence Agency, and Director of National Intelligence, discussed policy, planning, and details of strikes against Houthi forces in Yemen that took place on March 15, 2025. The March 24, 2025 article alleged that the chat contained sensitive operational details that The Atlantic chose not to print because those details potentially contained classified information.

(U) On March 24 and 25, 2025, several officials who were included in the Signal chat group, including the National Security Advisor, Secretary of Defense, Director of the Central Intelligence Agency, and Director of National Intelligence, made public statements indicating that no information in the chat group was classified. Following those statements, The Atlantic published a subsequent article on March 26, 2025, that contained the details The Atlantic previously excluded regarding the composition and timing of the strikes against Houthi targets.² The transcript of the group chat, as downloaded from The Atlantic's website, is included in Appendix D.³ A partial copy of the transcript, as obtained from the Office of the Secretary of Defense (OSD), is also included in Appendix D. The Secretary's July 25, 2025 statement to the DoD OIG on his participation in the Signal chat is also included in Appendix D.

¹ (U) The Atlantic, "The Trump Administration Accidentally Texted Me Its War Plans," March 24, 2025.

² (U) The Atlantic, "Here Are the Attack Plans That Trump's Advisors Shared on Signal," March 26, 2025.

³ (U) The DoD OIG requested and The Atlantic consented to our use of portions of its copyrighted material in this report. All excerpts in Appendix D remain copyrighted by The Atlantic.

(U) The Secretary of Defense and OSD Receive Communications Support from the Office of the Chief Information Officer

(U) The DoD Office of the Chief Information Officer (OCIO) provides assistance to the Secretary, OSD, and all of the DoD by overseeing and implementing DoD policies and procedures on the use of commercially available messaging applications, such as Signal, and protecting the security of digital information. According to DoD Directive (DoDD) 5144.02, "DoD Chief Information Officer," the Chief Information Officer is the principal staff assistant for information technology and responsible for all DoD information enterprise matters, including communications, network policy and standards, information systems, and cybersecurity.⁴ The Chief Information Officer also develops DoD strategy and policy on the operation and protection of all DoD information technology, including enforcement, operation, and maintenance of systems, such as identifying solutions for messaging applications in accordance with DoD policies.

(U) The OCIO also provides communications support directly to the Secretary and OSD. Specifically, the Secretary of Defense Communications Team (SD Comms) is contained in the OCIO and responsible for providing 24/7 command and control communications support to the Secretary and Deputy Secretary of Defense (Deputy Secretary) while located in the Pentagon, personal residences, command posts, relocation sites, and executive communications vehicles. SD Comms provides both the Secretary and Deputy Secretary with individuals known as personal communicators (PCs) who accompany the Secretaries wherever they travel. The PCs provide the Secretary and Deputy Secretary with immediate access to senior government officials through multiple forms of unclassified and classified voice- and text-based digital communications anywhere in the world. A PC from SD Comms is on duty at all times with both the Secretary and Deputy Secretary.

(U) DoD Policy on the Use of Commercially Available Messaging Applications and Classification, Declassification, and Protection of Information

(U) DoD policy provides specific guidance for the use of commercially available messaging applications, such as Signal, to conduct official USG business, as well as classifying, declassifying, and protecting controlled and classified information. Specifically, DoD policy: (1) prohibits the use of nonapproved commercially available messaging applications, such as Signal, for USG business, with limited exceptions; (2) requires DoD personnel to protect

(U) DoD policy prohibits the use of nonapproved commercially available messaging applications, such as Signal, for official business, with limited exceptions.

⁴ (U) DoDD 5144.02, "DoD Chief Information Officer," November 21, 2014 (Incorporating Change 1, September 19, 2017).

(U) nonpublic or classified DoD information; (3) establishes procedures for declassifying information; and (4) requires DoD personnel to comply with Federal law by retaining official records. The purpose of these policies is to protect DoD information from unauthorized access and ensure retention of records that have continued value to the public and are required by law to be retained.

(U) DoD Policy on the Use of Commercially Available Messaging Applications, Such as Signal

(U) DoD Instruction (DoDI) 8170.01, “Online Information Management and Electronic Messaging,” prohibits the use of nonapproved and non-DoD-controlled commercially available messaging applications for official USG business, with limited exceptions.⁵ Specifically, DoDI 8170.01 states, “Do not use non-DoD-controlled electronic messaging services to process nonpublic DoD information, regardless of the service’s perceived appearance of security.” The instruction and subsequent guidance give examples of nonapproved applications, such as private accounts or groups or encrypted messages on popular commercially available messaging applications, such as Signal, WhatsApp, and Facebook Messenger.

(U) DoDI 8170.01 also states that DoD personnel and contractors may only send classified information by electronic messaging on classified networks or those encrypted with National Security Agency-approved cryptography. DoDI 8170.01 requires compliance with DoD records retention, cybersecurity, and information security policies. The 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.⁶

(U) Additionally, DoDI 8170.01 prohibits personnel from using personal, nonofficial accounts for personal convenience or preference. DoD policy says that “DoD personnel 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.

⁵ (U) DoDI 8170.01, “Online Information Management and Electronic Messaging,” January 2, 2019 (Incorporating Change, March 12, 2025). For the purposes of this report, we refer to non-DoD-controlled electronic messaging services as nonapproved commercially available messaging applications, which include Signal.

⁶ (U) The definition of a record is included in the section below titled “DoD Policy on Records Retention.”

- (U) The use is in the interest of DoD or other USG missions.

(U) DoDI 8170.01 further states that OSD and DoD Component heads may approve, as appropriate, official use of nonapproved commercially available messaging applications, but the instruction does not provide a mechanism or specific parameters for exercising the exception. In October 2023, the DoD Chief Information Officer issued a memorandum that created a process for DoD Components to request an exception to policy that requires final exception approval from the DoD Chief Information Security Officer.⁷ However, the newest version of DoDI 8170.01, published in March 2025, did not incorporate this exception request or clarify that a Component head cannot provide final approval for the policy exception.

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

(U) According to DoDD 5205.02E, “DoD Operations Security (OPSEC) Program,” 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.⁸ This includes protecting classified information, such as SECRET, TOP SECRET, and controlled unclassified information (CUI), during physical and electronic storage and transmission.⁹

(U) DoDI 8582.01, “Security of Non-DoD Information Systems Processing Unclassified Non-Public DoD Information,” defines DoD information as any information that: (1) “is in or related to DoD custody and control;” (2) “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 (3) “is developed by a non-DoD entity in support of an official DoD activity.”¹⁰ DoD information can be either public or nonpublic. Public DoD information is DoD information that has been cleared for public release in accordance with DoDI 5230.09, “Clearance of DoD Information for Public Release.”¹¹ Nonpublic DoD information is any DoD information that has not been cleared for public release and must be protected, according to DoDI 5230.09. Nonpublic

⁷ (U) DoD Chief Information Officer Memorandum, “Use of Unclassified Mobile Applications in Department of Defense,” October 6, 2023.

⁸ (U) DoDD 5205.02E, “DoD Operations Security (OPSEC) Program,” June 20, 2012 (Incorporating Change 2, August 20, 2020).

⁹ (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.”

¹⁰ (U) DoDI 8582.01, “Security of Non-DoD Information Systems Processing Unclassified Non-Public DoD Information,” December 9, 2019.

¹¹ (U) DoDI 5230.09, “Clearance of DoD Information for Public Release,” January 25, 2019.

(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 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	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	(U) Information that, if disclosed, could reasonably be expected to cause exceptionally grave damage to national security

(U) Controlled Unclassified Information

¹² (U) DoDI 5200.48, "Controlled Unclassified Information," March 6, 2020.

(U) Classified Information

(U) Executive Order (EO) 13526, “Classified National Security Information,” defines requirements for government officials to classify information.¹³ EO 13526 identifies officials who have original classification authority (OCA), including the President, Vice President, agency heads (such as the Secretary of Defense), officials designated by the President, and other USG officials to whom the President or another OCA has delegated their OCA authority. EO 13526 also identifies the three levels of classification outlined in Figure 1, their definitions, and the types of information eligible for classification. According to EO 13526, information eligible for classification falls into one of the following eight categories.

- (U) Military plans, weapons systems, or operations
- (U) Foreign government information
- (U) Intelligence activities (including covert action), intelligence sources or methods, or cryptology
- (U) Foreign relations or foreign activities of the United States, including confidential sources
- (U) Scientific, technological, or economic matters related to national security
- (U) USG programs for safeguarding nuclear materials or facilities
- (U) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services related to national security
- (U) The development, production, or use of weapons of mass destruction

(U) According to DoD Manual (DoDM) 5200.01, Volume 1, “DoD Information Security Program: Overview, Classification, and Declassification,” 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.¹⁴

(U) In accordance with EO 13526, as agency heads, the Secretary of Defense and the Secretaries of the Military Departments possess OCA over information and programs

¹³ (U) EO 13526, “Classified National Security Information,” December 29, 2009.

¹⁴ (U) DoDM 5200.01, Volume 1, “DoD Information Security Program: Overview, Classification, and Declassification,” February 24, 2012 (Incorporating Change 3, January 17, 2025).

(U) within their control in the DoD. Under DoDM 5200.45, other senior DoD positions assigned a unique mission may be delegated OCA by the Secretary of Defense or Secretaries of the Military Departments. At the time an OCA classifies information, the OCA establishes a specific date or event for declassification based on the duration of the national security sensitivity of the information. An OCA can also determine when a combination of unclassified information should be classified.

(U) The Secretary of Defense and the Secretaries of the Military Departments possess original classification authority over information and programs within their control in the DoD.

(U) According to DoDM 5200.01, Volume 1, and DoDM 5200.45, “Original Classification Authority and Writing a Security Classification Guide,” OCAs must issue security classification guidance for each system, plan, program, project, or mission involving classified information.¹⁵ 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 (USCENTCOM) security classification guide (SCG) establishes the basic policies for properly marking, classifying, downgrading, and declassifying information related to USCENTCOM or units operating in its area of responsibility.¹⁶ 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.

(U) EO 13526 and DoDM 5200.01, Volume 2, “DoD Information Security Program: Marking of Information,” state that OCAs must mark classified documents they create at the top and bottom of each page of the document to indicate the highest level of classification (Confidential, SECRET, or TOP SECRET) contained in the document.¹⁷ These markings are known as banner markings. The EO and DoDM additionally state that individual portions of a classified document must contain markings to indicate which portions of the document are classified and at what level. These markings are known as portion markings. EO 13526 states that classified information is considered as classified at its banner-marked level of classification in the absence of other required markings.

(U) Declassification

(U) EO 13526 and DoDM 5200.01, Volume 1, also identify the requirements for declassification of classified information and state that information will be declassified as soon as it no longer meets the standards for classification. Both

¹⁵ (U) DoDM 5200.45, “Original Classification Authority and Writing a Security Classification Guide,” January 17, 2025.

¹⁶ (U) USCENTCOM SCG, Central Command Regulation 380-14, November 16, 2022.

¹⁷ (U) DoDM 5200.01, Volume 2, “DoD Information Security Program: Marking of Information,” February 24, 2012 (Incorporating Change 4, July 28, 2020).

(U) EO 13526 and DoDM 5200.01, Volume 1, outline the four separate and parallel processes for declassifying information, specifically processes:

- (U) requiring the OCA to decide, at the time they classify the information, when it may be declassified;
- (U) of automatic declassification, no later than December 31 of the year 25 years from the date of classification, unless action is taken to keep it classified;
- (U) for mandatory declassification review, triggered by a request for possible declassification; and
- (U) of systematic review for information in a DoD Component's custody for possible declassification.

(U) EO 13526 and DoDM 5200.01 do not identify methods for OCAs to declassify information outside of these four processes. According to EO 13526 and DoDM 5200.01, three different types of officials may declassify information: the responsible OCA, the OCA's supervisory official if they also have OCA, or officials with delegated declassification authority. The authority to declassify information extends only to information for which the specific official has classification, program, or functional responsibility.

(U) EO 13526 states that before public release, all declassified records will be appropriately marked to reflect declassification. DoDM 5200.01 also 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." DoDM 5200.01 also states that guidance may be in the form of declassification guides, sections of SCGs, or memorandums.

(U) DoD Policy on Records Retention

(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

(U) 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.¹⁸

(U) DoDI 5015.02 also states that “DoD records will be managed as national assets” in compliance with the requirements of Title 44 United States Code.¹⁹ Both DoD policy and Federal law provide specific requirements for maintaining records and include instructions for using nonofficial electronic messaging accounts. If personnel use a nonofficial electronic messaging account, both 44 U.S.C. § 2911 and DoDI 5015.02 require the official to forward a copy of the record to their official account at the time of transmission or within 20 days of its original creation.

¹⁸ (U) DoDI 5015.02, “DoD Records Management Program,” February 24, 2015 (Incorporating Change 1, August 17, 2017).

¹⁹ (U) Title 44, United States Code, Chapter 29, “Records Management by the Archivist of the United States and by the Administrator of General Services,” Chapter 31, “Records Management by Federal Agencies,” Chapter 33, “Disposal of Records,” and Chapter 35, “Coordination of Federal Information Policy.”

(U) Finding

(U) The Secretary of Defense Sent Operational Information That He Determined Did Not Require Classification over Signal on His Personal Phone

(S//NF) On March 15, 2025, at approximately 1345 EDT, U.S. forces began air and missile strikes on Houthi forces in Yemen [REDACTED]

(S//NF) Before and during the operation, the USCENTCOM Commander sent four emails on March 14 and 15, classified as SECRET and not releasable to foreign nationals (SECRET//NOFORN), to the attention of the Secretary and the Acting Chairman of the Joint Chiefs of Staff (A-CJCS) to provide operational details and updates to senior DoD leadership. Specifically, the USCENTCOM Commander sent the first of these emails at 2054 EDT on March 14, approximately 17 hours before the planned strike time. The USCENTCOM Commander sent three additional emails on March 15—approximately 1 hour before the strikes, at the time the strikes occurred, and at the end of the day.

[REDACTED] The four emails contained banner markings indicating their overall level of classification but not portion markings, as required by DoDM 5200.01, Volume 2.

(U) We determined that USCENTCOM officials classified the information in the Commander's emails consistent with existing guidance in EO 13526 and the USCENTCOM SCG. Specifically, EO 13526 identifies the types of information eligible for classification, and the USCENTCOM SCG provides specific guidance that the operational movement of aircraft should be classified SECRET. On April 14, USCENTCOM personnel confirmed to us that the content of the Commander's emails was classified SECRET//NOFORN. In accordance with EO 13526, we concluded that without portion markings, all information in the USCENTCOM emails was classified as SECRET//NOFORN.

(U) Based on information from four current and former DoD officials, we determined that on Saturday, March 15, three individuals (the Secretary, his junior military assistant [JMA], and his PC) were present at the Secretary's residence at Fort McNair in the lead-up to and execution of the strikes. The four officials we interviewed stated that the Secretary, JMA, and PC were located in a temporary sensitive compartmented

(U) information facility (SCIF) at the Secretary's residence. According to two officials, the Secretary held several classified conversations in the SCIF with USCENTCOM personnel that day.

(U) We requested a copy of the Secretary's communications on Signal on or about March 15. According to a senior official in the OSD, the Secretary declined to provide us direct access to his personal cell phone. The DoD did provide a partial copy of Signal messages from the Secretary's personal cell phone that included some messages The Atlantic had previously reported. However, the partial copy did not include all messages, including the strike messages that had auto-deleted because of settings in Signal chosen by one of the group chat participants. Therefore, we reviewed a transcript of the chat The Atlantic posted publicly ("Houthi PC Small Group") for a full record of the chat.

(U) We compared The Atlantic Signal chat transcript to the emails from the USCENTCOM Commander and found that some of the information the Secretary sent was in USCENTCOM's classified emails. Specifically, in a July 25 written statement to the DoD OIG, the Secretary wrote that he posted information in the chat at 1144 EDT on March 15, approximately 2 to 4 hours before the strikes. This message substantially restated details from the USCENTCOM Commander's first classified email from 2054 EDT on March 14, marked as SECRET//NOFORN. The Secretary's message included the following information on the means and timing of strikes, aircraft type, and weapon systems employed.

- (U) "1215et: F-18s LAUNCH (1st strike package)"
- (U) "1345: 'Trigger Based' F-18 1st Strike Window Starts (Target Terrorist is @ his Known Location so SHOULD BE ON TIME) – also, Strike Drones Launch (MQ-9s)"
- (U) "1410: More F-18s LAUNCH (2nd strike package)"
- (U) "1415: Strike Drones on Target (THIS IS WHEN THE FIRST BOMBS WILL DEFINITELY DROP, pending earlier "Trigger Based" targets)"
- (U) "1536: F-18 2nd Strike Starts – also, first sea-based Tomahawks launched."
- (U) The phrase "We are currently clean on OPSEC."

(U) In comparison, the USCENTCOM Commander's SECRET//NOFORN email from March 14 provided the following details.

- (S//NF) [REDACTED]

- (S//NF) [REDACTED]
[REDACTED]
- (S//NF) [REDACTED]
- (S//NF) [REDACTED]
- (S//NF) [REDACTED]
- (S//NF) [REDACTED]
- (S//NF) [REDACTED]
- (S//NF) [REDACTED]

(U) The Secretary declined to be interviewed for this evaluation. However, in his July 25 written statement, the Secretary said that he determined that the information he shared on Signal from the USCENTCOM Commander's email did not require classification. Specifically, the Secretary stated the following.

- (U) He received the email briefing from the USCENTCOM Commander, classified as SECRET//NOFORN, on March 14.
- (U) As an OCA, he retains authority under EO 13526 to decide whether information should be classified and whether classified materials no longer require protection.
- (U) At 1144 EDT on March 15, "I took non-specific general details which I determined, in my sole discretion, were either not classified, or that I could safely declassify" and created an "unclassified summary" of the USCENTCOM strike details to provide to participants of the Signal chat.

(U) The Secretary's full statement to the DoD OIG is included in Appendix D.

(U) We concluded that the Secretary does have the authority to determine the required level of classification for all DoD information under EO 13526 and DoDM 5200.45. However, based on the Secretary's written statement indicating that he sent sensitive, nonpublic, operational information over Signal from his personal cell phone 2 to 4 hours before the strikes occurred, we concluded that the Secretary's actions did not comply with DoDI 8170.01, which prohibits using a personal device for official business and using a nonapproved commercially available messaging application to send nonpublic DoD information.

(S//NF) The Secretary's transmission of nonpublic operational information over Signal to an uncleared journalist and others 2 to 4 hours before planned strikes using his personal cell phone exposed sensitive DoD information. Using a personal cell phone to conduct official business and send nonpublic DoD information through Signal risks potential compromise of sensitive DoD information, which could cause harm to DoD personnel and mission objectives. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) USCENTCOM Provided Classified Strike Details to the Secretary in Advance of and Throughout the March 15 Strikes

(S//NF) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) The USCENTCOM Commander Sent Four Classified Emails to the Attention of the Secretary and the Acting Chairman of the Joint Chiefs of Staff on March 14 and 15

(U) In the lead-up to the March 15 strikes against Houthi forces, the USCENTCOM Commander provided the Secretary and A-CJCS with information on the planned operational details and timeline through a series of four emails classified as SECRET//NOFORN. The USCENTCOM Commander sent each of these emails over the DoD's SECRET Internet Protocol Router Network (SIPRNET) to the Secretary's JMA, the A-CJCS, and multiple other senior DoD officials.

(U) The USCENTCOM Commander sent the first email at 2054 EDT on March 14, approximately 17 hours before the planned strike time. This email provided the Secretary and A-CJCS with specific details of the planned strikes, including information on the targets, weapons packages prepared for deployment, and planned aircraft use. The email was banner marked SECRET//NOFORN but did not contain portion markings identifying the level

(U) The email was banner marked SECRET//NOFORN but did not contain portion markings identifying the level of classification of specific items in the email.

(U) of classification of specific items in the email, as required by EO 13526 and DoDM 5200.01, Volume 2.²⁰ This email is included in Appendix D. Therefore, we recommend that the Chief of the USCENTCOM Special Security Office review classification procedures and ensure that clear requirements are communicated to USCENTCOM personnel for portion marking classified information in accordance with EO 13526 and DoDM 5200.01, Volume 2. If the review finds that the procedures are insufficient, the Chief should update, issue, and provide instruction on additional procedures. If the review finds that the procedures are sufficient, the Chief should develop and implement additional training for USCENTCOM personnel to instruct them in proper techniques for marking classified information.

(U) The USCENTCOM Commander also sent three additional SECRET//NOFORN emails to the attention of the Secretary and A-CJCS later on March 15, approximately 1 hour before the strikes (1255 EDT), at the time the strikes occurred (1346 EDT), and at the end of the day (2111 EDT). USCENTCOM officials stated that the process of providing senior DoD leadership with real-time updates was not uncommon for high-profile missions. These three additional emails from the USCENTCOM Commander are also included in Appendix D.

(U) Each Classified USCENTCOM Email Provided Updated and Adjusted Strike Timing Details Based on Operational Conditions

(S//NF) The USCENTCOM Commander sent emails before, during, and following the March 15 strikes, providing updates and adjustments to the strike times and operational details based on operational conditions. Specifically, [REDACTED]

[REDACTED]
[REDACTED]

[REDACTED] As a result, each of these additional emails contained slightly different information.

(S//NF) The initial email the USCENTCOM Commander sent on the evening of March 14 included approximate launch times and time on target for F/A-18As, MQ-9 UAVs, F-15Es, and Tomahawk Land Attack Missiles. The three subsequent emails updated these launch times and time on target to reflect changes in the operational environment that required slight adjustments in the overall schedule. For example, the USCENTCOM Commander's initial estimate for the time on target of the first F/A-18A strike was 1345 EDT on March 15. [REDACTED]

[REDACTED]

²⁰ (U) DoDM 5200.01, Volume 2, states that the overall classification level of a document is determined by the banner markings and that, absent portion markings, all information in the document is treated as classified at that overall classification level.

(S//NF) [REDACTED]
[REDACTED]
[REDACTED]

(U) Table 1 contains a chronology of the planning and execution of the strikes, as well as public media reporting on the use of Signal to communicate information related to the strikes. Throughout this table, we use EDT for consistency among events taking place in multiple time zones.

(U) Table 1. Chronology of Events and Communications Related to the March 15, 2025 Strikes on Houthi Targets in Yemen (in EDT)

(S//NF) Date and Time	Event
[REDACTED]	[REDACTED] [REDACTED]
[REDACTED]	[REDACTED] [REDACTED] on planned strikes in Yemen to take place on March 15.
[REDACTED]	[REDACTED] [REDACTED] on planned strikes in Yemen to take place on March 15.
March 14, 2054 EDT	The USCENTCOM Commander sent an email to the Secretary's office providing an executive brief for the upcoming strikes to take place at 1345 EDT the following day. This email contained specific times and strike packages, as well as the phrase "We are currently clean on OPSEC," all of which appeared substantially restated or verbatim in the March 15 Signal chat.
March 15, 1135 EDT	The Secretary had a call with the USCENTCOM Commander, [REDACTED] [REDACTED]
March 15, 1144 EDT	The Secretary sent a message to the Signal group chat on his personal cell phone stating, "TIME NOW (1144et): Weather is FAVORABLE. Just CONFIRMED w/ CENTCOM we are a GO for mission launch." This message also contained specific details regarding the strike package, such as "1215et: F-18s LAUNCH (1st strike package)," which appeared in the email from the USCENTCOM Commander sent approximately 15 hours earlier.
March 15, 1255 EDT	The USCENTCOM Commander provided an email update to the Secretary's office approximately 1 hour before strikes were to occur, noting that [REDACTED] [REDACTED] (S//NF)

<p>(S//NF)</p> <p>Date and Time</p>	<p>Event</p>
<p>March 15, 1255 EDT</p>	<p>[REDACTED] The times for strikes listed in this email no longer corresponded to the times indicated in the group chat, indicating that the email sent at 2054 EDT on March 14 was the source of the Signal chat information.</p>
<p>March 15, 1346 EDT</p>	<p>The USCENTCOM Commander provided another email update to the Secretary's office indicating that [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]</p>
<p>March 15, 1348 EDT</p>	<p>The National Security Advisor stated in the Signal group chat, "VP [referring to the Vice President]. building collapsed. Had multiple positive ID. Pete [Hegseth], [General] Kurilla, the [Intelligence Community], amazing job."</p>
<p>March 15, 1720 EDT</p>	<p>The Secretary sent a message to the Signal group chat on his personal cell phone stating, "CENTCOM was/is on point. Great job all. More strikes ongoing for hours tonight, and will provide full initial report tomorrow. But on time, on target, and good readouts so far."</p>
<p>March 15, 2111 EDT</p>	<p>The USCENTCOM Commander sent an email with a summary of the day's strikes.</p>
<p>March 24</p>	<p>The Atlantic published its initial story, along with copies of the group chat messages on which one of its reporters had been mistakenly included.</p>
<p>March 25</p>	<p>The Secretary made a statement to the media, stating, "Nobody was texting war plans, and that's all I have to say about that." Separately, the Director of National Intelligence and the Director of the Central Intelligence Agency stated to Congress that the group chat contained no classified information.</p>
<p>March 26</p>	<p>The Atlantic published a second story that contained additional excerpts from the group chat showing that the Secretary texted details on his personal cell phone about the timing and methods of the March 15 strikes before they occurred.</p> <p style="text-align: right;">(S//NF)</p>

(U) Source: DoD OIG analysis of USCENTCOM-provided information and public reporting.

(U) USCENTCOM Classified the Operational Information Provided to the Secretary as SECRET, Consistent with Existing Guidance

(U) We reviewed EO 13526 and the USCENTCOM SCG, which provide guidance to government and DoD officials on the types of information requiring classification and which level of classification to apply. EO 13526 outlines eight specific types of information that require classification, including “military plans, weapons systems, or operations,” and “vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.” Although these categories are broad, they provide guidance to DoD security officials who develop individual command SCGs.

(U) The USCENTCOM SCG provides more specific guidance on the classification level of operational information. The SCG states that, among others, the following categories of operational information should carry SECRET classification.

- (U) Concepts of operations
- (U) Current operations briefings
- (U) Operations emails
- (U) Operational movement of personnel, ammunition, aircraft, or equipment
- (U) Operational capabilities or shortfalls

(U) We determined that the information the USCENTCOM Commander sent to the Secretary on March 14 contained elements of all of these categories and that the email was therefore classified SECRET, consistent with the requirements of the USCENTCOM SCG.

(U) We determined that the email the USCENTCOM Commander sent to the Secretary on March 14 was classified SECRET in accordance with the USCENTCOM SCG.

Additionally, on April 14 and 15, a USCENTCOM official confirmed the classification level of the operational information in the USCENTCOM Commander’s emails from March 14 and 15 as SECRET//NOFORN and stated that, to their knowledge, no request had been made to declassify the information, which remained classified. The USCENTCOM official also indicated that the command made the determination to classify the information consistent with the USCENTCOM SCG and stated that the command regularly classifies sensitive, operations-related information as SECRET to prevent any risk to the mission or U.S. forces. USCENTCOM officials stated that following an operation, the command sometimes declassifies specific operational

(U) details, such as photographs or mission-related information, but that this is not typically done before an operation is complete.

(U) The Secretary Oversaw the March 15, 2025 Strikes from a SCIF at His Fort McNair Residence Alongside Two Aides

(U) According to details provided by four DoD officials who were either present with the Secretary or told us they were aware of his movements on March 15, we determined that the Secretary spent the day in a temporary SCIF at his Fort McNair residence. We also determined that the Secretary's JMA and PC were also located at the residence that day and assisted the Secretary by setting up communications and providing the Secretary with up-to-date information on the operation. No other DoD officials were present in the Secretary's residence during the lead-up to and execution of the strikes, according to interviews with the JMA and PC.

(U) The Secretary Held Classified Discussions with Officials and Reviewed Information in a Temporary SCIF

(U) Based on information from four officials we spoke with, we determined that during the morning and early afternoon of March 15, the Secretary monitored the operation against the Houthis from a temporary SCIF at his residence.²¹ Specifically, two aides present with the Secretary stated that the Secretary communicated over secure, classified communications systems with USCENTCOM personnel in the SCIF during the planning and execution of the strikes against Houthi targets that day and reviewed information related to the strikes. In the SCIF, the Secretary had access to multiple means of secure communication that allowed him to provide the necessary operational details and updates to non-DoD government officials on the Signal group chat.

(S//NF) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Among the information provided to the Secretary for his review in the SCIF on the morning of March 15 was the USCENTCOM Commander's email sent on the evening of March 14. This email provided detailed information regarding the upcoming strikes. The contents of that email were included in the Secretary's March 15 daily information packet, known as a "drop." Each page of the email in the drop contained a banner

²¹ (U) An official stated that the temporary SCIF existed because the DoD had yet to install more permanent facilities in the Secretary's residence.

(U) marking at the top and bottom of the page identifying the information as SECRET//NOFORN. The version of the USCENTCOM Commander's email from March 14 provided to the Secretary in the drop is included in Appendix D.

(U) We Were Unable to Obtain Access to the Secretary's Personal Cell Phone or a Full Transcript of the Signal Chat from the DoD

(U) As part of our evaluation, we requested access to the Secretary's personal cell phone to determine the source and validity of the information The Atlantic reported. We also requested copies of all messages the Secretary sent on Signal on or around March 15. A senior official in the OSD stated that they would not provide the Secretary's personal cell phone. The OSD did provide a portion of the Signal group chat that matches the same portion of the chat transcript reported in The Atlantic, and OSD officials stated that the information came from the Secretary's personal cell phone. The OSD-provided chat document excludes a number of messages that had auto-deleted by the time the information was captured from the Secretary's phone because of settings in the chat. This partial chat copy is included in Appendix D.

(U) We identified that the DoD declared that, as part of an ongoing court case, it preserved a record of the Signal chat in a Federal Records Act-compliant system.²² Specifically, in an April 14, 2025 filing, an official from the DoD Office of General Counsel stated that screenshots were taken of the existing messages and preserved in a recordkeeping system in the OSD. Furthermore, a May 7, 2025 filing stated that the DoD received an email from the White House Counsel's Office that contained a consolidated version of the group chat based in part on publicly available information and information saved from participants' phones. We requested that the DoD provide us with a copy of the record of the Signal group chat identified in the May 7, 2025 filing. However, the DoD declined our request for a copy of the complete transcript because it was not a DoD-created record. As a result, we relied on The Atlantic's version of the Signal group chat.

(U) The Secretary Sent Sensitive, Nonpublic Information over Signal, an Application Not Approved for Transmission of Nonpublic DoD Information

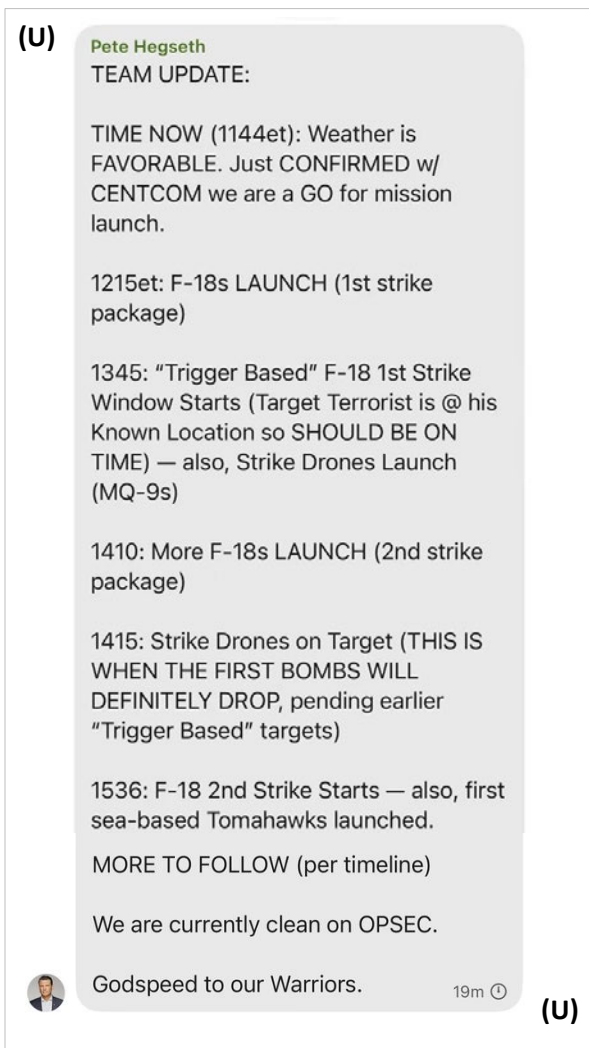
(U) We reviewed copies of Signal group chat messages provided by the DoD and through public reporting, information provided by USCENTCOM officials, sworn and recorded interviews with DoD officials, and a statement provided to the DoD OIG by the Secretary. From this information, we concluded that the Secretary sent sensitive,

²² (U) *Am. Oversight v. Hegseth*, Case No. 1:25-cv-883, (D.D.C. filed March 25, 2025) (ongoing).

(U) nonpublic, DoD operational information that he determined did not require classification over Signal on his personal cell phone. Although EO 13526 grants the Secretary the authority to determine the proper level of classification of DoD information, we concluded that the Secretary's actions did not comply with DoDI 8170.01, which prohibits using a personal device for official business and sending nonpublic information over a nonapproved commercially available messaging application.

(U) In his July 25 written statement to the DoD OIG, the Secretary confirmed that at 1144 EDT on March 15, he sent the message in Figure 2 on Signal.

(U) *Figure 2. Secretary of Defense Communication on Signal*



(U) Source: The Atlantic.

(U) This message to the Signal chat group contained sensitive operational details provided to the Secretary's office in the USCENTCOM Commander's email at 2054 EDT on March 14, approximately 15 hours earlier (See Figure 3).

(U) Figure 3. Excerpt of Email from the USCENTCOM Commander to the Secretary of Defense and A-CJCS from March 14 at 2054 EDT



(U) Source: USCENTCOM. Portion markings added to this figure represent derivative classification by the DoD OIG based on the markings in the source documents. Information highlighted in the figure was part of the original source document.

(S//NF) Overall, the Signal group chat message summarizes [REDACTED] as described in the email in Figure 3 that the USCENTCOM Commander provided to the Secretary. For example, the email identifies the same EDT and aircraft used (F/A-18As) and that this was the first strike package launching at that time. This language matches

(S//NF) the information shared in the group chat. The email timeline additionally identifies the EDT and trigger-based time on target and that MQ-9 “drones” were launching at that same time. Both the USCENTCOM Commander’s email and the group chat also feature the specific phrase, “We are currently clean on OPSEC.”

(U) The Secretary Determined the Information He Sent Did Not Require Classification, but the Secretary Did Not Comply with DoDI 8170.01 When He Sent Sensitive, Nonpublic DoD Information on Signal

(U) The Secretary provided a written statement to the DoD OIG on July 25, stating that under EO 13526, he is the OCA with “sole discretion to decide whether something should be classified or whether classified materials no longer require protection and can be declassified.” In his statement, the Secretary also wrote that he used “non-specific general details” that he deemed “not classified or that [he] could safely declassify” to develop an “unclassified summary” to provide to senior government officials. The Secretary also stated that the Signal message he sent contained no additional information that differed from what was sent to himself and other senior government officials through official classified communications channels. The details that the Secretary entered into the chat included information from the USCENTCOM email detailing the types of aircraft, launch times, and strike times for the operation. According to the USCENTCOM SCG, the operational movement of aircraft should be classified as SECRET. However, based on EO 13526, as the OCA for the DoD, the Secretary of Defense is authorized to declassify information as appropriate.

(U) In his statement, the Secretary wrote that he used “non-specific general details” to develop an “unclassified summary” to provide to senior government officials.

(U) We concluded that under EO 13526, the Secretary, as the agency head for the DoD, has the OCA authority to determine the required level of classification for any DoD information he communicates, such as through a document, message, or speech. DoDM 5200.45 identifies that the Secretary’s authority supersedes the authority of other OCAs in the DoD, including the USCENTCOM Commander, because all OCAs in the DoD are accountable to the Secretary. Although EO 13526 defines eight specific types of government information that may be classified, OCAs possess the discretion to determine whether any particular piece of information they create requires classification and at what level. That determination can be overridden by an OCA who supervises them. Under EO 13526, only the President can override a classification decision made by the Secretary of Defense.

(U) We also concluded that the Secretary’s actions did not comply with DoDI 8170.01 when he sent sensitive, nonpublic, DoD operational information over Signal from his

(U) personal cell phone. DoDI 8170.01 prohibits the use of personal devices for official government business and the use of nonapproved commercially available messaging applications, such as Signal, to process nonpublic or classified DoD information. Although the Secretary did not comply with DoDI 8170.01, we are not making a recommendation because the use of Signal to send sensitive, nonpublic, operational information is only one instance of a larger, DoD-wide issue. DoD OIG report no. DODIG-2026-022, "Evaluation of DoD Policy and Oversight Reports Related to Using Non-DoD-Controlled Electronic Messaging Systems to Conduct Official Business," recommends that the DoD improve training for DoD senior officials on maintaining the security of nonpublic DoD information.²³ Implementation of and adherence to that recommendation will eliminate noncompliance with DoD policies.

(U) The Secretary and OSD Did Not Retain the Secretary's Conversations on Signal as Official Records, as Required by Federal Law and DoD Policy

(U) We also found that the Secretary and OSD did not retain records of the Secretary's conversations on Signal discussing official government business, as required by 44 U.S.C. § 2911 and DoDI 5015.02, "DoD Records Management Program." Specifically, on April 30, 2025, we requested copies of the Signal messages the Secretary sent from his personal cell phone on or about March 15. In response to our request, the DoD provided a partial transcript of the Signal messages based on screenshots taken from the Secretary's personal cell phone on March 27, but this record did not include a significant portion of the Secretary's conversations disclosed by The Atlantic. When we asked whether the information provided represented the information the DoD preserved from the Secretary's cell phone, an OSD official stated that the DoD had provided all messages that were available at the time the screenshots were taken. Based on that statement and a review of the Signal chat settings described in the messages reported by The Atlantic, we concluded that some previous messages auto-deleted before preservation. Because we sent our request for copies of the messages more than 20 days after the messages were sent from the Secretary's personal cell phone, we concluded that the Secretary and OSD did not comply with 44 U.S.C. § 2911 and DoDI 5015.02. Specifically, those regulations require officers and employees of Executive Branch agencies and DoD employees to forward a complete copy of any record created on a nonofficial electronic messaging account to an official account within 20 days of the original creation or transmission of the record.

(U) Even though we identified that the Secretary did not comply with 44 U.S.C. § 2911 and DoDI 5015.02, we are not making a recommendation on this topic because records

²³ (U) DoD OIG Report No. DODIG 2026-022, "Evaluation of DoD Policy and Oversight Reports Related to Using Non-DoD-Controlled Electronic Messaging Systems to Conduct Official Business," December 2, 2025.

(U) management issues arising from the use of Signal and other commercially available messaging applications are a DoD-wide issue. DoD OIG report no. DODIG-2026-022 also recommends that the DoD improve training for DoD senior officials on compliance with records retention laws and policies. Implementation of and adherence to that recommendation will eliminate noncompliance with DoD policies.

(U) As a result of an ongoing court case, the DoD did preserve a record of the Signal chat in a Federal Records Act-compliant system.²⁴ However, this record did not originate from the Secretary or DoD and, therefore, did not meet the requirements of 44 U.S.C. § 2911 and DoDI 5015.02 for the Secretary to forward a complete copy of a record created on a nonofficial electronic messaging account to an official account within 20 days of the record's creation or transmission. Specifically, a May 7, 2025 filing with a Federal district court stated that the DoD received an email from the White House Counsel's Office containing a consolidated version of the Signal chat created based on publicly available information and information saved from participants' phones. We requested that the DoD provide us with a copy of the Signal chat referenced in the May 7, 2025 court filing. However, the DoD declined our request for a copy of the complete transcript because it was not a DoD-created record.

(U) The Secretary's Communication of Nonpublic DoD Information Created Additional Risks to U.S. Forces and Missions

(U) The Secretary sent information identifying the quantity and strike times of manned U.S. aircraft over hostile territory over an unapproved, unsecure network approximately 2 to 4 hours before the execution of those strikes. Although the Secretary wrote in his July 25 statement to the DoD OIG that "there were no details that would endanger our troops or the mission," if this information had fallen into the hands of U.S. adversaries, Houthi forces might have been able to counter U.S. forces or reposition personnel and assets to avoid planned U.S. strikes. Even though these events did not ultimately occur, the Secretary's actions created a risk to operational security that could have resulted in failed U.S. mission objectives and potential harm to U.S. pilots.

(U) The Secretary's actions created a risk to operational security that could have resulted in failed U.S. mission objectives and potential harm to U.S. pilots.

(S//NF) Using a personal cell phone to conduct official business and send nonpublic DoD information through Signal risks potential compromise of sensitive DoD information. [REDACTED]

²⁴ (U) *Am. Oversight v. Hegseth*, Case No. 1:25-cv-883, (D.D.C. filed March 25, 2025) (ongoing).

(S//NF) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) We are not making any recommendations in this report related to the Secretary's use of Signal to send sensitive nonpublic information because it represented only one instance of an identified, DoD-wide issue. DoD OIG report no. DODIG-2026-022 recommends that the DoD improve training and implementation of information security procedures and record retention requirements for DoD senior officials. Implementation of and adherence to that recommendation will address the finding of this report.

(U) Management Comments on the Finding and Our Response

(U) Although not required to comment, the DoD's Deputy General Counsel for Legislation, Investigations, and Oversight provided management comments on the report's finding. Specifically, the Deputy General Counsel provided additional contextual language for the DoD OIG to consider regarding the Secretary's participation in the Signal chat and the retention duration that the chat participants set for the messages. The Deputy General Counsel also provided additional context that questions the accuracy of The Atlantic's record of the Signal chat, as well as a justification for the Secretary's noncompliance with Federal recordkeeping law and DoD policy regarding retention of electronic messages. Specifically, the Deputy General Counsel cited the Secretary's pressing work and travel schedule following the March 15 strikes as preventing him from retaining copies of all of the chat messages in accordance with law and policy.

(U) Our Response

(U) We appreciate the Deputy General Counsel's comments on the report finding. However, the Deputy General Counsel did not provide any documentation to support this additional context. As a result, we could not independently verify the Deputy General Counsel's information. Therefore, in accordance with our evaluation standards and without evidence to support this information, we did not include this language in the body of the report. We included the Deputy General Counsel's full response with the additional context in the Management Comments section of this report.

(U) Recommendation, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the Chief of the U.S. Central Command Special Security Office review the command's classification procedures and ensure that clear requirements are communicated to U.S. Central Command personnel for portion marking classified information in accordance with DoD Manual 5200.01, Volume 2. If the review finds that the procedures are insufficient, the Chief should update, issue, and provide instruction on additional procedures. If the review finds that the procedures are sufficient, the Chief should develop and implement additional training for U.S. Central Command personnel to instruct them in proper techniques for marking classified information.

(U) U.S. Central Command Special Security Office Comments

(U) The Chief of the USCENTCOM Special Security Office agreed with the recommendation and described how USCENTCOM met its intent. Specifically, the Chief stated that the USCENTCOM Special Security Office conducted an in-depth review of USCENTCOM's classification procedures and found that the command has a well-established and comprehensive training program to provide USCENTCOM personnel with guidance on properly marking classified information. The Chief identified that USCENTCOM has five initial and annual trainings that cover the requirements to properly mark classified information, including with portion markings for each paragraph. The Chief also provided a copy of one of USCENTCOM's annual security trainings demonstrating the comprehensive discussion regarding portion marking classified documents.

(U) Our Response

(U) Comments from the Chief addressed the recommendation. Additionally, the Chief provided training documentation and USCENTCOM guidance on the command's requirements to portion mark classified documents, including emails. Based on the comments and our review of the documentation and guidance provided, we determined that USCENTCOM met the intent of the recommendation; therefore, the recommendation is closed. We appreciate USCENTCOM's rapid attention to addressing the recommendation.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this evaluation from April through October 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) The scope of our evaluation focused on identifying the factual circumstances and adherence to policies and procedures surrounding the Secretary’s reported use of Signal to conduct official government business from approximately March 14 through March 16, 2025. As a result, our report does not try to identify whether any person violated criminal laws.

(U) To perform this evaluation and achieve our objective, we obtained and reviewed information from the OSD, DoD OCIO, and USCENTCOM. Specifically, we issued requests for information and documentation to those offices and reviewed their responses for relevance to our project objective. We also conducted sworn and recorded interviews with 10 current and former DoD officials from the OSD and OCIO to obtain testimonial evidence to support our finding.

(U) Additionally, we collected and reviewed the following laws, policies, directives, regulations, memorandums, and command-specific guidance on proper safeguarding of classified information, authorized use of commercially available messaging applications, and the declassification of classified information.

- (U) Presidential and Federal Records Act Amendments of 2014, Pub. L. No. 113-187
- (U) 44 U.S.C. § 2911, “Disclosure Requirements for Official Business Conducted Using Non-Official Electronic Messaging Accounts”
- (U) 32 C.F.R. § 2002.4, “Definitions”
- (U) Executive Order 13526, “Classified National Security Information,” December 29, 2009

- (U) DoD Directive (DoDD) 5205.16, "The DoD Insider Threat Program," September 30, 2014 (Incorporating Change 2, August 28, 2017)
- (U) DoDD 5210.50 "Management of Serious Security Incidents Involving Classified Information," October 27, 2014 (Incorporating Change 2, September 18, 2020)
- (U) DoDD 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012 (Incorporating Change 2, August 20, 2020)
- (U) DoDI 5015.02, "DoD Records Management Program," February 24, 2015 (Incorporating Change 1, August 17, 2017)
- (U) DoDI 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019 (Incorporating Change 1, February 9, 2022)
- (U) DoDI 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
- (U) DoDI 5015.02, "DoD Records Management Program," February 24, 2015 (Incorporating Change 1, August 17, 2017)
- (U) DoDI 5200.48, "Controlled Unclassified Information," March 6, 2020
- (U) DoDI 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019 (Incorporating Change, March 12, 2025)
- (U) DoDI 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Non-Public DoD Information," December 9, 2019
- (U) DoDM 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012 (Incorporating Change 3, January 17, 2025)
- (U) DoDM 5200.01, Volume 2, "DoD Information Security Program: Marking of Information," February 24, 2012 (Incorporating Change 4, July 28, 2020)
- (U) DoDM 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012 (Incorporating Change 4, January 17, 2025)
- (U) DoDM 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012

- (U) DoDM 5200.45, “Original Classification Authority and Writing a Security Classification Guide,” January 17, 2025
- (U) DoD Chief Information Officer Memorandum, “Mobile Application Security Requirements,” October 6, 2017
- (U) Secretary of Defense Memorandum, “Review of Department of Defense Security Policies and Procedures,” April 14, 2023
- (U) DoD Chief Information Officer Memorandum, “Use of Unclassified Mobile Applications in Department of Defense,” October 6, 2023
- (U) Deputy Secretary of Defense Memorandum, “Mobile Device Restrictions in the Pentagon,” May 22, 2018
- (U) USCENTCOM SCG, Central Command Regulation 380-14, November 16, 2022

(U) We reviewed the documentary evidence provided by OSD, OCIO, and USCENTCOM officials, as well as the recorded and sworn interviews we conducted. Because of gaps in the information the DoD provided regarding the Signal chat, we also relied on the public reporting from The Atlantic to obtain a full transcript of the group chat.

(U) Use of Computer-Processed Data

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

(U) Use of Technical Assistance

(U) We obtained support from the Administrative Investigations and Defense Criminal Investigative Service Components in the DoD OIG. Both Components advised and assisted the project team with analysis of potential criminal conduct and taking recorded and sworn testimony from DoD officials.

(U) Appendix B

(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 direct 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]

[REDACTED]

(S) [REDACTED]

(S) [REDACTED]

(S) [REDACTED]
[REDACTED]
[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, DoDM 5200.01, and Secretary of Defense 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]
[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 was 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]

[REDACTED]

(CU) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[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.”

(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 posed 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 found that DoD personnel violated policy and misused mobile applications because the DoD did not have a comprehensive mobile device and application policy that addressed the operational and cybersecurity risks associated with the use of mobile devices and applications. In addition, the Defense Information 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 varied widely in the features and applications that users were permitted to access and use. DoD officials might not be aware of the operational and cybersecurity risks that unmanaged applications pose to the DoD. DoD personnel might 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 Chief Information Officer (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 Under Secretary of Defense for Intelligence and Security, 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 application and mobile device features;
- (U) address the DoD records management requirements of DoDI 5015.02 and 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; and²⁶
- (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]
[REDACTED]
[REDACTED]
[REDACTED]
[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, USCENTCOM, 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]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[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 impeded their ability to use DoD-controlled systems.

(U) The report made 13 recommendations, of which 5 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 Under Secretary of Defense for Intelligence and Security develop policy to strengthen the DoD operational security program. This recommendation is closed.
- (U) the Under Secretary of Defense for Intelligence and Security develop operational security 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, USCENTCOM, U.S. European Command, U.S. Indo-Pacific Command, 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, USCENTCOM, and U.S. European Command but remain open for the U.S. Indo-Pacific Command and 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 course of 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 DoD record retention policies.

(U) The report recommended that the then Secretary of Defense 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 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 C

(U) Additional Information Related to the Secretary's Use of Signal to Conduct Official Business

(U) During our evaluation, additional public reporting alleged that the Secretary's use of Signal extended beyond the "Houthi PC Small Group" reported by The Atlantic. At the additional request of the Members of Congress, we included those additional matters in our evaluation. Specifically, according to eight officials in the OSD and OCIO, the Secretary communicated using Signal on his personal cell phone for official DoD business outside of the March 2025 "Houthi PC Small Group" chat. According to the officials, this led to the creation of multiple Signal group chats in which the Secretary and others allegedly discussed official DoD business and nonpublic information. Additionally, officials in SD Comms stated that, at the request of the Secretary's junior military assistant (JMA), SD Comms created and installed a unique system that provided the Secretary with access to his personal cell phone from inside his secure office space in the Pentagon.

(U) The Secretary Allegedly Participated in Several Additional Signal Chats, According to DoD Officials

(U) Five officials from the OSD and OCIO identified in interviews the existence of multiple additional Signal group chats in which the Secretary allegedly participated to conduct official DoD business and transmit nonpublic DoD information. Two officials stated that they were part of several group chats, and one of them stated that the Secretary and others used the chats to coordinate meetings, respond to media inquiries, or alert staff to check their official email accounts. One official also stated that they were part of a Signal group chat on their personal cell phone titled "Defense Team Huddle," which included non-DoD personnel, but the official did not provide us with copies of the messages. The official stated that the Secretary occasionally used this group chat to direct staff to perform specific DoD work tasks, "such as creating a Secretary directive or research whether a social media post concerning [Diversity, Equity, and Inclusion] was correct." Lastly, one official told us that while on official travel, the Secretary used Signal on his personal cell phone to coordinate with DoD officials for events in his capacity as Secretary. All of the officials we spoke with stated that the Secretary participated in these additional group chats using his personal cell phone, not a government-furnished electronic device.

(U) One of the officials we spoke with stated that the Secretary posted the same sensitive operational information concerning the Houthi attack plans on the "Defense Team Huddle" group chat. As a result, we requested copies of messages from these other Signal group chats, as well as access to the Secretary's personal cell phone.

(U) However, a senior official in the Secretary's office stated that the Secretary would not provide access to his personal cell phone. Therefore, we were not able to verify whether any of the additionally identified Signal chats also contained sensitive, classified, or other nonpublic DoD information.

(U) The Secretary's JMA Facilitated the Installation of a Unique System to Allow the Secretary to Access His Personal Cell Phone from Inside His Secure Office

(U) During our evaluation, we also learned that, at the request of the Secretary, the JMA requested and oversaw the installation of a unique capability through which the Secretary could access and control his personal cell phone from inside his secure office. Based on the description SD Comms officials provided, the unique system was designed to mirror and access the contents of the Secretary's personal cell phone from in his Pentagon office, connecting a keyboard, mouse, and monitor by cable to his personal cell phone, which was located outside of his office. SD Comms officials provided photographic documentation depicting this arrangement and stated that it was consistent with DoD information security requirements, which did not allow for any cell phones to be brought into the Secretary's suite. The Secretary acknowledged the creation of this system in his July 25 statement to the DoD OIG, saying, "It is true that upon taking this job, I asked my comms team whether it was possible to get access to my personal cell phone in my office so I could more easily receive non-official, communications during the workday.... The comms team prepared a compliant solution that would allow me this access while also maintaining proper security." Figure 4 shows the prototype of the system in testing.

(U) Figure 4. Prototype of Tethering Solution Allowing the Secretary to Access His Personal Cell Phone from His Office at the Pentagon



(CUI) Source: Secretary of Defense Communications Team. [REDACTED]
[REDACTED]
[REDACTED]

(U) According to a May 22, 2018 Deputy Secretary of Defense memorandum, personal and government mobile devices that transmit, store, or record data are prohibited inside secure spaces in the Pentagon, such as the Secretary's office suite, unless an exemption to policy is granted. The May 22, 2018 memorandum also states that mobile devices may be used in common areas and spaces in the Pentagon that are not designated or accredited for processing, handling, or discussing classified information. While SD Comms officials stated that they implemented the tethering solution on February 27, 2025, allowing the Secretary to access his personal cell phone from in his office while the phone remained outside of a secure space, we were not able to directly observe this implementation. According to SD Comms officials, officials from the OSD removed the system by late April 2025. As a result, we could not determine whether it met DoD information security requirements.

(U) Appendix D

(U) Transcript of the Signal Group Chat Published by The Atlantic on March 24 and March 26, 2025



(U) Transcript of the Signal Group Chat Published by The Atlantic on March 24 and March 26, 2025 (cont'd)

(U)

Brian
B Brian McCormack for NSC 6:34 PM

Today

Michael Waltz
Team, you should have a statement of conclusions with taskings per the Presidents guidance this morning in your high side inboxes.

State and DOD, we developed suggested notification lists for regional Allies and partners.

Joint Staff is sending this am a more specific sequence of events in the coming days and we will work w DOD to ensure COS, OVP and POTUS are briefed.

8:05 AM

Today

JD Vance
Team, I am out for the day doing an economic event in Michigan. But I think we are making a mistake.

3 percent of US trade runs through the suez. 40 percent of European trade does. There is a real risk that the public doesn't understand this or why it's necessary.

The strongest reason to do this is, as POTUS said, to send a message. But I am not sure the president is aware how inconsistent this is with his message on Europe right now. There's a further risk that we see a moderate to severe spike in oil prices.

I am willing to support the consensus of the team and keep these concerns to myself. But there is a strong argument for delaying this a month, doing the messaging work on why this matters, seeing where the economy is, etc.

8:16 AM

(U)

(U) Transcript of the Signal Group Chat Published by The Atlantic on March 24 and March 26, 2025 (cont'd)

(U)

Joe Kent

There is nothing time sensitive driving the time line. We'll have the exact same options in a month.

The Israelis will likely take strikes & therefore ask us for more support to replenish whatever they use against the Houthis. But that's a minor factor.

I will send you the unclass data we pulled on BAM shipping.

JK

8:22 AM ⓘ

John Ratcliffe

From CIA perspective, we are mobilizing assets to support now but a delay would not negatively impact us and additional time would be used to identify better starting points for coverage on Houthi leadership

JR

8:26 AM ⓘ

Pete Hegseth

Today

VP:

I understand your concerns — and fully support you raising w/ POTUS. Important considerations, most of which are tough to know how they play out (economy, Ukraine peace, Gaza, etc). I think messaging is going to be tough no matter what — nobody knows who the Houthis are — which is why we would need to stay focused on: 1) Biden failed & 2) Iran funded.

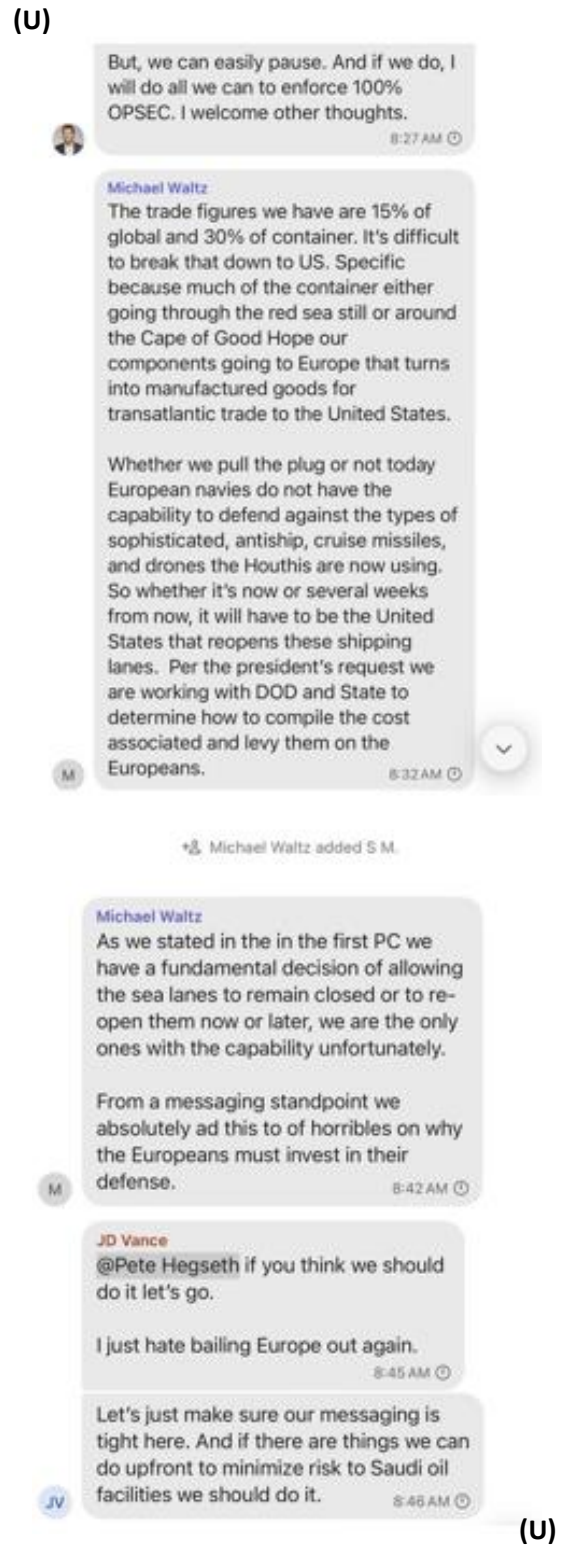
Waiting a few weeks or a month does not fundamentally change the calculus. 2 immediate risks on waiting: 1) this leaks, and we look indecisive; 2) Israel takes an action first — or Gaza cease fire falls apart — and we don't get to start this on our own terms. We can manage both.

We are prepared to execute, and if I had final go or no go vote, I believe we should. This not about the Houthis. I see it as two things: 1) Restoring Freedom of Navigation, a core national interest; and 2) Reestablish deterrence, which Biden cratered.

✓

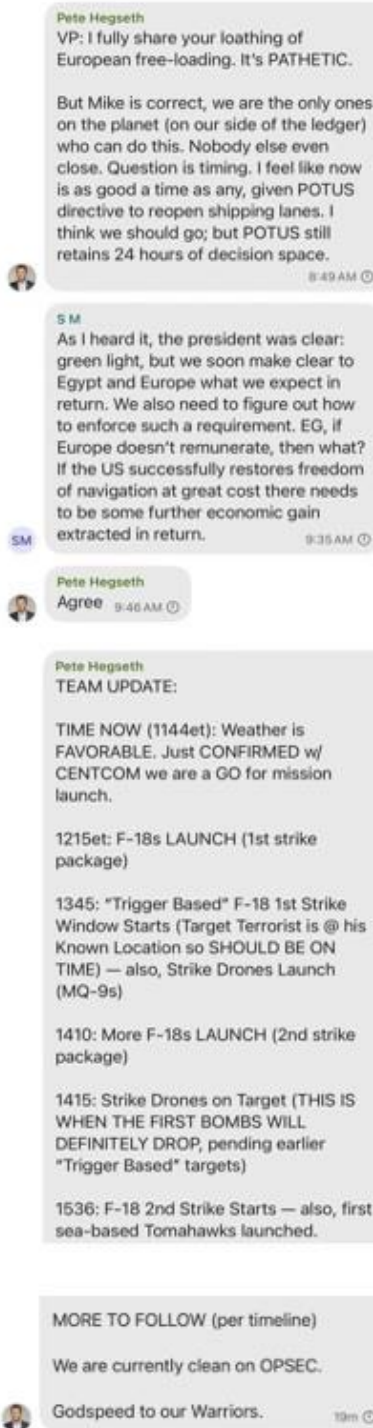
(U)

(U) Transcript of the Signal Group Chat Published by The Atlantic on March 24 and March 26, 2025 (cont'd)



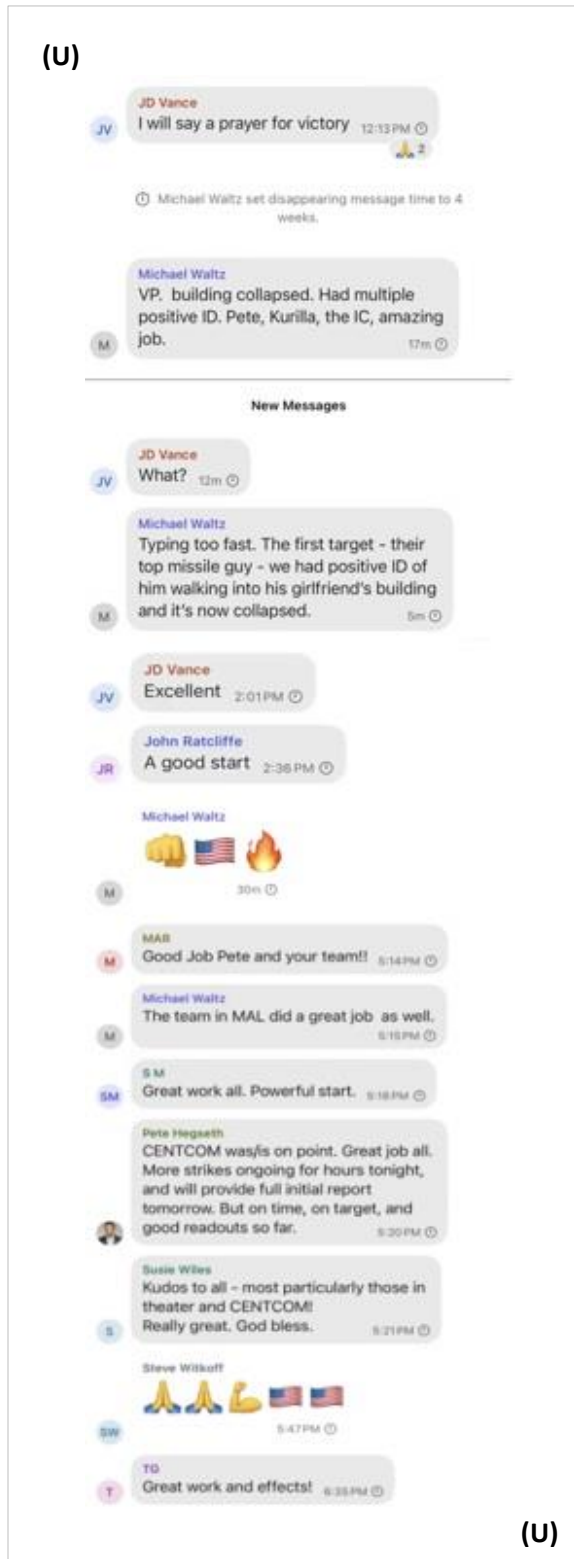
(U) Transcript of the Signal Group Chat Published by The Atlantic on March 24 and March 26, 2025 (cont'd)

(U)

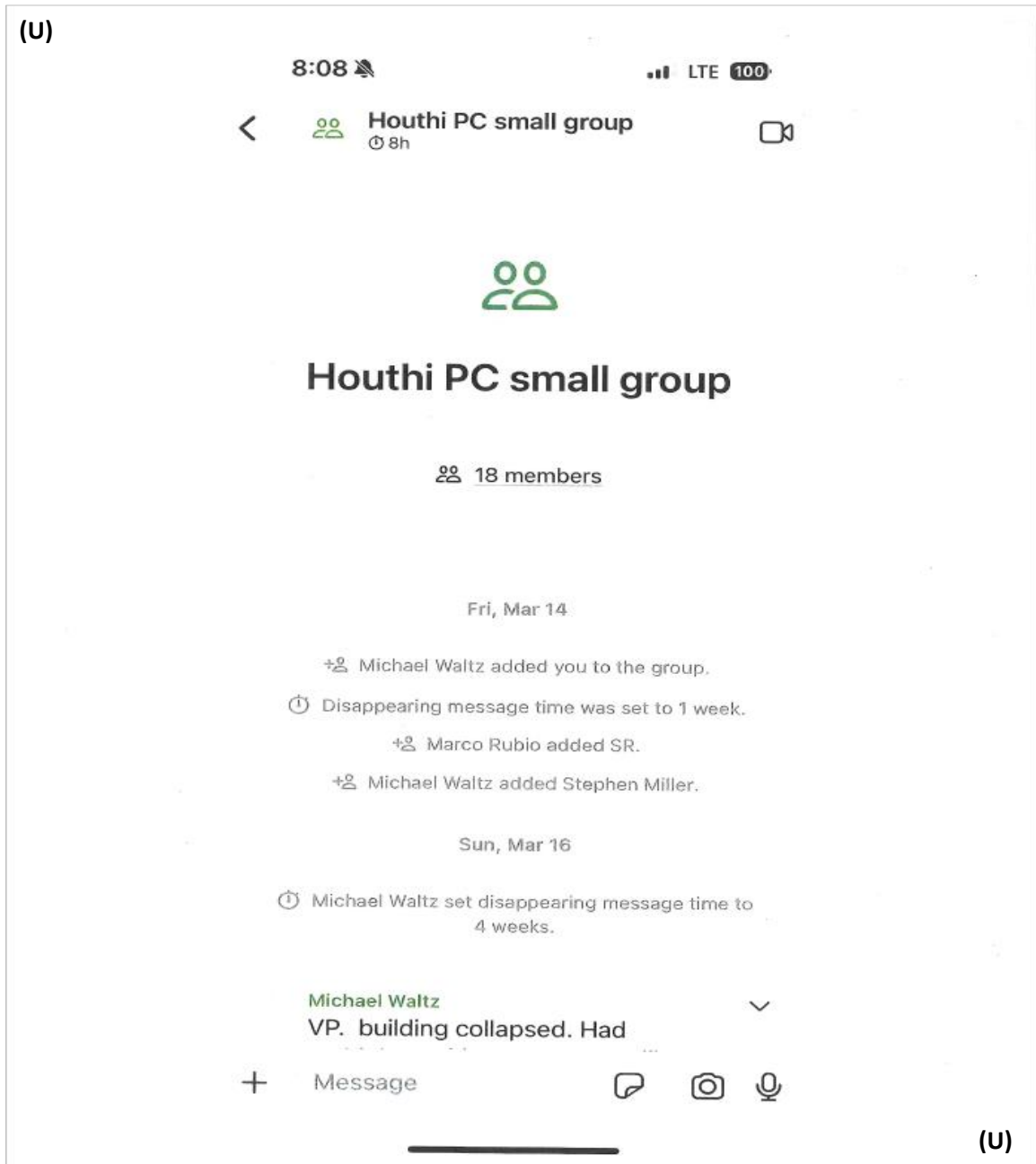


(U)

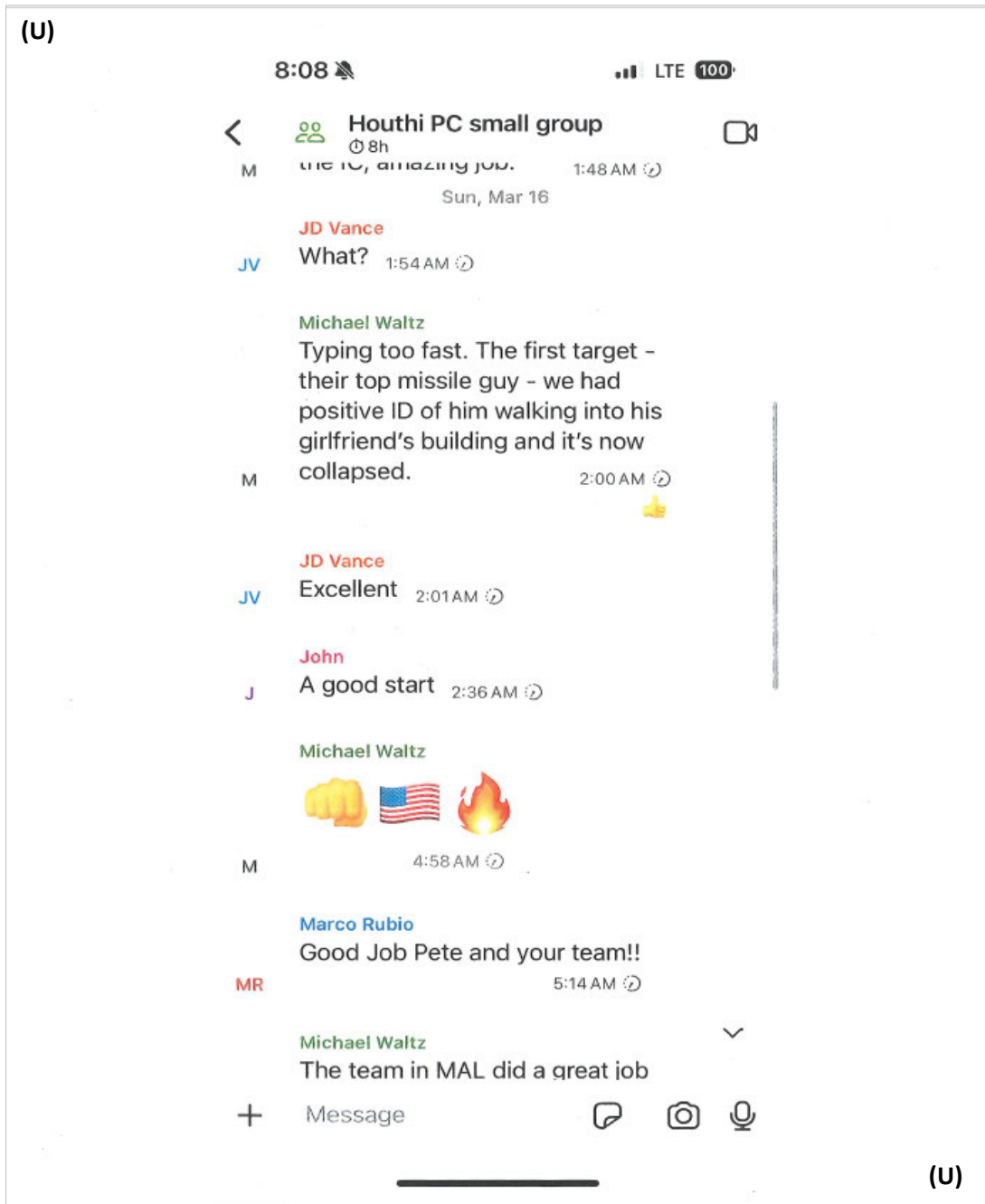
(U) Transcript of the Signal Group Chat Published by The Atlantic on March 24 and March 26, 2025 (cont'd)



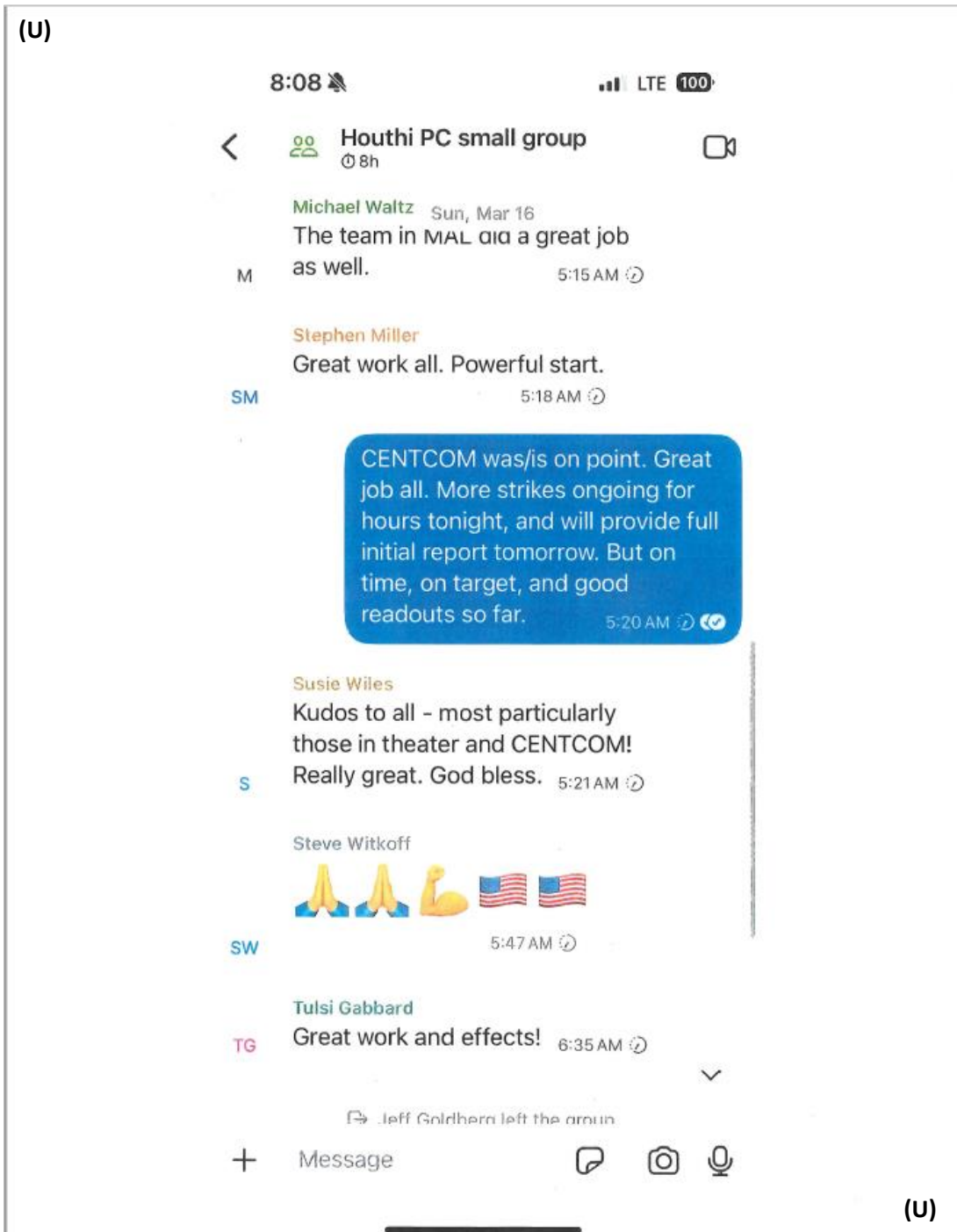
(U) Partial Transcript of the Signal Group Chat Retained by the DoD on March 27, 2025, from the Secretary of Defense's Personal Cell Phone



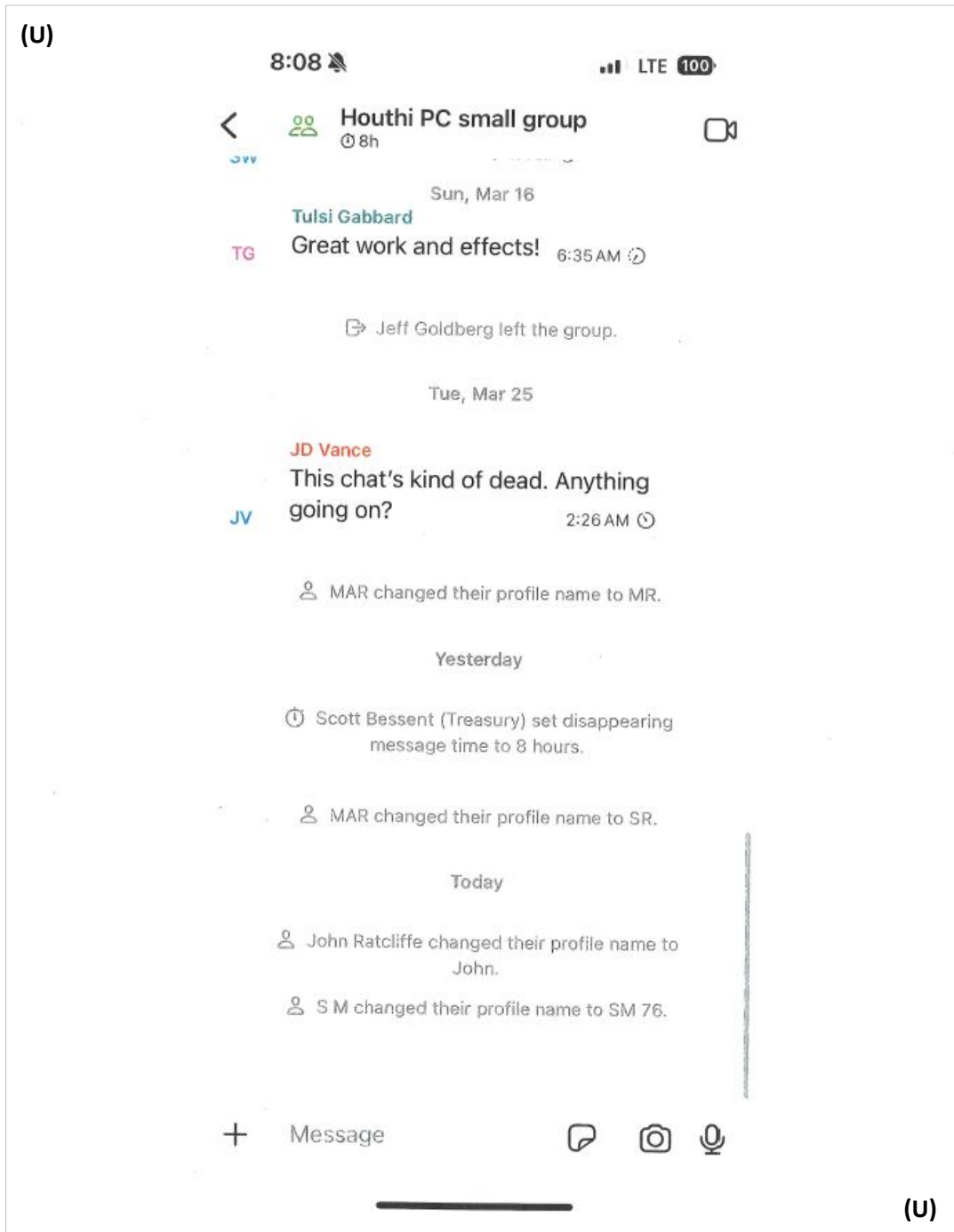
(U) Partial Transcript of the Signal Group Chat Retained by the DoD on March 27, 2025, from the Secretary of Defense's Personal Cell Phone (cont'd)



(U) Partial Transcript of the Signal Group Chat Retained by the DoD on March 27, 2025, from the Secretary of Defense's Personal Cell Phone (cont'd)



(U) Partial Transcript of the Signal Group Chat Retained by the DoD on March 27, 2025, from the Secretary of Defense's Personal Cell Phone (cont'd)



(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 2054 EDT on March 14, 2025

~~(S//NF)~~

From: Kurilla, Michael Erik GEN USARMY CENTCOM CCCG (USA)
Sent: Friday, March 14, 2025 8:54 PM
To: Buria, Ricky D Col USMC HQMC (USA); Grady, Christopher W ADM USN JS OCJCS (USA)
Cc: [REDACTED] Kasper, Joseph R SES (USA); ActingDepSecDef36; Carroll, Collin J SES (USA); Velez-Green, Alexander J SES (USA); GARD-WEISS, Dustin J SES OSD OUSD INTEL & SEC (USA); Dory, Amanda J SES OSD OUSD POLICY (USA); Young, Charles L SES OSD OGC (USA); Clearfield, Joseph R BGen USMC OSD OSD (USA); Thompson, Katherine E SES (USA); Zakriski, Jennifer N SES OSD OUSD POLICY (USA); Jenkins, Colby C SES (USA); Sims, Douglas Arthur (D.A.) II LTG USARMY JS ODJS (USA); Henry, Dimitri LtGen USMC JS J2 (USA); Grynkeiwich, Alexis G Lt Gen USAF JS J3 (USA); Spedero, Paul C Jr RADM USN JS J3 (USA); McGee, Joseph P (JP) LTG USARMY JS J5 (USA); Osborne, Erin P RDML USN JS J5 (USA); Morgan, Shane P BG USARMY JS J3 (USA); [REDACTED] CENTCOM Macdill AFB CENTCOM HQ List CENTCOM JDIR Small Group
Subject: ~~(SECRET//NOFORN)~~ USCENTCOM OPN ROUGH RIDER C Houthi Campaign (POD 15/16 MAR) Update
Attachments: [REDACTED]

Classification: ~~SECRET//NOFORN~~

~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 2054 EDT on March 14, 2025 (cont'd)

~~(S//NF)~~



~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 2054 EDT on March 14, 2025 (cont'd)

~~(S//NF)~~

VR,
Erik

People, Partners, Innovation

GEN Michael E. Kurilla
Commander, U.S. Central Command

~~Classified By: Kurilla, Michael Erik GEN USARMY CENTCOM CCCC (USA)~~
~~Derived From: USCENTCOM SCG, CCR 380-14, 16 November 2022~~
~~Declassify On: 2050-03-14~~
~~Classification: ~~SECRET//NOFORN~~~~

~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 1255 EDT on March 15, 2025

~~(S//NF)~~

From: Kurilla, Michael Erik GEN USARMY CENTCOM CCCG (USA)
Sent: Saturday, March 15, 2025 12:55 PM
To: Grady, Christopher W ADM USN JS OCJCS (USA); Buria, Ricky Col SD
Cc: [REDACTED] Kasper, Joseph R SES (USA);
ActingDepSecDef36; Carroll, Colin J SES (USA); Velez-Green, Alexander J SES (USA);
GARD-WEISS, Dustin J SES OSD OUSD INTEL & SEC (USA); Dory, Amanda J SES OSD
OUSD POLICY (USA); Young, Charles L SES OSD OGC (USA); Clearfield, Joseph R BGen
USMC OSD OSD (USA); Thompson, Katherine E SES (USA); Zakriski, Jennifer N SES OSD
OUSD POLICY (USA); Jenkins, Colby C SES (USA); Sims, Douglas Arthur (D.A.) II LTG
USARMY JS ODJS (USA); Henry, Dimitri LtGen USMC JS J2 (USA); Grynkeiwich, Alexis G
Lt Gen USAF JS J3 (USA); Spedero, Paul C Jr RADM USN JS J3 (USA); McGee, Joseph P
(JP) LTG USARMY JS J5 (USA); Osborne, Erin P RDML USN JS J5 (USA); Morgan, Shane P
BG USARMY JS J3 (USA); [REDACTED] CENTCOM
Macdill AFB CENTCOM HQ List CENTCOM JDIR Small Group
Subject: ~~(S//NF)~~ USCENTCOM OPN ROUGH RIDER C-Houthi Campaign H-1:00
Update (15 1645Z MAR)

Classification: ~~SECRET//NOFORN~~

~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 1255 EDT on March 15, 2025 (cont'd)


~~(S//NF)~~



~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 1255 EDT on March 15, 2025 (cont'd)


~~(S//NF)~~



VR,
Erik

People, Partners, Innovation

GEN Michael E. Kurilla
Commander, U.S. Central Command



~~Classified By: Kurilla, Michael Erik GEN USARMY CENTCOM CCCC (USA)~~
~~Derived From: USCENTCOM SCG, CCR 380-14, 16 November 2022~~
~~Declassify On: 2050-03-15~~
~~Classification: SECRET//NOFORN~~

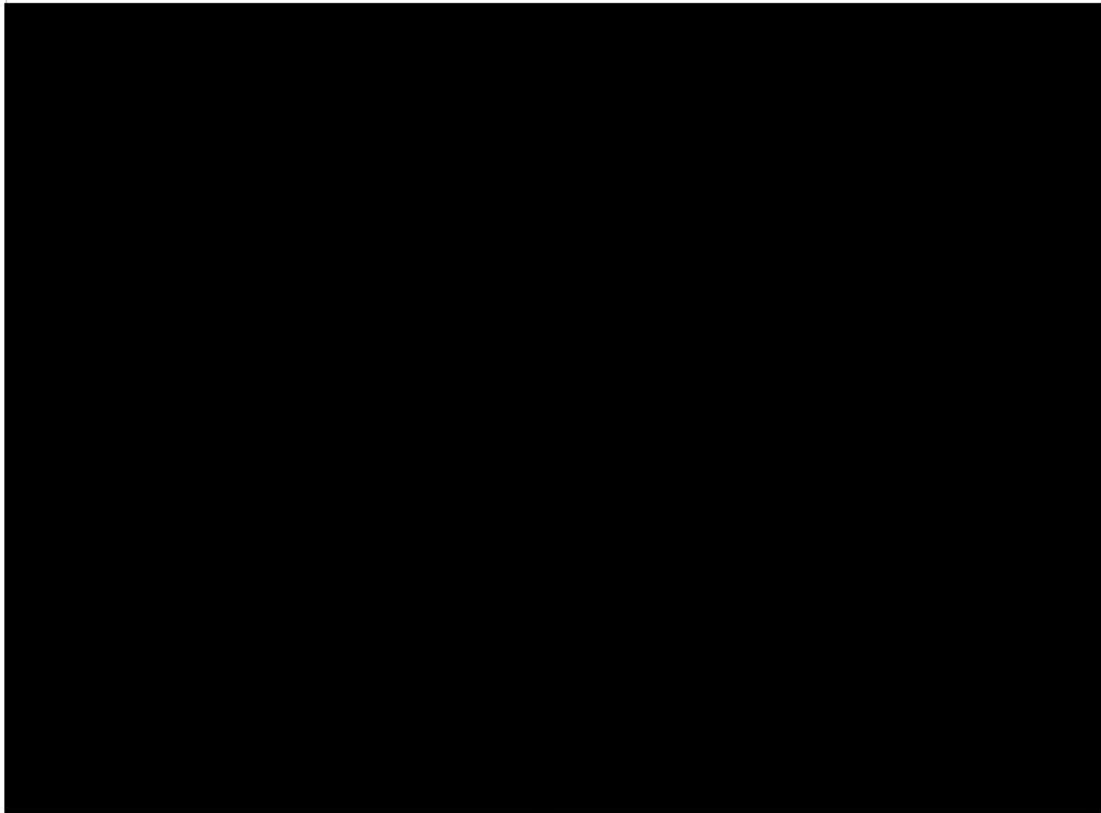
~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 1346 EDT on March 15, 2025

~~(S//NF)~~

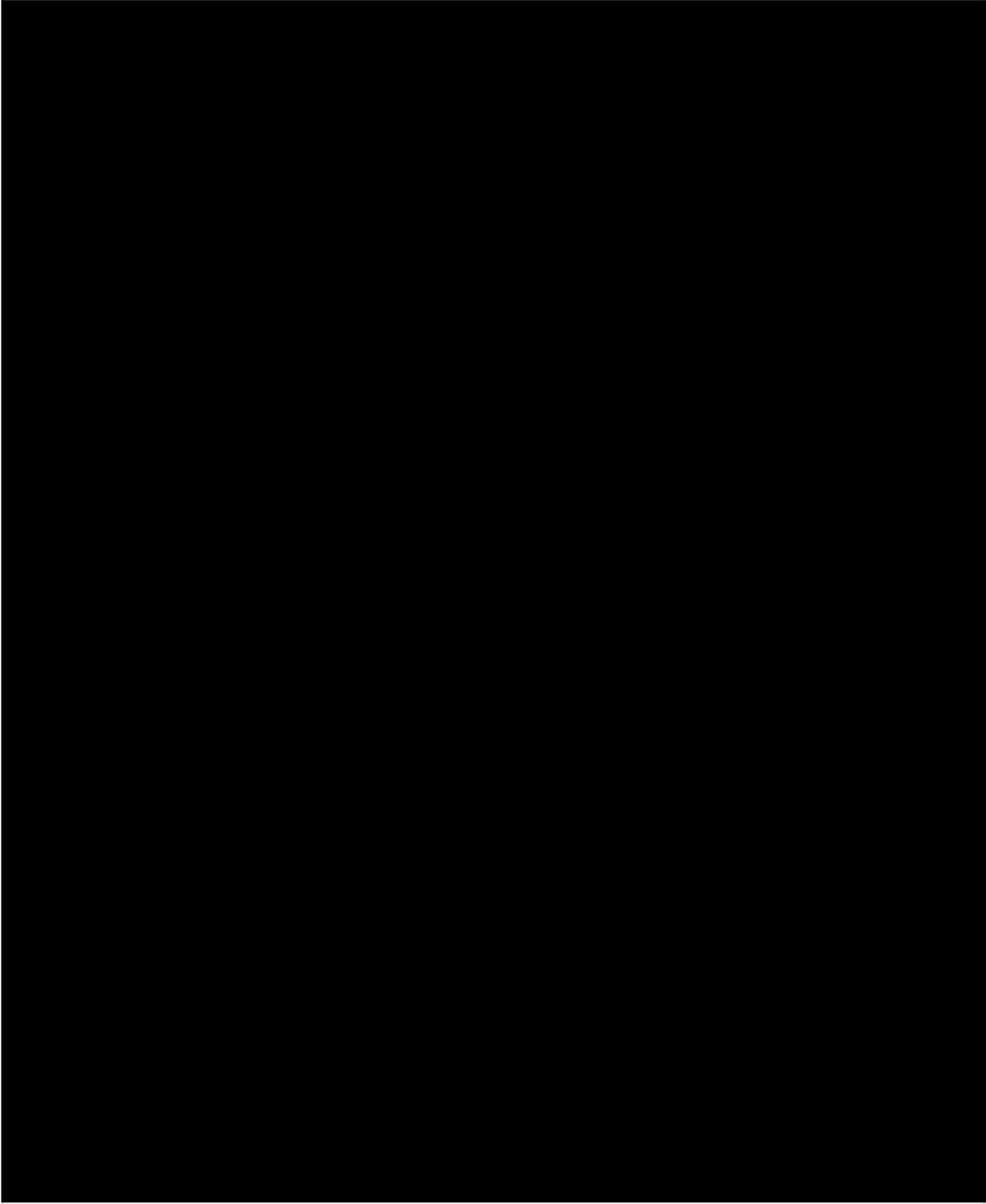
From: Kurilla, Michael Erik GEN USARMY CENTCOM CCCG (USA)
Sent: Saturday, March 15, 2025 1:46 PM
To: Grady, Christopher W ADM USN JS OCJCS (USA); Buria, Ricky Col SD
Cc: [REDACTED] Kasper, Joseph R SES (USA); ActingDepSecDef36; Carroll, Colin J SES (USA); Velez-Green, Alexander J SES (USA); GARD-WEISS, Dustin J SES OSD OUSD INTEL & SEC (USA); Dory, Amanda J SES OSD OUSD POLICY (USA); Young, Charles L SES OSD OGC (USA); Clearfield, Joseph R BGen USMC OSD OSD (USA); Thompson, Katherine E SES (USA); Zakriski, Jennifer N SES OSD OUSD POLICY (USA); Jenkins, Colby C SES (USA); Sims, Douglas Arthur (D.A.) II LTG USARMY JS ODJS (USA); Henry, Dimitri LtGen USMC JS J2 (USA); Grynkeiwich, Alexis G Lt Gen USAF JS J3 (USA); Spedero, Paul C Jr RADM USN JS J3 (USA); McGee, Joseph P (JP) LTG USARMY JS J5 (USA); Osborne, Erin P RDML USN JS J5 (USA); Morgan, Shane P BG USARMY JS J3 (USA); [REDACTED] CENTCOM Macdill AFB CENTCOM HQ List CENTCOM JDIR Small Group
Subject: ~~(SECRET//NOFORN)~~ USCENTCOM OPN ROUGH RIDER C-Houthi Campaign H-Hour Update (15 1745Z MAR)

Classification: ~~SECRET//NOFORN~~



(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 1346 EDT on March 15, 2025 (cont'd)

~~(S//NF)~~



~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 1346 EDT on March 15, 2025 (cont'd)

~~(S//NF)~~

Erik

People, Partners, Innovation

GEN Michael E. Kurilla
Commander, U.S. Central Command

~~Classified By:~~ Kurilla, Michael Erik GEN USARMY CENTCOM CCCC (USA)

~~Derived From:~~ USCENTCOM SCG, CCR 380-14, 16 November 2022

~~Declassify On:~~ 2050-03-15

~~Classification:~~ ~~SECRET//NOFORN~~

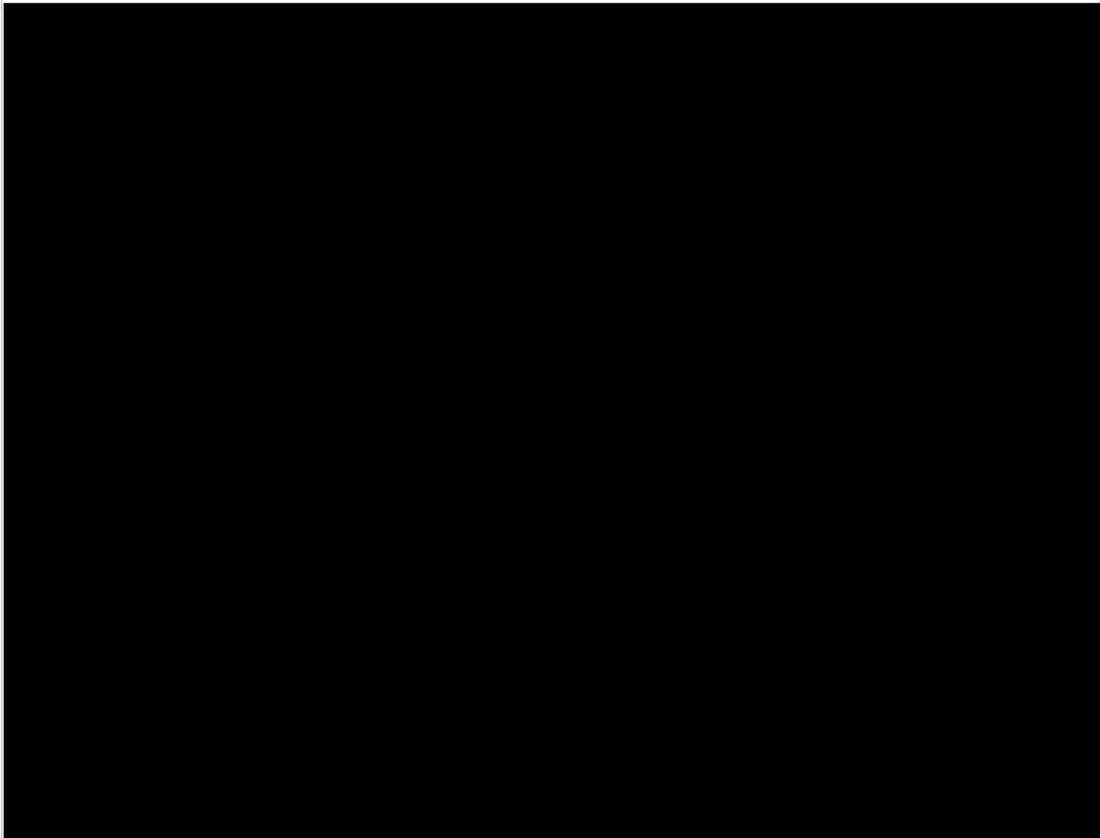
~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 2111 EDT on March 15, 2025

~~(S//NF)~~

From: Kurilla, Michael Erik GEN USARMY CENTCOM CCCG (USA)
Sent: Saturday, March 15, 2025 9:11 PM
To: Grady, Christopher W ADM USN JS OCJCS (USA); Buria, Ricky Col SD
Cc: [REDACTED] Caldwell, Daniel D Jr SES (USA); Kasper, Joseph R SES (USA); ActingDepSecDef36; Carroll, Colin J SES (USA); Velez-Green, Alexander J SES (USA); GARD-WEISS, Dustin J SES OSD OUSD INTEL & SEC (USA); Dory, Amanda J SES OSD OUSD POLICY (USA); Young, Charles L SES OSD OGC (USA); Clearfield, Joseph R BGen USMC OSD OSD (USA); Thompson, Katherine E SES (USA); Zakriski, Jennifer N SES OSD OUSD POLICY (USA); Jenkins, Colby C SES (USA); Sims, Douglas Arthur (D.A.) II LTG USARMY JS ODJS (USA); Henry, Dimitri LtGen USMC JS J2 (USA); Grynkeiwich, Alexis G Lt Gen USAF JS J3 (USA); Spedero, Paul C Jr RADM USN JS J3 (USA); McGee, Joseph P (JP) LTG USARMY JS J5 (USA); Osborne, Erin P RDML USN JS J5 (USA); Morgan, Shane P BG USARMY JS J3 (USA); [REDACTED]
Subject: [REDACTED] CENTCOM Macdill AFB CENTCOM HQ List CENTCOM JDIR Small Group ~~(SECRET//NOFORN)~~ USCENTCOM OPN ROUGH RIDER C Houthi Campaign D-Day Final Update (16 0100Z MAR)

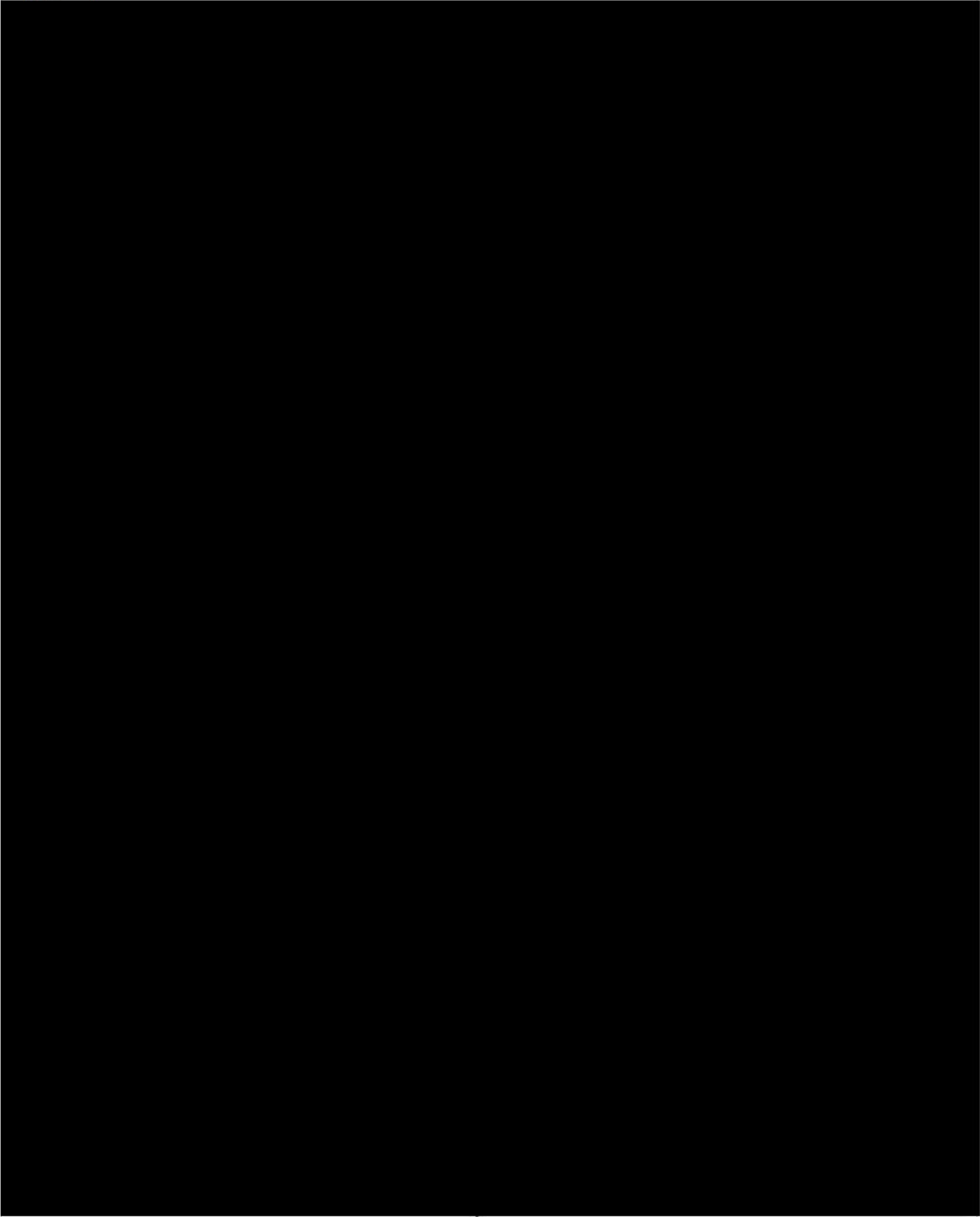
Classification: ~~SECRET//NOFORN~~



~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 2111 EDT on March 15, 2025 (cont'd)

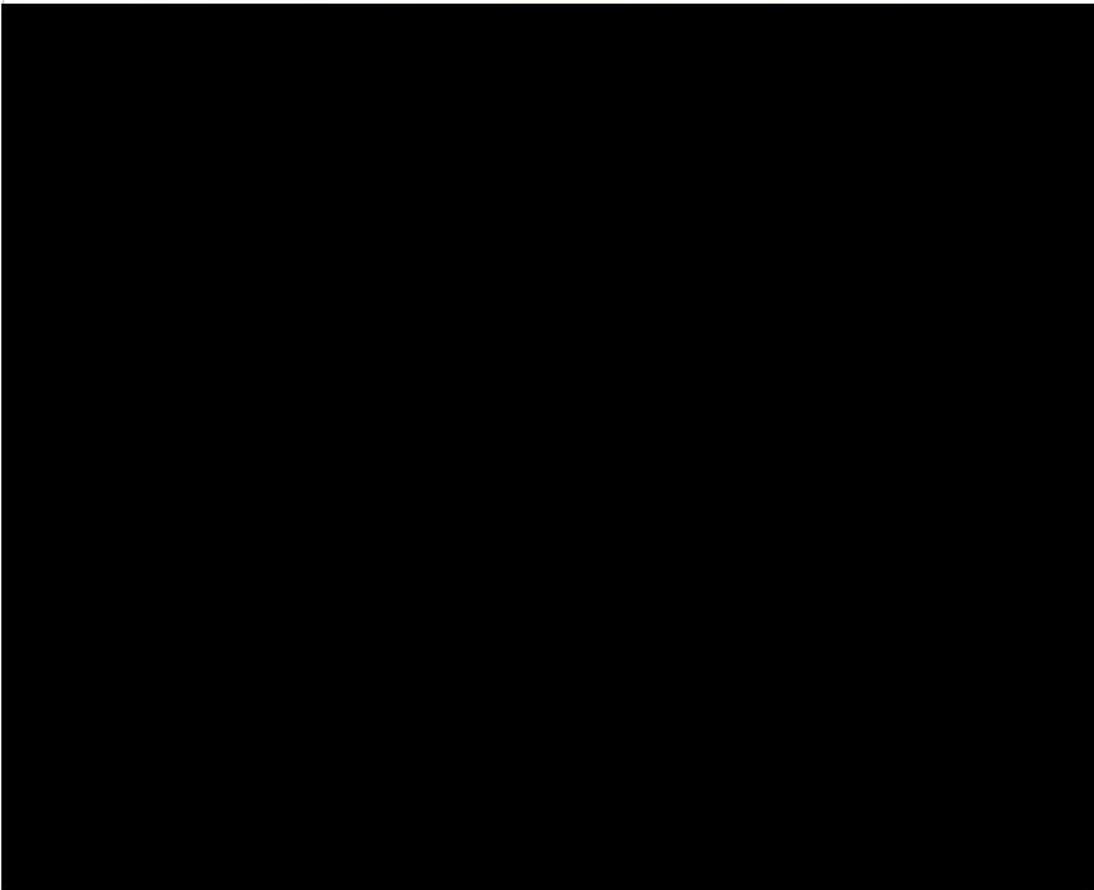
~~(S//NF)~~



~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS at 2111 EDT on March 15, 2025 (cont'd)

~~(S//NF)~~



VR,
Erik

People, Partners, Innovation

GEN Michael E. Kurilla
Commander, U.S. Central Command



~~Classified By:~~ Kurilla, Michael Erik GEN USARMY CENTCOM CCCC (USA)
~~Derived From:~~ USCENTCOM SGC, CCR 380-14, 16 November 2022
~~Declassify On:~~ 2050-03-15
~~Classification:~~ ~~SECRET//NOFORN~~

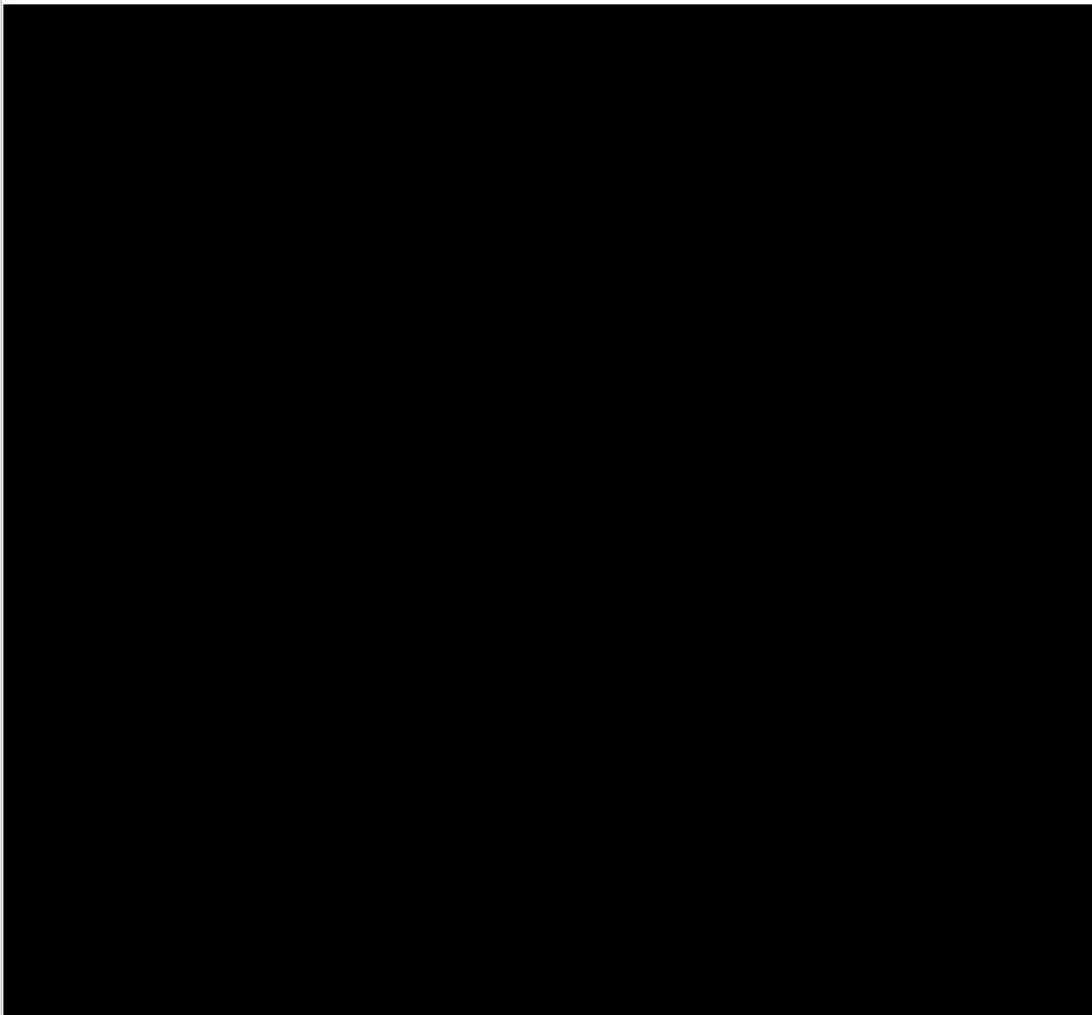
~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS Included in the Secretary's March 15, 2025 Information Packet

~~(S//NF)~~

~~SECRET//NOFORN~~

From: Kurilla, Michael Erik GEN USARMY CENTCOM CCCG (USA) <michael.e.kurilla2.mil@mail.smil.mil>
Sent: Friday, March 14, 2025 8:54 PM
Subject: ~~(S//NF)~~ USCENTCOM OPN ROUGH RIDER C-Houthi Campaign (POD 15/16 MAR)
~~Update~~



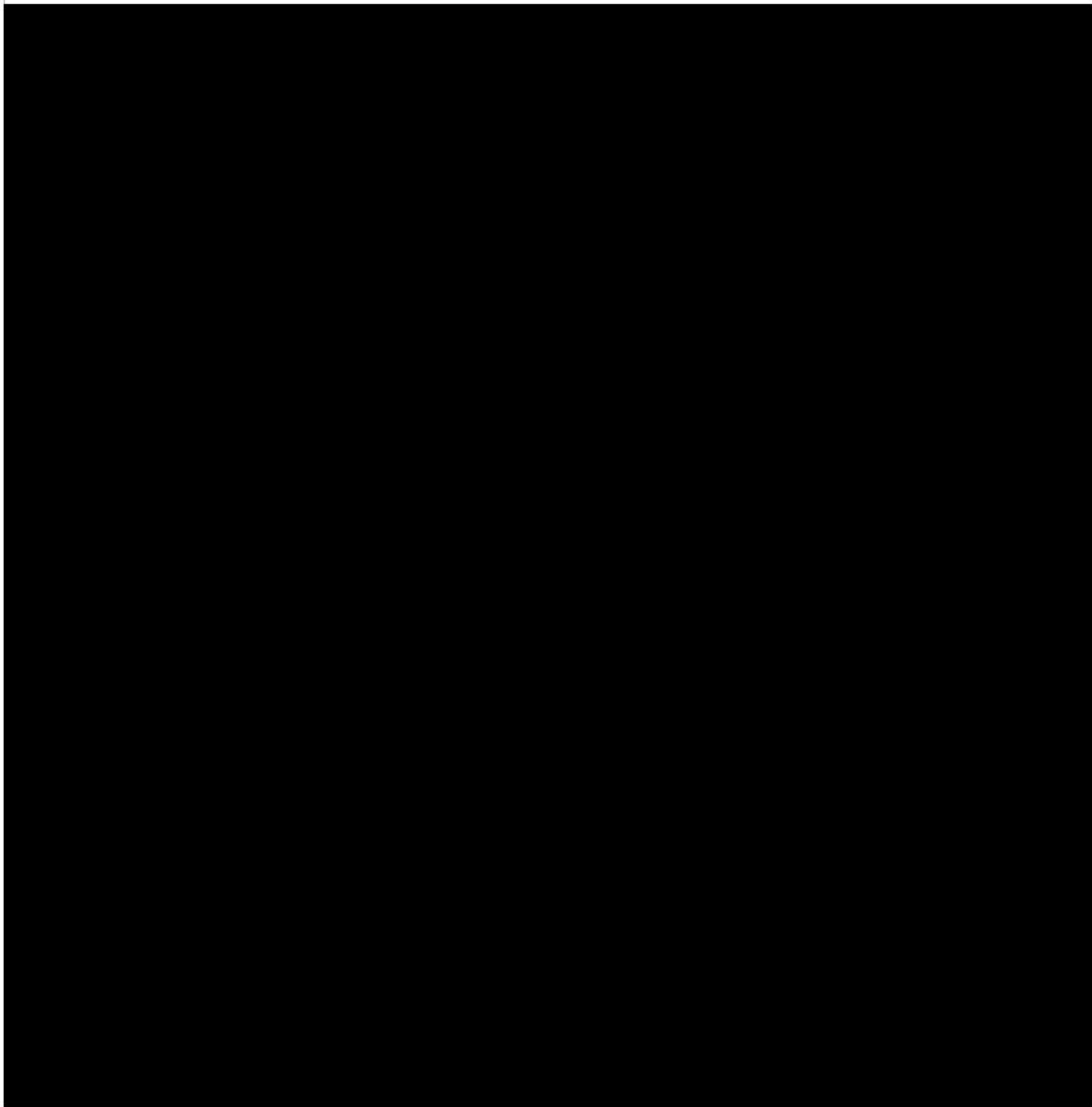
~~SECRET//NOFORN~~

~~(S//NF)~~

(U) USCENTCOM Commander Email to the Secretary of Defense and A-CJCS Included in the Secretary's March 15, 2025 Information Packet (cont'd)

~~(S//NF)~~

~~SECRET//NOFORN~~



VR,
Erik
GEN Michael E. Kurilla
Commander, U.S. Central Command

~~SECRET//NOFORN~~

~~(S//NF)~~

(U) Secretary of Defense Statement to the DoD OIG, Received on July 25, 2025

(U)



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

I am providing the following statement in the context of the ongoing DoD Inspector General Evaluation of the use of Signal (Project No. D2025-DEVOPC-0095.000).

On or about 14 March 2025, I received a detailed briefing from GEN Kurilla on Operation Rough Rider through SIPRNET. This briefing was marked SECRET//NOFORN, but contained no portion markings. My understanding was that a similar detailed brief was sent to the White House and other principals through official communications channels. Pursuant to Executive Order 13526, I am the Original Classification Authority and, in this capacity, I retain the sole discretion to decide whether something should be classified or whether classified materials no longer require protection and can be declassified. On 15 March 2025, at 1144ET, I took non-specific general details which I determined, in my sole discretion, were either not classified, or that I could safely declassify, which I then typed into the Signal chat. In making this determination, I chose to keep the details only to the overt actions of DoD assets, which would be readily apparent to any observer in the area and did not include any details about targets or intelligence which may have been derived from other agencies outside of DoD. The purpose of this was to give the principals in the chat thread a heads up on the timeline, as I knew that they were going to shortly be notifying partner nations and within hours would also be giving media interviews about what we had done.

Again, this was an unclassified summary, whereas the full details were communicated separately on official SIPRNET channels. There was nothing classified in this text. There were no locations or targets identified. There were no details that would endanger our troops or the mission. The details which were included would be useless without also knowing the undisclosed details. There was no additional substantive content that was included in the Signal message that would be different from what was sent through official channels. And the mission was a complete success.

I also understand that your office has expanded your evaluation to look at whether I had unsecured connections installed in my government computer. I do not and never have. It is true that upon taking this job, I asked my comms team whether it was possible to get access to my personal cell phone in my office so I could more easily receive non-official communications during the workday. It is my understanding that Secretary Austin achieved this by violating security protocols and keeping his personal cell phone in the SCIF, which was not how I wanted to operate. The comms team prepared a compliant solution that would allow me this access while also maintaining proper security.

This entire situation has been politicized by the media and those looking to obstruct and derail this administration's progress by creating a false narrative. I am disappointed to see that the media has been reporting on an allegedly leaked information from your evaluation, which falsely claims that the Signal messages included classified information. As outlined above, this allegation is false as a matter of law. I hope that these reports are inaccurate, as it would be incredibly irresponsible for your Office to even make (let alone leak) conclusions about the supposed classification level of the information before obtaining a statement from the original classification authority. If true, it undermines confidence in your conclusions and plays into the same false partisan narrative.

(U)

(U) Appendix E

(U) Senate Committee on Armed Services Chairman and Ranking Member Letter to the Acting Inspector General on March 26, 2025

(U)

ROGER F. WICKER, MISSISSIPPI, CHAIRMAN
 JACK REED, RHODE ISLAND
 DEB FISHBEIN, VERMONT
 TOM COTTUM, ARIZONA
 MIKE ROUNDS, SOUTH DAKOTA
 JOHN H. EMMETT, KANSAS
 DAN SULLIVAN, ALASKA
 KEVIN GRAVES, NORTH DAKOTA
 FRICK SCOTT, FLORIDA
 TOMMY TUBERVILLE, ALABAMA
 HARRINGTON MULLIN, OKLAHOMA
 TED LUGO, NORTH CAROLINA
 DICK SCHWITZ, MISSOURI
 JIM SANDS, INDIANA
 TIM SANDY, MONTANA
 JACK REED, RHODE ISLAND
 JENNIFER SHAHEEN, NEW HAMPSHIRE
 ERIC L. E. SULLIVAN, NEW YORK
 RICHARD BLUMENTHAL, CONNECTICUT
 MAUREN HIRONO, HAWAII
 TIM KAHLE, WYOMING
 ANDREW D. KING, JR., MAINE
 EUGENE M. GARRETT, MASSACHUSETTS
 GARY C. FITZGERALD, MICHIGAN
 TANGY DUC KROTH, ILLINOIS
 JACOB FORD, IDAHO
 MARK KELLY, ARIZONA
 ELISSA SLOTTEN, MICHIGAN
 JOHN P. KEAST, MAJORITY STAFF DIRECTOR
 ELIZABETH L. BIRD, MINORITY STAFF DIRECTOR

United States Senate
 COMMITTEE ON ARMED SERVICES
 WASHINGTON, DC 20510-8050

March 26, 2025

Mr. Steven A. Stebbins
 Acting Inspector General
 U.S. Department of Defense - Office of Inspector General
 4800 Mark Center Drive
 Alexandria, VA 22350-1500

Dear Mr. Stebbins,

On March 11, 2025, Jeffrey Goldberg, the Editor-in-chief of The Atlantic, was reportedly included on a group chat on the commercially available communications application called Signal, which included members of the National Security Council. This chat was alleged to have included classified information pertaining to sensitive military actions in Yemen. If true, this reporting raises questions as to the use of unclassified networks to discuss sensitive and classified information, as well as the sharing of such information with those who do not have proper clearance and need to know.

Accordingly, we ask that you conduct an inquiry into, and provide us with an assessment of, the following:

1. 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. Department of Defense (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. An assessment of DOD classification and declassification policies and processes and whether these policies and processes were adhered to;
4. How the policies of the White House, Department of Defense, the intelligence community, and other Departments and agencies represented on the National Security Council on this subject differ, if at all;
5. An assessment of whether any individuals transferred classified information, including operational details, from classified systems to unclassified systems, and if so, how;
6. Any recommendations to address potential issues identified.

Please include a classified annex to these responses as needed. The Senate Armed Services Committee will work with you to schedule a briefing immediately upon completion of your review.

Sincerely,


 Jack Reed
 Ranking Member


 Roger F. Wicker
 Chairman

(U)

(U) Management Comments

(U) Document Provided by DoD Deputy General Counsel on September 24, 2025, Suggesting Additional Context for the Report Finding

(U) On September 24, 2025, the DoD's Deputy General Counsel for Legislation, Investigations, and Oversight provided the following unsigned statement for consideration in the final report. The Deputy General Counsel's accompanying email stated that the below document captures the entirety of the DoD response to the report.

(U)

(U) In consultation with the Secretary of War's front office, the Office of the General Counsel makes the following statement clarifying and adding context to the substance of the report, on behalf of the Department of War.

(U) On March 14, 2025, the Secretary was added by another member of the National Security Council (NSC) to a Signal chat, which was already set for a 1-week disappearing message cycle. On March 16, 2025, the same NSC member extended the disappearing message cycle to a four-week cycle. Thus, all existing messages within the chat, those sent or received by participants prior to March 16, 2025, remained on a seven-day disappearing message cycle but new messages after the extension were on a 28-day disappearing message cycle. As a result of the Secretary's busy travel schedule to INDOPACOM, meeting with servicemembers, and meeting with foreign leaders both at the Pentagon and abroad, his focus and attention were on matters of national security during the seven-day timeframe following March 14, 2025. When the Secretary was notified that he was required to preserve the records per the Federal Records Act, he timely captured the record that was available to him as a participant in the chat, not the originator. This is evidenced by the exhibit titled "Partial Transcript of the Signal Group Chat Retained by the DoD on March 27, 2025, from the Secretary of Defense's Personal Cell Phone" in Appendix D, which reflects messages beginning on March 16, 2025. DoD's retention of the messages on March 27, 2025, from the Secretary's personal cell phone is within the 20-day window requirement set for records found on non-official electronic messaging accounts.

(U) While the transcript published by the Atlantic contains messages that are not contained in the exhibit titled "Partial Transcript of the Signal Group Chat Retained by the DoD on March 27, 2025, from the Secretary of Defense's Personal Cell Phone", there is also at least one message contained in the Secretary's partial transcript that is not contained in the Atlantic's transcript. This creates some reliability issues with the Atlantic transcript as a point of comparison for what was or was not on the Secretary's phone. In addition, there were also mitigating circumstances outside of his control that may have prevented the capture of the complete record including but not limited to the seven-day disappearing message timer set by another individual and the Secretary's pressing work and travel schedule following the events at issue. As noted above, DoW's retention of the messages on March 27, 2025, from the Secretary's personal cell phone is within the 20-day window requirement set for records found on non-official electronic messaging accounts.

(U)

(U) Chief, U.S. Central Command Special Security Office**(CUI)****CUI**

UNITED STATES CENTRAL COMMAND
7115 SOUTH BOUNDARY BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5101

September 8, 2025

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

SUBJECT: Response to Department of Defense Office of Inspector General (DoDIG) draft report, "Evaluation of the Secretary of Defense's Reported Use of a Commercially Available Messaging Application for Official Business".

Ref(s): (a) Executive Order 13526, *Classified National Security Information*, December 29, 2009
(b) DoD Manual 5200.01, Volume 2, *DoD Information Security Program: Marking of Classified Information*, Incorporating Change 4, July 28, 2012
(c) DoD Manual 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, Incorporating Change 3, July 28, 2020
(d) DoD IG draft report: Project No. D2025-DEV0PC-0095.000, *Evaluation of the Secretary of Defense's Reported Use of a Commercially Available Messaging Application for Official Business*, August 22, 2025

1. United States Central Command (USCENTCOM) concurs with comments regarding the DoDIG findings and recommendations in Reference (d). We appreciate the thorough evaluation, and the recommendations provided to enhance the security and compliance of classified information handling within the DoD and USCENTCOM.

2. In response to Reference (d), the Chief, USCENTCOM Special Security Office (SSO) conducted an in-depth review of the Command's classification procedures. Findings of the in-depth review reveal that USCENTCOM SSO has a well-established comprehensive training program to promote awareness for Command personnel's responsibility to mark classified information as defined by Reference (b). Further, the USCENTCOM SSO Information Security (INFOSEC) Program includes specific training on Section 17b, Figure 16 of Reference (b) as part of the Security Education and Training requirement outlined in Enclosure 5 of Reference (c). This training is integrated into the following USCENTCOM security awareness initiatives:

- (a) USCENTCOM "What About Me" required annual Computer-Based Training.
- (b) Original Classification Authority training (initial and annual).
- (c) USCENTCOM rotating digital training posters throughout facility (Command Close Circuit TV).

Controlled by: CCI-SSO
CUI Category: PRIVCY
Limited Discrimination: FEDCON
Page: [REDACTED]

CUI**(CUI)**

(U) Chief, U.S. Central Command Special Security Office (cont'd)

(CUI)

~~CUI~~

(d) Security Manager (SM)/Representative training (initial and quarterly).

(e) Annual SM inspections, which includes random document sampling for classification compliance (to include e-mails).

3. These practices, along with Command-wide access to security policies via the USCENTCOM SSO Security Portal and Command Policy and Regulations Portal, enable access and awareness to all Command personnel of proper procedures for marking classified information as required by Section 1.6 of Reference (a).

4. Per Reference (d), USCENTCOM's classification procedures are determined to be both appropriate and sufficient based on Paragraph 2 and consistent with References (a) and (b).

5. USCENTCOM SSO recommends coordination between the DoD Chief Information Office and the Office of the Under Secretary of Defense for Intelligence and Security to mandate a standardized DoD-wide Classification Management Tools to enforce the presence of mandatory classification markings, to include paragraph portion markings in e-mails. This recommendation would effectively address the overarching issues leading to this incident and prevent future repeat occurrences across the DoD.

6. The point of contact for this memorandum is USCENTCOM SSO-INFOSEC, which can be reached by phone at: [REDACTED] or via electronic mail at: [REDACTED]

[REDACTED]
Chief, Special Security Office

Attachments:

TAB A: Chief, USCENTCOM SSO in-depth review documents (training where classification marking requirements are highlighted to include in e-mails)

~~CUI~~

(CUI)

(U) List of Classified Sources

(U) The documents listed below are sources used to support information in this report.

Source 1

~~(S//REL TO FVEY) USCENTCOM OPERATION POSEIDON ARCHER FRAGO-016
(14 MAR 2025)
Derived From: Multiple sources
Declassify On: 150048z MAR 25~~

Source 2

~~(S//REL TO FVEY) USCENTCOM ORR v3.0 CAO 15MAR25_1x Slide
Classified By: [REDACTED]
Derived From: Multiple Sources
Declassify On: 20340424~~

Source 3

~~(S//REL TO USA, FVEY) OPN ROUGH RIDER D-Day Deliberate Strikes EXCHECK V3.2
Classified By: KURILLA, MICHAEL ERIK GEN USARMY CENTCOM CCGG USA
Declassify On: 20500314~~

Source 4

~~(S//REL TO USA, FVEY) OPN ROUGH RIDER D-Day+1 OPN Mercury Intruder Deliberate
Strikes EXCHECK V1.1
Classified By: CENTCOM Macdill AFB CENTCOM HQ Mailbox CENTCOM JOC
TEAM CHIEF
Declassify On: 20500315~~

Source 5

~~(S//NOFORN) Email OPN ROUGH RIDER D-Day Deliberate Strikes EXCHECK V3.2
Classified By: KURILLA, MICHAEL ERIK GEN USARMY CENTCOM CCGG USA
Declassify On: 20500314~~

Source 6

~~(S//NOFORN) Email "USCENTCOM OPN ROUGH RIDER C_Houthi Campaign H-1_00
Update _15_1645Z, MAR"
Classified By: KURILLA, MICHAEL ERIK GEN USARMY CENTCOM CCGG USA
Declassify On: 20500315~~

Source 7

~~(S//NOFORN) Email- "USCENTCOM OPN ROUGH RIDER C-Houthi Campaign H-Hour Update (15 1745Z MAR)"~~

~~Classified By: KURILLA, MICHAEL ERIK GEN USARMY CENTCOM CCGG USA~~

~~Declassify On: 20500315~~

Source 8

~~(S//NOFORN) Email- "USCENTCOM OPN ROUGH RIDER C-Houthi Campaign D-Day Final Update (16 0100Z MAR)"~~

~~Classified By: KURILLA, MICHAEL ERIK GEN USARMY CENTCOM CCGG USA~~

~~Declassify On: 20500315~~

Source 9

~~(S//NOFORN) Email- "USCENTCOM Dates CDR Met with SD and POTUS~~

~~Classified By: [REDACTED] CENTCOM CCIG (USA)"~~

~~Declassify On: 20500519~~

Source 10

~~(S//NOFORN) Email- "FW: (S//NF) CENTCOM Counter-Houthi (OPN YUKON BLAZE) Update (10 MAR)"~~

~~Classified By: KURILLA, MICHAEL ERIK GEN USARMY CENTCOM CCGG USA~~

~~Declassify On: 20500310~~

Source 11

~~(S//NOFORN) DODIG-2022-076, "(U) Evaluation of Combatant Commands' Communication Challenges with Foreign Partner Nations During Coronavirus Disease-2019 Pandemic and Mitigation Efforts," March 28, 2022~~

~~Classified By: [REDACTED], PROGRAM MANAGER, OVERSEAS CONTINGENCY OPERATIONS, EVALUATIONS~~

~~Declassify On: 20470328~~

Source 12

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

~~Classified By: [REDACTED] ACTING ASSISTANT INSPECTOR GENERAL FOR PROGRAMS AND COMBATANT COMMANDS~~

~~Declassify On: 20331102~~

Source 13

~~(S) DODIG-2024-109, "(U) Management Advisory: U.S. Air Forces in Europe Handling of Sensitive Information at Logistics Enabling Node-Romania," July 11, 2024~~

~~Classified By: [REDACTED] ASSISTANT INSPECTOR GENERAL FOR PROGRAMS AND COMBATANT COMMANDS~~

~~Declassify On: 20490711~~

Source 14

~~(S) DODIG-2025-006, "(U) 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~~

~~Classified By: [REDACTED] ASSISTANT INSPECTOR GENERAL FOR PROGRAMS AND COMBATANT COMMANDS~~

~~Declassify On: 20341011~~

(U) Acronyms and Abbreviations

A-CJCS	Acting Chairman of the Joint Chiefs of Staff
CUI	Controlled Unclassified Information
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
EDT	Eastern Daylight Time
EO	Executive Order
JMA	Junior Military Assistant
NOFORN	Not Releasable to Foreign Nationals
OCA	Original Classification Authority
OCIO	Office of the Chief Information Officer
OPSEC	Operational Security
OSD	Office of the Secretary of Defense
PC	Personal Communicator
SCG	Security Classification Guide
SCIF	Sensitive Compartmented Information Facility
USCENTCOM	U.S. Central Command
USG	U.S. Government

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