Report No. DODIG-2025-053

INSPECTOR GENERAL

U.S. Department of Defense

December 13, 2024

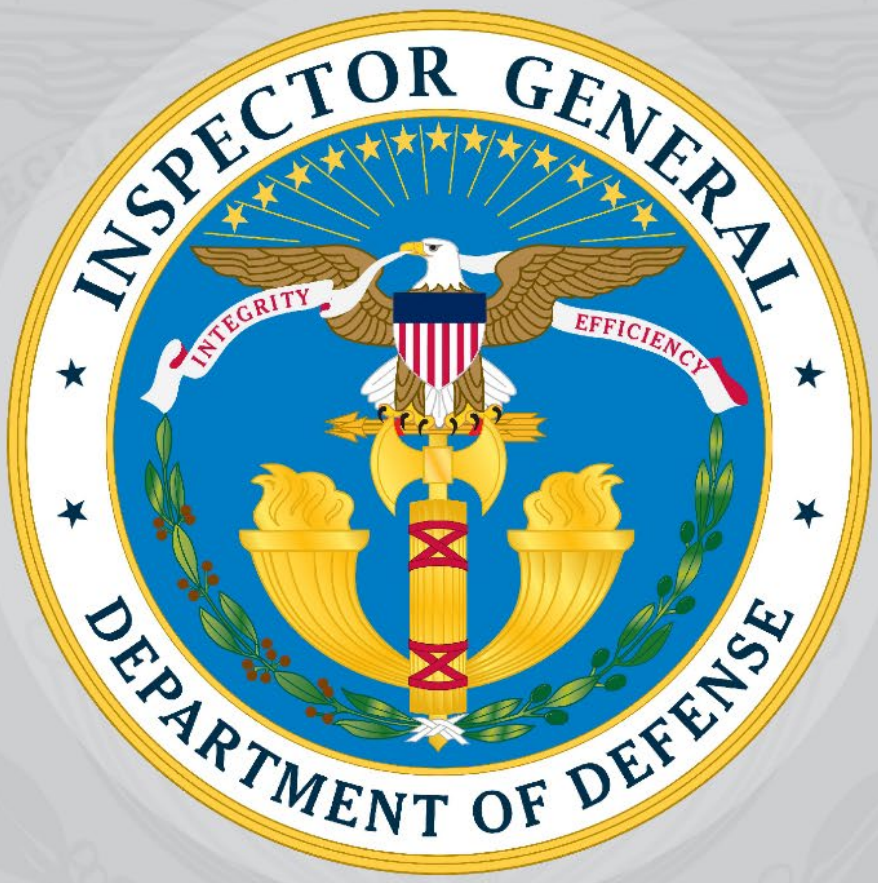
(U) Audit of Cybersecurity of DoD Classified Mobile Devices

~~Classified By:~~ [redacted]
~~Derived From: Multiple Sources~~
~~Declassify On: December 13, 2049~~

~~Controlled By: DoD OIG~~
~~Controlled By: Audit~~
~~CUI Category: ISVI, OPSEC~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC:~~ [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 [cite specific reference, where possible, or state "the applicable classification guide(s)"]. It must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DoDI 5230.09 prior to public release.~~

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★TRANSPARENCY


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

(U) Results in Brief

(U) Audit of Cybersecurity of DoD Classified Mobile Devices

(U) December 13, 2024

(U) Objective

(U) The objective of this audit was to determine whether DoD Components implemented cybersecurity controls to protect classified mobile devices and classified information accessed, transferred, and stored on those devices, in accordance with Federal and DoD guidance. Cybersecurity controls are safeguards and countermeasures designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted on or through systems and networks.

(U) Background

(U) Mobile devices are portable computing devices with communication capabilities, such as smart phones or tablets, designed to wirelessly transmit and receive information. We reviewed the effectiveness of select cybersecurity controls on classified mobile devices at the Defense Information Systems Agency (DISA), the U.S. European Command (USEUCOM), and two subcomponents of the U.S. Special Operations Command (USSOCOM).

(U) Findings

~~(CUI)~~ We determined that [redacted]. Specifically, they did not

- (U) maintain complete or accurate classified mobile device inventory records,
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]

(U) Findings (cont'd)

- ~~(CUI)~~ [redacted]
- (U) include all requirements in their user training programs or user agreements,
- ~~(CUI)~~ [redacted] or
- (U) annually review or approve their incident response plans.

~~(CUI)~~ This occurred because DoD Component authorizing officials, Classified Portable Electronic Device Managers (CPEDMs), and Program Managers were not prepared to effectively manage the increased demand for classified mobile devices caused by the COVID-19 pandemic and the transition to an unprecedented amount of telework beginning in March 2020. In addition, the DoD Component CPEDMs and Program Managers [redacted]

~~(S)~~ [redacted]

(U) Results in Brief

(U) Audit of Cybersecurity of DoD Classified Mobile Devices

(U) Recommendations

(U) We made 40 recommendations to address the findings of this report. Among other recommendations, we recommend that DISA, USEUCOM, and USSOCOM HQ authorizing officials conduct a review of their classified mobile device programs, identify deficient cybersecurity controls, and develop and implement a corrective action plan. We also recommend that the Director of DISA's Joint Enterprise Services Directorate; USEUCOM Chief Information Office Division Chief; and USSOCOM Director for Command, Control, Communications and Computer/Cyber, Chief Information Officer:

- ~~(CUI)~~ Develop and implement [redacted]
- (U) Immediately revalidate and document the user justification for their devices and recall the devices if the user no longer has a valid mission need; revise existing access policies to require detailed written justifications for obtaining classified mobile devices; and establish processes to, at least annually, revalidate the need for continued access to the devices.
- (U) Develop and implement classified mobile device training that includes all 23 Office of the Secretary of Defense technical and administrative requirements.
- ~~(CUI)~~ [redacted].

(U) We also recommend that the DoD Chief Information Officer direct the DoD Component heads to review their classified mobile device programs for the issues identified in this report and take corrective actions as applicable.

(U) Management Comments and Our Response

(U) The Director of DISA's Joint Enterprises Services Directorate agreed with and provided planned actions for eight recommendations; therefore, these recommendations are resolved but open. We will close the recommendations once we verify that the Director has implemented the agreed upon actions. The Director agreed or partially agreed with but did not provide planned actions for the remaining five recommendations; therefore, these recommendations are unresolved, and we request that the Director of DISA's Joint Enterprises Services Directorate provide comments addressing the recommendations, within 30 days, in response to the final report.

(U) Chief, Chief Information Office Division, U.S. European Command agreed with and provided planned actions to address 11 recommendations. Therefore, the recommendations are resolved but open. We will close the recommendations once we verify that the Chief has implemented the agreed upon actions.

(U) Director for Command, Control, Communications and Computer/Cyber, Chief Information Officer, U.S. Special Operations Command, did not respond to the 14 recommendations directed to it in the report; therefore, the recommendations are unresolved. We request that the Director provide comments addressing the recommendations, within 30 days, in response to the final report.

(U) The Chief Information Officer, DoD, agreed with and provided planned actions for two recommendations; therefore, the recommendations are resolved but open. We will close the recommendations once we verify that the DoD Chief Information Officer has implemented the agreed upon actions. Please see the Recommendations Table on the next page for the status of the recommedations.

(U) Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief Information Officer, Department of Defense	None	4, 5	None
Director, Joint Enterprises Services Directorate, Defense Information Systems Agency	3.a, 3.b, 3.e, 3.f, 3.j	3.c, 3.d, 3.g, 3.h, 3.i, 3.k, 3.l, 3.m	None
Director for Command, Control, Communications and Computer/Cyber, Chief Information Officer, U.S. Special Operations Command	2.a, 2.b, 2.c, 2.d, 2.e, 2.f, 2.g, 2.h, 2.i, 2.j, 2.k, 2.l, 2.m, 2.n	None	None
Chief, Chief Information Office Division, U.S. European Command	None	1.a, 1.b, 1.c, 1.d, 1.e, 1.f, 1.g, 1.h, 1.i, 1.j, 1.k	None (U)

(U) Please provide Management Comments by January 15, 2025.

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

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

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

December 13, 2024

(U) MEMORANDUM FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
COMMANDER, U.S. EUROPEAN COMMAND
COMMANDER, U.S. SPECIAL OPERATIONS COMMAND
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

(U) SUBJECT: Audit of Cybersecurity of DoD Classified Mobile Devices (Report No. DODIG-2025-053)

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

(U) This report contains 19 recommendations that are considered unresolved because the Director, Defense Information Systems Agency Joint Enterprises Services Directorate, did not fully address recommendations, and the Director for Command, Control, Communications, and Computer/Cyber, Chief Information Officer, U.S. Special Operations Command, did not provide a response to the report. We will track these recommendations until management has agreed to take actions that we determine to be sufficient to meet the intent of the recommendations and submit adequate documentations showing that all agreed-upon actions are completed.

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

(U) This report also contains 21 recommendations that we consider resolved and open. We will close these recommendations when the Chief Information Officer; Director, Joint Enterprises Services Directorate, Defense Information Systems Agency; and Chief, Chief Information Office Division, U.S. European Command, provides us documentation showing that all agreed-upon actions are completed. Therefore, within 90 days please provide us your response concerning specific actions in process or completed on the recommendations. Send your response to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET.

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

FOR THE INSPECTOR GENERAL:

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

(U) Contents

(U) Introduction 1

(U) Objective 1

(U) Background 1

~~(CUI)~~ Finding. [redacted] 9

~~(CUI)~~ [redacted] 10

(U) DoD Components Were Not Prepared for the Increased Demand for Classified Mobile Devices or Enforcing Policy for Senior Officials 24

~~(CUI)~~ [redacted] 25

(U) Recommendations, Management Comments, and Our Response 26

(U) Appendixes 40

(U) Appendix A. Scope and Methodology 40

(U) Internal Control Assessment and Compliance 44

(U) Use of Computer-Processed Data 44

(U) Use of Technical Assistance 44

(U) Prior Coverage 45

(U) Appendix B. Classified Mobile Devices Training Program Requirements 46

(U) Appendix C. Classified Mobile Device User Agreement Requirements 48

(U) Management Comments 52

(U) DoD Chief Information Officer 52

(U) U.S European Command 53

(U) Defense Information Systems Agency 55

(U) Annex: Sources of Classified Information 58

(U) Acronyms and Abbreviations 59

(U) Glossary 60

(U) Introduction

(U) Objective

(U) The objective of this audit was to determine whether DoD Components implemented cybersecurity controls to protect classified mobile devices and classified information accessed, transferred, and stored on those devices in accordance with Federal and DoD guidance.[1] See Appendix A for discussion of the scope, methodology, and prior audit coverage related to the objective.[2]

(U) We initiated this audit in August 2021; however, the COVID-19 pandemic operationally impacted DoD Components resulting in delays to our requests for classified information. In addition, in December 2021, we suspended the audit while we completed a statutorily required audit. Because of those delays, we requested updated information for some of the controls tested, which the DoD Components provided between June 2023 and May 2024. Although these circumstances extended the time needed to complete this audit, the findings and recommendations in this report remain relevant to current operations.

(U) Background

(U) Mobile devices are portable computing devices with communication capabilities, such as smart phones or tablets, designed to wirelessly transmit and receive information. Some smart phones, tablets, and e-readers are equipped to store information and allow voice communication.

(U) Classified Mobile Devices

(U) The DoD provides select DoD personnel with commercial-off-the-shelf mobile devices configured to securely access classified information. DoD Components must follow National Security Agency (NSA) cybersecurity requirements, organized into "capability packages," to operate classified mobile devices that receive, access, or store information. The NSA's Commercial Solutions for Classified (CSfC) Program Management Office is responsible for developing, approving, and publishing the capability packages. DoD Components must follow the requirements provided in the

[1] (U) Cybersecurity controls are safeguards and countermeasures designed to protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted on or through systems and networks.

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

(U) capability packages when developing hardware, software, mobile applications, network connection services, and other elements of their classified mobile device solution. Once the NSA verifies that a mobile device solution meets all capability package requirements, the NSA approves the solution for use.

(U) The NSA CSfC Program Management Office developed and approved four capability packages for DoD use.[3]

- (U) Mobile Access – Provides a mobile device connection to a classified network through two layers of encryption.[4] This is the only capability package that allows access to classified information outside of secure facilities.

- (U) Multiple Site Connectivity – Provides a connection to two or more networks operating at the same security level through encryption to securely transmit classified data.

- (U) Campus Wireless Local Access Network – Provides network protection that allows devices to securely send and receive classified information using a wireless network within a secure facility.

- (U) Data-at-Rest (DAR) – Provides storage capabilities for classified information.

(U) The Mobile Access capability package allows DoD Components to choose from the following three options for classified mobile devices.

- (U) Thin end-user device (EUD) – "Thin" refers to devices (mobile and desktop) that do not have a storage capability on the device itself. When using these devices, the user accesses classified information that is stored on a server instead of the device. A thin EUD prevents classified information from being stored on a device, which reduces the risk that unauthorized users can access classified information.

- (U) EUD with DAR – Classified mobile devices with DAR have a storage capability and can store classified information. Components using this option must register a separate DAR capability package with the NSA.

[3] (U) DoD Components can customize their CSfC solutions by combining one or more of the NSA CSfC capability packages.

[4] (U) Encryption is the process of changing plain text to an unreadable format for the purpose of security or privacy.

- (U) Classified EUD – Classified mobile devices that can store classified information, but can be used only in physically protected environments. The DoD Component's authorizing official must approve physical security measures implemented to protect classified EUDs before they can be used.[5] Because classified information is stored on the device, the device requires DAR protection.

(U) DoD Components appoint and train a Classified Portable Electronic Device Manager (CPEDM) to manage and sustain their CSfC device programs.[6] The CPEDMs are responsible for configuring, maintaining, provisioning, tracking, and decommissioning the CSfC devices. In addition, the CPEDMs train CSfC device users on how and when to use their device and execute processes required for reporting security incidents.

(U) Federal and DoD Guidance for Protecting Classified Mobile Devices

(U) Federal and DoD guidance defines the requirements for protecting classified mobile devices and the information that resides on those devices. The following guidance focuses on standards and directives related to classified mobile device capability packages, authorizations, and user agreements.

- (U) Committee on National Security Systems Policy (CNSSP) No. 7 requires Federal agencies to ensure that their CSfC solutions comply with NSA requirements to protect national security systems that transmit, receive, process, or store information.[7] CNSSP No. 7 also requires authorizing officials to acknowledge and accept residual risks of operating a CSfC solution registered with the NSA.

- (U) Committee on National Security Systems Directive (CNSSD) No. 504 requires Federal agencies to establish capabilities to prevent, deter, detect, and mitigate the risk of insider threat to their national security systems and

[5] (U) An authorizing official is a senior Federal official or executive with the authority to assume responsibility for operating an information system at an acceptable level of risk to agency operations.

[6] (U) The DoD Components have the following position titles to refer to their CPEDMs: DISA – DoD Mobility Classified Capability – SECRET Program Manager, USEUCOM – CSfC Personal Electronic Device (PED) Manager, and USSOCOM – CPEDM.

[7] (U) CNSSP No. 7, "Policy on the use of Commercial Solutions to Protect National Security Systems," December 9, 2015. The Committee on National Security Systems is a Government interagency committee that issues policies and implementing guidance on information security issues, including secure modes of communication using classified mobile devices.

(U) the national security information that resides on them.[8] CNSSD No. 504 also requires Federal agency heads to implement user activity monitoring as part of their insider threat program with triggers that monitor user activities on a network.[9]

- (U) CNSSD No. 520 requires Federal agencies using CSfC mobility solutions to configure the solution according to NSA-developed capability packages. The Directive also states that users must only use classified mobile devices outside of secure spaces when there is a mission need.[10] CNSSD No. 520 requires users to sign a user agreement that includes:
    - (U) the approved operating environment and any user mitigations required to avoid the monitoring, collection, or interception of national security information;
    - (U) the monitoring requirements that the user must consent to before using the device;
    - (U) a statement that the classification level of the information stored, processed, or transmitted on the device must not exceed the approved classification level of either the device or the user's clearance level;
    - (U) the user's acknowledgement that they have been trained to properly use the classified mobile device and only connect to authorized information systems, accessories, or charging stations;
    - (U) the user's responsibilities to immediately report incidents;
    - (U) the prohibiting of a user to modify, update, or alter the device's software or hardware; and

[8] (U) CNSSD No. 504, "Directive on Protecting National Security Systems from Insider Threat," September 2021. An insider threat is the threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

[9] (U) User activity monitoring is the technical capability to observe and record the actions and activities of all users, at any time, on any device accessing national security information in order to detect insider threats. Triggers are a set of rules applied to a data stream that produce an alert when an anomalous incident or behavior occurs.

[10] (U) CNSSD No. 520, "The Use of Mobile Devices to Process National Security Information Outside of Secure Spaces," November 2021.

- (U) the procedures for the users to return the device for periodic software updates or security patches and end-of-life procedures.

- (U) DoD Instruction 5000.64 requires all accountable property and respective data elements to be tracked in an accountable property system of record, the government system used to control and manage accountable property records.[11]

- (U) DoD Instruction 8500.01 requires the DoD Chief Information Officer (CIO) to develop, establish, and oversee the implementation of DoD cybersecurity policy and guidance.[12] The Instruction also requires that all DoD information systems be categorized in accordance with Committee on National Security Systems Instruction No. 1253, "Categorization and Control Selection for National Security Systems." The Instruction further requires DoD Components to implement a corresponding set of security controls from National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53).[13]

- (U) An Office of the Secretary of Defense (OSD) memorandum on securing and operating classified portable devices requires DoD Components to develop and implement guidance related to classified mobile device user training, user agreements, and device monitoring.[14]

- ~~(CUI)~~ A December 11, 2020 DoD CIO memorandum on commercial solutions for classified programs requires the [redacted] In addition, the memorandum requires the [redacted][15]

[11] (U) DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," April 27, 2017 (Change 3 Effective June 10, 2019).

[12] (U) DoD Instruction 8500.01, "Cybersecurity," October 7, 2019.

[13] (U) NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, April 2013 (Updated January 22, 2015). Withdrawn September 23, 2021.

[14] ~~(CUI)~~ [redacted]

[15] ~~(CUI)~~ [redacted]

- (U) Chairman of the Joint Chiefs of Staff Manual 6510.01B provides DoD guidance for detecting, analyzing, responding, recovering, and reporting cyber incidents.[16]

(U) DoD Components and Cybersecurity Controls Reviewed

~~(CUI)~~ We selected the following DoD Components for review because they were the only Components with active registered [redacted][17]

- (U) Defense Information Systems Agency (DISA)
- (U) U.S. European Command (USEUCOM)
- (U) U.S. Special Operations Command (USSOCOM) Headquarters (HQ)
- (U) USSOCOM Central (SOCCENT)[18]

~~(CUI)~~ Between October 2021 and January 2022, the four DoD Components reported a total of [redacted] as identified in Table 1.[19]

[16] (U) Chairman of the Joint Chiefs of Staff Manual 6510.01B, "Cyber Incident Handling Program," December 2014.

[17] ~~(CUI)~~ We initially included the U.S. Strategic Command in our review; however, during the audit, [redacted] therefore, this report does not include findings and recommendations concerning the U.S. Strategic Command.

[18] (U) USSOCOM's enterprise consists of 12 subcomponents that conduct global special operations and activities within an area of responsibility. Although USSOCOM HQ and SOCCENT are considered subcomponents, for purposes of this report, we refer to them as Components.

[19] ~~(CUI)~~ Our universe included classified mobile devices that process or store data at the SECRET level. As of December 2023, the four DoD Components reported an updated total inventory of [redacted]

(U) Table 1. Number and Type of Classified Mobile Devices for DoD Components Reviewed

~~(CUI)~~ DoD Component	Device Type	Number of Devices (as of January 2022)
DISA	Laptops, phones, and tablets	[redacted]
USEUCOM	Laptops	
USSOCOM HQ	Laptops	
SOCCENT	Laptops	
Total		~~(CUI)~~

(U) Source: The DoD OIG.

(U) We selected a nonstatistical sample of 42 devices from DISA, 21 devices from USEUCOM, 4 devices from USSOCOM HQ, and 5 devices from SOCCENT to review. We requested the classified mobile user agreements for these devices to determine whether the DoD Components retained signed user agreements and verified the classified mobile device's information and the user's mission need. We attempted phone interviews with the users of the sampled devices; however, we were only able to contact 26 DISA, 12 USEUCOM, 1 USSOCOM HQ, and 3 SOCCENT users.

(U) We also requested and reviewed the inventory lists of the classified mobile devices on hand during our site visits to determine whether the four DoD Components were maintaining accurate inventories. DISA did not have classified mobile devices on hand at the facilities we visited, and SOCCENT had issued all its devices to users at the time of our site visit in December 2022. We counted and verified the serial number or unique identifiers for USEUCOM's and USSOCOM HQ's on-hand inventory of classified mobile devices. We also requested and reviewed user activity logs for the four Components to determine whether the Components disabled and deleted the accounts of classified mobile device users in accordance with their own policies. See Appendix A for more information regarding the universe and our sample selection.

(U) To determine whether DoD Components protected classified mobile devices and the data accessed, transferred, and stored on those devices in accordance with Federal and DoD guidance, we focused our review on cybersecurity controls that we determined, if

(U) not in place, could present a higher risk of compromise for mobile devices.[20] Specifically, we reviewed cybersecurity controls regarding inventory, configuration management, user access, training, physical security, continuous monitoring, and incident response.

[20] (U) The NSA Mobile Access capability package, NSA DAR capability package, and NSA Continuous Monitoring Requirements Annex include the cybersecurity requirements that DoD Components must implement when developing hardware, software, mobile applications, network connection services, and other elements of their classified mobile device solution. The NSA requirements align to specific NIST SP 800-53 cybersecurity controls.

(U) Finding

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]. Specifically, they did not:

- (U) maintain complete or accurate classified mobile device inventory records,
- ~~(CUI)~~ [redacted],
- ~~(CUI)~~ [redacted],
- ~~(CUI)~~ [redacted],
- (U) include all 23 OSD technical and administrative requirements in their classified mobile device training,
- (U) include all 11 CNSSD No. 520 and 11 NSA Mobile Access capability package requirements in their classified mobile user agreements,
- ~~(CUI)~~ [redacted], or
- (U) annually review and approve incident response plans.

~~(CUI)~~ This occurred because DoD Component authorizing officials, CPEDMs, and Program Managers were not prepared to effectively manage the increased demand for classified mobile devices caused by the COVID-19 pandemic and the transition to an unprecedented amount of telework beginning in March 2020. In addition, the DoD Component CPEDMs and Program Managers [redacted].

~~(S)~~ [redacted]

~~(S)~~ [redacted].

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]. Specifically, they did not maintain complete or accurate classified mobile device inventories, [redacted] ensure that users were adequately trained and understood their responsibilities, [redacted], or annually review and approve their incident response plans.

(U) DISA, USEUCOM, USSOCOM HQ, and SOCCENT Did Not Maintain Complete or Accurate Classified Mobile Device Inventories

(U) DISA, USEUCOM, USSOCOM HQ, and SOCCENT did not maintain complete or accurate classified mobile device inventory records as required by CNSSD No. 520 and DoD Instruction 5000.64. At a minimum, DoD Components must maintain records identifying the following six elements in an accountable property system of record.

- (U) Name and organization of the user
- (U) Type of device
- (U) Device serial number
- (U) Assigned user phone number
- (U) Classification of data stored or transmitted on the device
- (U) Condition of device use[21]

[21] (U) "Condition of device use" describes how, when, and where the user can operate the device. The user agreement defines the conditions of use and each user must sign an agreement before receiving a classified mobile device.

(U) To determine whether the classified mobile device inventories were complete and accurate, we reviewed DoD Component inventory records to verify that they contained information for all six elements, conducted a physical inventory of the on-hand classified mobile devices that were ready for issuance or had been returned, and selected a nonstatistical sample of users from each Component to verify whether their serial number and type of device matched the inventory records.

(U) DISA, USEUCOM, USSOCOM HQ, and SOCCENT Inventory Records Did Not Contain All Required Elements

(U) DISA, USEUCOM, USSOCOM HQ, and SOCCENT inventory records as of January 2024 did not include information for all six of the elements in an accountable property system of record. Specifically, DISA did not include information for four of the six elements in its inventory records, USEUCOM did not include three of the elements, and USSOCOM HQ and SOCCENT did not include information for two of the elements as indicated in Table 2.

(U) Table 2. Compliance with Federal Inventory Record Elements

(U) DoD Components	Organization and User	Type of Device	Serial Number	Phone Number	Classification of Data	Condition of Use
DISA	No	Yes	No	Yes	No	No
USEUCOM	Yes	Yes	Yes	No	No	No
USSOCOM HQ	Yes	Yes	Yes	No	Yes	No
SOCCENT	Yes	Yes	Yes	No	Yes	No (U)

(U) Source: The DoD OIG.

(U) Maintaining complete inventory records enables DoD Components to locate and account for each classified mobile device. For instance, inventory accountability ensures that assigned devices are properly administered and that organizations can contact property custodians if action is required, such as when the device is involved in a cybersecurity breach or needs to be recalled, replaced, or relocated. Therefore, the Director of DISA's Joint Enterprise Services Directorate; USEUCOM CIO Division Chief; and USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO, should update inventory records for all classified mobile devices to include

(U) information for the six elements in the accountable property system of record as required by CNSSD No. 520 and DoD Instruction 5000.64.[22]

(U) DISA and USSOCOM HQ Inventory Records Contained Inaccurate Information for Some Devices

(U) In addition to the CNSSD No. 520 requirements, DISA and USSOCOM had Component-level guidance concerning classified mobile device inventories. However, DISA and USSOCOM HQ did not consistently comply with the Component-level guidance.

(U) DISA's Standard Operating Procedure for the Defense Mobility Classified Capability requires the DISA Mobility Team to assign new equipment a record number and update the mobility program system of record with the device's serial number, phone number, and subscriber identity module card number.[23] DISA did not have classified mobile devices on hand at the facilities we visited; therefore, to review DISA's inventory records, we interviewed 26 of the 42 classified device users in our sample.[24] Of the 26 users, the serial numbers for three of the devices did not match the inventory records, and two of the devices had been turned in, but the inventory records still listed them as issued. Therefore, the Director of DISA's Joint Enterprise Services Directorate should develop and implement a process to ensure that inventories are conducted periodically and records are updated in a timely manner; immediately reconcile all issued and onsite classified mobile devices; update inventory records; and take appropriate action if they are unable to properly reconcile a classified mobile device.

~~(CUI//NF)~~ USSOCOM's CSfC Implementation Guidance requires USSOCOM subcomponent CPEDMs to actively manage and report all CSfC devices, the device's serial number, and their assigned users to USSOCOM HQ for auditing purposes.[25] However, USSOCOM HQ did not have [redacted]. Moreover, it took USSOCOM HQ officials more than 7 months to compile and provide us an updated list of the classified mobile devices for all of their subcomponents, including USSOCOM HQ and SOCCENT. At the time of our site visit, USSOCOM HQ personnel provided us their inventory records of the devices on-hand at their facility. Therefore, we limited our testing to the on-hand inventory records. USSOCOM HQ's inventory records indicated that

[22] (U) In October 2023, DISA reorganized the agency and renamed the Director of the Joint Enterprise Services Directorate to the Director, Program Executive Office Services due to an agency reorganziation.

[23] (U) Standard Operating Procedure for Defense Mobility Classified Capability Secure Mobility Implementation Team, Version 1.0, December 7, 2020. A subscriber identity module card is a small memory card that contains unique information that identifies it to a specific mobile network.

[24] (U) The interviews took place over the phone and we had the users provide us the device's serial number.

[25] ~~(CUI)~~ [redacted].

~~(CUI//NF)~~ [redacted] classified mobile devices should have been in the on-hand inventory; however, we were able to account for only [redacted] devices ([redacted]). Therefore, the USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO, should update the CSfC Implementation Guidance to define the frequency for conducting inventories and reporting results to USSOCOM HQ; immediately conduct an inventory of all Component classified mobile devices; update their inventory records; and take appropriate action if they are unable to properly reconcile a classified mobile device.

~~(CUI)~~ SOCCENT's inventory records indicated that none of SOCCENT's [redacted] mobile devices were on-site and that all were assigned to users. Based on interviews with one USSOCOM HQ and three SOCCENT sampled device users, we verified that the inventory records matched for those devices, the devices were in the user's possession, or users turned in the device, and the inventory records were updated accordingly.

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]. To determine whether the users were periodically connecting their devices to the network, we requested user account data from the four DoD Components, reviewed the users' login data, and calculated the elapsed time between the last login and the day of our review.

~~(S)~~ We were unable to determine whether DISA classified mobile device users complied with the connection requirements because, according to DISA's Network Operations administrator, [redacted].[26] Between January 2020 and December 2021, DISA issued eight versions of the classified mobile device user agreement that require [redacted]. The most recent version, dated July 2024, requires [redacted]. Therefore, the Director of DISA's Joint Enterprise Services Directorate

[26] (U) A directory service stores information about objects on a network, such as information about user accounts, and makes the information available to network users and administrators.

~~(S)~~ should [redacted].

~~(S)~~ We were also unable to determine whether USEUCOM classified mobile device users complied with the connection requirements in USEUCOM's CSfC program guide. [redacted].[27] [redacted]. Therefore, the USEUCOM CIO Division Chief should take immediate action to develop and implement [redacted].

~~(CUI//NF)~~ USSOCOM's Enterprise CSfC Implementation Guidance requires users, including USSOCOM HQ and SOCCENT users, [redacted]. USSOCOM used an automated process to track mobile device connection data. The user login data that USSOCOM HQ personnel provided indicated that [redacted].[28] Therefore, the USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO, should take immediate action to [redacted].

~~(S)~~ [redacted]. Effective configuration settings and regular software updates reduce the threat posed by vulnerabilities. [redacted].

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

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

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]. CNSSD No. 504 requires DoD Components to integrate user activity monitoring into their insider threat program with triggers that monitor and record the actions and activities of all users, at any time, on any device on the network to detect insider threats and support authorized investigations. In addition, the NSA CSfC Continuous Monitoring Annex requires a multilayered approach to continuously monitoring the CSfC devices to validate the operational status and monitor network behavior or systems for malicious activity or policy violations using an intrusion detection system.[29] Failure to continuously monitor the network and the activity on the devices may result in observable network behavior that significantly deviates from the established baselines. To determine whether the DoD Components continuously monitored the activity of classified mobile device users, we reviewed the Component's system security plan, observed the DoD Components officials' activities to monitor the networks that devices accessed, and interviewed the Component's mobility division personnel.

~~(CUI)~~ DISA's Mobility Chief Engineer stated that DISA's [redacted]. However, officials from the [redacted].

~~(S//NF)~~ [redacted].[30]

~~(CUI)~~ According to the NSA Mobile Access capability package, continuously monitoring network traffic and system log data allows DoD Components to detect, react to, and report any attacks against the classified mobile devices.[31] [redacted]. Therefore, the Director of DISA's Joint

[29] (U) "NSA Central Security Service CSfC Continuous Monitoring Annex," Version 1.0, August 4, 2021. An intrusion detection system is a device or software application that monitors a network or system for malicious activity or policy violations and generates a notification when that activity happens.

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

[31] (U) "NSA Central Security Service CSfC Mobile Access Capability Package," Version 2.5.1, February 18, 2022.

~~(CUI)~~ Enterprise Services Directorate; USEUCOM's CIO Division Chief; and USSOCOM's Director for Command, Control, Communications and Computer/Cyber, CIO, should develop and implement [redacted].

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]. CNSSD No. 504 requires Federal agencies to develop and implement standardized access control methodologies in accordance with NIST SP 800-53, including procedures to create, enable, modify, disable, and remove user accounts to ensure that authorized users only access information needed to complete assigned responsibilities.

(U) To determine whether DoD Components developed and implemented access control procedures, we reviewed the Components' access control policies, interviewed access management administrators, reviewed a nonstatistical sample of user agreements, and analyzed user termination records.

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]. CNSSD No. 520 requires only documented and authorized users with a mission need to have access to classified mobile devices. Although Component guidance required that user mission need be verified before a classified mobile device could be issued, the Components issued devices without documentation supporting the need for access, or the documentation did not sufficiently describe the need for access.

(U) DISA could not provide documentation to justify the user's need for access for any of the 26 users we interviewed from our sample. DISA officials stated that the user agreement files were corrupted. We also determined that documentation for 8 (38.1 percent) of the 21 USEUCOM users we sampled provided vague justifications, such as an organization name or "COVID-19." In another example, USSOCOM documentation for all eight users sampled—three USSOCOM HQ and five SOCCENT—did not include written justification for access. SOCCENT officials stated that they issued classified mobile devices only after SOCCENT's Chief of Staff approved the mission need through email. However, we requested, and SOCCENT did not provide, the emails.

(U) Classified mobile devices have inherent risk due to the nature of their intended use outside of secure facilities. Despite policies to limit risk and establish user need for access, documentation did not consistently support the need for users to have classified mobile devices. The Public Health Emergency for COVID-19 expired on May 11, 2023; therefore, it is imperative that DoD Components reevaluate mission needs for classified mobile devices outside of secure spaces and recall devices no longer used or needed. Therefore, the Director of DISA's Joint Enterprise Services Directorate; USEUCOM CIO Division Chief; and the USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO should immediately revalidate and document the user justification for the devices and recall the device if the user no longer has a valid mission need, revise existing access policies to require detailed written justifications for obtaining classified mobile devices, and establish processes to periodically, at least annually, revalidate the need for continued access to the devices.

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]. We could not determine whether DISA and USEUCOM disabled or removed inactive user accounts in accordance with guidance because [redacted]. CNSSD No. 504 requires Federal agencies to develop and implement standardized access control methodologies in accordance with NIST SP 800-53 security controls, including establishing procedures for removing user accounts. In accordance with CNSSD No. 504, the Components had their own internal account management guidance for disabling and removing inactive user accounts.

(U) To determine whether the Components disabled and removed user accounts in accordance with their guidance, we obtained user login data, reviewed the Components' access control policies and procedures, and compared the user login dates to the timelines defined in the guidance.

~~(CUI)~~ We were unable to determine whether DISA officials disabled and removed inactive accounts because, [redacted]. In addition, the DISA systems administrator stated that [redacted]. Therefore, the Director of DISA's Joint

~~(CUI)~~ Enterprise Services Directorate should [redacted]. In addition, the Director of DISA's Joint Enterprise Services Directorate should [redacted].

~~(S)~~ We were also unable to determine whether USEUCOM officials complied with account management requirements to disable and remove inactive accounts. USEUCOM's access control policy requires the USEUCOM Helpdesk to [redacted]. In October 2022, USEUCOM officials manually tracked classified mobile device user logins. In June 2024, USEUCOM officials stated that they used software to automatically disable and disconnect user accounts; however, this software did not differentiate between desktop and classified mobile device Secret Internet Protocol Router Network user accounts. Therefore, the USEUCOM CIO Division Chief should take immediate action to [redacted]. In addition, the USEUCOM CIO Division Chief should implement processes to ensure that the [redacted].

~~(CUI//NF)~~ USSOCOM's access control policy requires [redacted]. However, USSOCOM HQ [redacted]. Of the login data as of December 2022 for the [redacted] USSOCOM HQ classified mobile devices, we found that [redacted].

~~(CUI//NF)~~ Of the [redacted] SOCCENT classified mobile devices, as of February 2024, we found that [redacted].[32] SOCCENT officials stated that [redacted]. Therefore, the USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO, should [redacted]. In addition, the USSOCOM Director for Command, Control,

[32] ~~(CUI//NF)~~ [redacted].

~~(CUI//NF)~~ Communications and Computer/Cyber, CIO should [redacted].

(U) DISA, USEUCOM, USSOCOM HQ, and SOCCENT Classified Mobile Device Training Did Not Include All Requirements

(U) DISA, USEUCOM, USSOCOM HQ, and SOCCENT classified mobile device training did not include all 23 OSD technical and administrative requirements. The OSD memorandum requires DoD Components to develop and provide users with comprehensive training that includes, at a minimum, 23 technical and administrative requirements.[33] For example, technical requirements include how to check the device for tampering, wipe the device, and operate classified email; and administrative requirements include learning when not to send or receive classified emails.

(U) To determine whether DoD Components included all 23 OSD requirements in their training programs, we reviewed their training programs and interviewed training managers. Table 3 provides an overview of the DoD Components' compliance with the OSD memorandum requirements. See Appendix B for a list of the 23 training requirements and DoD Component compliance with each requirement.

(U) Table 3. DoD Components' Compliance with OSD Training Requirements

~~(CUI)~~ DoD Component	Technical Requirements		Administrative Requirements	
	Number Included	Number Not Included	Number Included	Number Not Included
DISA (laptops)	[redacted]			
DISA (phones and tablets)				
USEUCOM				
USSOCOM				~~(CUI)~~

(U) Source: The DoD OIG.

(U) Inadequate training increases the risk that users will not properly use or protect classified mobile devices and information. Therefore, the Director of DISA's Joint Enterprise Services Directorate, USEUCOM CIO Division Chief, and USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO, should revise

[33] (U) OSD memorandum, "Security and Operational Guidance for Classified Portable Electronic Devices," September 25, 2015.

(U) existing or develop new classified mobile device training programs that include information on all 23 OSD memorandum requirements. In addition, the Director of DISA's Joint Enterprise Services Directorate; USEUCOM CIO Division Chief; and USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO, should provide all existing classified mobile device users with the updated training that includes all 23 OSD memorandum requirements.

(U) DISA, USEUCOM, USSOCOM HQ, and SOCCENT User Agreements Did Not Include All Requirements

(U) DISA, USEUCOM, USSOCOM HQ, and SOCCENT's user agreements did not include all CNSSD No. 520 and NSA requirements. CNSSD No. 520 requires that users sign a user agreement before receiving and using a classified mobile device. The user agreement must contain 11 requirements, to include a statement notifying the user that they are forbidden from altering software or hardware and that they must maintain constant physical control of the device. The NSA CSfC Mobile Access capability package requires that the user agreements contain an additional 11 requirements to include a justification for access. See Appendix C for a list of the 11 CNSSD No. 520 user agreement requirements and 11 NSA Mobile Access capability package requirements with DoD Component compliance status for each requirement.

(U) Between January 2020 and December 2021, DISA issued eight versions of its user agreement for classified mobile devices. None of the agreements met CNSSD No. 520 requirements, and six of the eight did not meet NSA requirements. However, in July 2024, DISA developed a user agreement that met all the requirements. New and active users are required to sign the updated user agreements only when they bring their devices in for updates. Additionally, DISA officials stated that the updated user agreement was available on DISA's website, but they did not require all users to review and acknowledge the updated user agreement. Therefore, we recommend that the Director of DISA's Joint Enterprise Services Directorate establish a mechanism to track the status of all classified mobile device user agreements and ensure that all users have acknowledged the most recent version of the user agreement.

(U) Although USEUCOM's user agreement included all NSA requirements, it did not include a requirement to complete periodic user training as required by CNSSD No. 520. Periodic training reminds users of how to properly safeguard and handle the classified mobile device entrusted to them. Therefore, the USEUCOM CIO Division Chief should update the classified mobile device user agreement to include all CNSSD No. 520 requirements and ensure that all users have acknowledged the updated user agreement.

~~(CUI)~~ USSOCOM's user agreement did not include 3 of the 11 CNSSD No. 520 requirements and 4 of the 11 NSA requirements. During the audit, in June 2022,

~~(CUI)~~ USSOCOM issued a draft user agreement; however, the draft agreement still did not include a requirement to complete periodic user training as required by CNSSD No. 520. In addition, the draft user agreement did not include requirements to [redacted]. Therefore, the USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO, should update the classified mobile device user agreement to include all CNSSD No. 520 and NSA requirements and ensure that all users have acknowledged the updated user agreement.

(U) In addition, DISA, USSOCOM HQ, and SOCCENT did not retain copies of signed user agreements for 48 (85.7 percent) of the 56 users we sampled. Completed and signed user agreements provide the DoD a written record of a user's acknowledgement of their security responsibilities for using and securing classified mobile devices. Without maintaining completed and signed agreements for each classified mobile device user, DoD Components have no written assurance that the users are aware of their responsibilities for using and securing classified mobile devices. Therefore, the Director of DISA's Joint Enterprise Services Directorate and USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO should develop and implement procedures for retaining signed classified mobile device user agreements.

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]. CNSSD No. 520 requires users to maintain control of the device when turned on and off. CNSSD No. 520 also requires Component heads to ensure that users receive annual training that includes physical security. The OSD memorandum requires users to protect their classified mobile device [redacted]. To determine whether users properly secured their devices when not in use, we reviewed DoD Components' training programs and user agreements, interviewed classified mobile device users, and interviewed DoD Components' physical security personnel.

~~(CUI)~~ Of the 26 DISA classified mobile device users we interviewed, [redacted].[34] DISA officials stated that DISA users were responsible for reading user guides and signing the user agreement, which [redacted]

[34] (U) We interviewed 26 of the 42 DISA sampled users.

~~(CUI)~~ [redacted].

~~(CUI)~~ Of the 12 USEUCOM classified mobile device users we interviewed, [redacted].[35] USEUCOM classified mobile device users received training when they were issued devices and signed a user agreement that [redacted].

~~(CUI)~~ Of the four USSOCOM HQ and SOCCENT classified mobile device users we interviewed, [redacted].[36] However, USSOCOM HQ and SOCCENT users received training when they were issued devices and signed a user agreement that requires [redacted]. The USSOCOM HQ user we interviewed [redacted].

~~(CUI)~~ [redacted]. Without regular and effective training programs that specifically define physical security requirements and [redacted]. Therefore, the Director of DISA's Joint Enterprise Services Directorate; USEUCOM CIO Division Chief; and USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO should develop and implement procedures to verify that their classified mobile device users [redacted] as required by CNSSD No. 520. The Director of DISA's Joint Enterprise Services Directorate; USEUCOM CIO Division Chief; and USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO should also [redacted].

(U) DISA, USEUCOM, USSOCOM HQ and SOCCENT Did Not Annually Approve Their Incident Response Plans

(U) DISA, USEUCOM, USSOCOM HQ, and SOCCENT incident response plans were not annually reviewed or approved. Chairman of the Joint Chiefs of Staff Manual 6510.01B

[35] (U) We interviewed 12 of the 21 USEUCOM sampled users.

[36] (U) We interviewed 1 of the 4 USSOCOM HQ and 3 of the 10 SOCCENT sampled users.

(U) requires an incident response plan to provide procedures for detecting, analyzing, responding to, recovering from, and reporting incidents.[37] Additionally, CNSSI No. 1253 requires organizations to implement the incident response plan controls from NIST SP 800-53, which requires Federal agencies to review incident response plans, at least annually, to incorporate lessons learned from past incidents and establish roles and responsibilities for those implementing the plan.

~~(S)~~ USEUCOM did not have an approved incident response plan at the time of our review. Instead, USEUCOM used the draft version of [redacted] from November 2022 and the [redacted] as its interim guidance. [redacted]. On January 29, 2024, USEUCOM officials approved [redacted].[38]

~~(CUI)~~ DISA's Incident Response Plan Artifact for DoD Mobility Classified Capability – Secret Version 1.4, was not annually reviewed or approved.[39] Specifically, DISA officials explained that because of the [redacted]. However, on December 8, 2022, during the audit, DISA officials updated and approved their new incident response plan.[40]

~~(CUI)~~ USSOCOM did not review or approve its incident response plan since September 1, 2016. USSOCOM used the Defensive Cyber Center Incident Response Plan, [redacted], [redacted] and the NSA's [redacted] to provide guidance to their personnel on how to respond to a cyber incident.[41] Therefore, the USSOCOM Director for Command, Control, Communications and Computer/Cyber, CIO, should implement a cyber incident response plan and controls to ensure that the plan is reviewed and approved annually.

[37] (U) Chairman of the Joint Chiefs of Staff Manual 6510.01B, "Cyber Incident Handling Program," July 10, 2012. The incident-handling life cycle is the detection of events, preliminary analysis and identification of incidents, preliminary response actions, incident analysis, response and recovery, and post-incident analysis as.

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

[39] (U) "Incident Response Plan Artifact for DMCC-S," Version 1.4, June 2021.

[40] ~~(CUI)~~ [redacted].

[41] ~~(CUI)~~ "USSOCOM Defense Cyber Center Incident Response Plan," September 2016; [redacted]; and [redacted].

(U) DoD Components Were Not Prepared for the Increased Demand for Classified Mobile Devices or Enforcing Policy for Senior Officials

~~(CUI)~~ Cybersecurity controls to protect classified mobile devices were inconsistently implemented because the DoD Components' authorizing officials, CPEDMs, and Program Managers were not prepared to effectively manage the increased demand for classified mobile devices caused by COVID-19 and the transition to an unprecedented amount of telework beginning in March 2020. In addition, the DoD Component CPEDMs and Program Managers wrongfully assumed that they [redacted].

~~(CUI)~~ DoD Components officials stated that the increase in demand for classified mobile devices resulting from the COVID-10 pandemic negatively affected their ability to effectively manage and maintain accountability of their Components' classified mobile devices. For example, USEUCOM officials explained that COVID-19 caused USEUCOM to expedite the distribution of the classified mobile devices and the development of its classified mobile device training program. Similarly, DISA and USEUCOM officials stated that they did not finalize or approve their incident response plan in a timely manner due to COVID-19, personnel turnover, and various urgent mission needs that took priority. Although we made recommendations to DISA, USEUCOM, USSOCOM HQ, and SOCCENT to correct the deficiencies identified in this report, other DoD Components that issue classified mobile devices may have similar deficiencies. Therefore, the DoD CIO should direct the DoD Component heads to review their classified mobile device programs for the issues identified in this report, take corrective actions as applicable, and report the results of their review and any corrective actions taken to the DoD CIO. At a minimum, DoD Component heads should ensure their classified mobile device programs,

- (U) maintain complete and accurate classified mobile device inventory records,
- ~~(CUI)~~ [redacted],
- ~~(CUI)~~ [redacted],
- ~~(CUI)~~ [redacted],
- (U) include all requirements in their classified mobile device training,
- (U) include all requirements in their classified mobile device user agreements,

- ~~(CUI)~~ [redacted], and
- (U) annually review and approve incident response plans.

~~(CUI)~~ The DoD Component CPEDMs and Program Managers also stated that they felt like [redacted]. This included the authority to enforce requirements to [redacted]. Additionally, CPEDMs and Program Managers were often discouraged by their leadership from [redacted]. [redacted] Additionally, USEUCOM's Computer and Information Technology Services Operations Lead stated that [redacted]. Similarly, SOCCENT's CPEDM stated that the SOCCENT Helpdesk [redacted]. Therefore, the DoD CIO should immediately issue a memorandum affirming that DoD policies [redacted] and supporting classified mobile device program managers to enforce their policies against [redacted].

~~(CUI)~~ [redacted]

~~(S)~~ [redacted].

~~(S)~~ Moreover, from January 2022 to January 2024, the number of classified mobile devices issued by some of the DoD Components we reviewed significantly increased. [redacted]

~~(S)~~ [redacted].[42] [redacted]
[redacted].

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the U.S. European Command Chief Information Office Division Chief:

a. (U) Update inventory records for all classified mobile devices to include information for the six elements required in an accountable property system of record.

(U) U.S. European Command Comments

(U) The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM will update the inventory for all classified mobile devices to include information for the six elements required in an accountable property system of record by March 31, 2025.

(U) Our Response

(U) Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM provides documentation verifying that the inventory was updated to include the six elements required in an accountable property system of record.

b. ~~(CUI)~~ Take immediate action to develop and implement [redacted]

(U) U.S. European Command Comments

~~(CUI)~~ The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM has taken immediate action [redacted]. The Division

[42] (U) As of January 2024, USEUCOM and SOCCENT reduced their number of issued classified mobile devices.

~~(CUI)~~ Chief also stated that the appropriate officials would be notified of non-compliant users, and that users who [redacted] will have to return the classified mobile device.

(U) Our Response

(U) Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM provides documentation verifying that the automated process has been implemented.

c. ~~(CUI)~~ Develop and implement [redacted].

(U) U.S. European Command Comments

~~(CUI)~~ The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM will develop and implement [redacted].

(U) Our Response

~~(CUI)~~ Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM provides documentation verifying that it implemented an [redacted].

d. (U) Immediately revalidate and document the user justification for the devices and recall the device if the user no longer has a valid mission need, revise existing access policies to require detailed written justifications for obtaining classified mobile devices, and establish processes to periodically, at least annually, revalidate the need for continued access to the devices.

(U) U.S. European Command Comments

(U) The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM has taken immediate action to revalidate and document the user's justification for the devices and recall the devices of users who no longer have a valid mission need. The Division Chief stated that USEUCOM has revised existing access policies to require detailed written justification for obtaining classified mobile devices, and will establish processes to periodically, at least annually, revalidate users' need for access to the devices.

(U) Our Response

(U) Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM provides documentation verifying that it revalidated and documented the justification of all its classified mobile device users, revised access policies, and implemented a the process to revalidate the need for continued access to the devices.

e. ~~(CUI)~~ Take immediate action to [redacted].

(U) U.S. European Command Comments

~~(CUI)~~ The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM has [redacted].

(U) Our Response

(U) Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM provides documentation verifying that it [redacted].

f. ~~(CUI)~~ [redacted].

(U) U.S. European Command Comments

~~(CUI)~~ The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM will [redacted].

(U) Our Response

~~(CUI)~~ Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM provides documentation [redacted] in accordance with USEUCOM policy.

g. (U) Revise existing or develop new classified mobile device training programs that include information on all 23 Office of the Secretary of Defense memorandum requirements.

(U) U.S. European Command Comments

(U) The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM will revise its existing classified mobile device training programs to include information on all 23 OSD Memorandum requirements by March 31, 2025.

(U) Our Response

(U) Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM provides documentation verifying that the revised classified mobile device training includes all 23 OSD Memorandum requirements.

h. (U) Provide all existing classified mobile device users with the updated training that includes all 23 Office of the Secretary of Defense memorandum requirements.

(U) U.S. European Command Comments

(U) The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM will provide all existing classified mobile device users with the revised training that includes all 23 OSD Memorandum requirements by March 31, 2025.

(U) Our Response

(U) Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM provides documentation verifying that all its classified mobile device users completed the revised training.

i. (U) Update the classified mobile device user agreement to include all Committee on National Security Systems Directive No. 520 requirements and ensure that all users have acknowledged the updated user agreement.

(U) U.S. European Command Comments

(U) The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM will update its classified mobile device user agreement to include all CNSSD No. 520 requirements. The Division Chief stated that all users will acknowledge the updated user agreement by March 31, 2025.

(U) Our Response

(U) Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM provides the updated classified mobile device user agreement and documentation verifying that all its classified mobile device users acknowledged receipt of the updated user agreement.

j. ~~(CUI)~~ Develop and implement procedures to verify that their classified mobile device users [redacted] as required by Committee on National Security Systems Directives No. 520.

(U) U.S. European Command Comments

~~(CUI)~~ The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM [redacted] by March 31, 2025.

(U) Our Response

~~(CUI)~~ Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM provides documentation of the procedures it implemented [redacted].

k. ~~(CUI)~~ [redacted]

(U) U.S. European Command Comments

~~(CUI)~~ The USEUCOM Chief Information Office Division Chief neither agreed nor disagreed, stating that USEUCOM [redacted] by March 31, 2025.

(U) Our Response

~~(CUI)~~ Comments from the Division Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once USEUCOM [redacted]

~~(CUI)~~ [redacted].

(U) Recommendation 2

(U) We recommend that the U.S. Special Operations Command Director for Command, Control, Communications and Computer/Cyber, Chief Information Officer:

a. **(U) Update inventory records for all classified mobile devices to include information for the six elements required in an accountable property system of record as required by CNSSD No. 520 and DoD Instruction 5000.64.**

b. **(U) Update the Commercial Solution for Classified Implementation Guidance to define the frequency for conducting inventories and reporting results to U.S. Special Operations Command Headquarters; immediately conduct an inventory of all Component classified mobile devices; update their inventory records; and take appropriate action if you are unable to properly reconcile a classified mobile device.**

c. **~~(CUI)~~ Take immediate action to** [redacted].

d. **~~(CUI)~~ Develop and implement** [redacted].

e. **(U) Immediately revalidate and document the user justification for the devices and recall the device if the user no longer has a valid mission need, and revise existing access policies to require detailed written justifications for obtaining classified mobile devices, and establish processes to periodically, at least annually, revalidate the need for continued access to the devices.**

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

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

~~(CUI)~~ [redacted]

h. **(U) Revise existing or develop new classified mobile device training programs that include information on all 23 Office of the Secretary of Defense memorandum requirements.**

i. **(U) Provide all existing classified mobile device users with the updated training that includes all 23 Office of the Secretary of Defense memorandum requirements.**

j. **(U) Update the classified mobile device user agreement to include all Committee on National Security Systems Directive No. 520 and National Security Agency requirements and ensure that all users have acknowledged the updated user agreement.**

k. **(U) Develop and implement procedures for retaining signed classified mobile device user agreements.**

l. ~~(CUI)~~ **Develop and implement procedures to verify that their classified mobile device users** [redacted] **as required by Committee on National Security Systems Directive No. 520.**

m. ~~(CUI)~~ [redacted].

n. **(U) Implement a cyber incident response plan and controls to ensure that the plan is reviewed and approved annually.**

(U) Management Comments Required

(U) The Director for Command, Control, Communications and Computer/Cyber, Chief Information Officer, Special Operations Command did not respond to the recommendations in the report. Therefore, the recommendations are unresolved. We request that the Director provide comments within 30 days of the final report that include actions to address the recommendation.

(U) Recommendation 3

(U) We recommend that the Director of the Defense Information Systems Agency's Joint Enterprise Services Directorate:

a. **(U) Update inventory records for all classified mobile devices to include information for the six elements required in an accountable property system of record.**

b. (U) Develop and implement a process to ensure inventories are conducted periodically and records are updated in a timely manner; immediately reconcile all issued and on-site classified mobile devices; update inventory records; and take appropriate action if you are unable to properly reconcile a classified mobile device.

(U) Defense Information Systems Agency Comments

(U) The Director, Program Executive Office, Services, partially agreed, stating that as a service provider, DISA does not maintain the inventory records for classified mobile devices that are owned and operated by mission partners.[43] The Director stated that it is standard for a mission partner to maintain its inventory records, including key data elements mandated by governing regulations.

(U) Our Response

(U) Comments from the Director did not address the specifics of the recommendations; therefore, the recommendations are unresolved. We acknowledge that DISA is not responsible for maintaining inventory records for classified mobile devices owned and operated by the DoD Components that subscribe to DISA's classified mobile capability services. However, DISA is responsible for maintaining inventory records for classified mobile devices owned and operated by DISA. The inventory records we reviewed included classified mobile devices issued to DISA personnel. We request that the Director provide comments within 30 days of the final report that include actions to address the recommendation.

c. ~~(CUI)~~ [redacted].

(U) Defense Information Systems Agency Comments

~~(CUI)~~ The Director, Program Executive Office, Services, agreed, stating that DISA manually compiles a monthly report to determine [redacted] and any actions to be taken. The Director stated that DISA will identify an automated solution and devise a plan for compliance. DISA expects to identify an automated solution and devise a plan for compliance by June 30, 2025.

(U) Our Response

~~(CUI)~~ Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once DISA provides documentation verifying that it implemented an

[43] (U) In October 2023, DISA renamed the Director of DISA's Joint Enterprise Services Directorate to the Director, Program Executive Office Services due to an agency reorganziation.

~~(CUI)~~ automated solution and the solution [redacted].

d. ~~(CUI)~~ Develop and implement [redacted].

(U) Defense Information Systems Agency Comments

(U) The Director, Program Executive Office, Services, agreed, stating that DISA is exploring technical solutions to automate [redacted] for all classified mobile devices. DISA expects to identify an automated solution and devise a plan for compliance by June 30, 2025.

(U) Our Response

~~(CUI)~~ Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once DISA provides documentation verifying that [redacted].

e. (U) Immediately revalidate and document the user justification for the devices and recall the device if the user no longer has a valid mission need, revise existing access policies to require detailed written justifications for obtaining classified mobile devices, and establish processes to periodically, at least annually, revalidate the need for continued access to the devices.

(U) Defense Information Systems Agency Comments

(U) The Director, Program Executive Office, Services, agreed, stating that DISA will investigate an automated solution as part of the device ordering process to capture validated need and annual revalidation. DISA expects to devise a plan for compliance by June 30, 2025.

(U) Our Response

(U) Comments from the Director partially addressed the recommendation; therefore, the recommendation is unresolved. DISA's proposed actions only address documenting the user justification once the user first requests a classified mobile device and annually thereafter. The Director's comments do not address our recommendation that DISA immediately revalidate and document the justification of existing classified mobile device users, recall any devices if the user no longer has a mission need, and revise existing access policies to require detailed written justifications for obtaining classified mobile devices. We request that the Director provide comments within 30 days of the final report that include actions to address the recommendation.

f. ~~(CUI)~~ [redacted].

(U) Defense Information Systems Agency Comments

~~(CUI)~~ The Director, Program Executive Office, Services, agreed, stating that DISA [redacted].

(U) Our Response

~~(CUI)~~ Comments from the Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. We acknowledge that DISA [redacted]. However, the Director's comments did not address our finding [redacted]. We request that the Director provide comments regarding [redacted] within 30 days of the final report that include actions to address the recommendation.

g. ~~(CUI)~~ [redacted]

(U) Defense Information Systems Agency Comments

~~(CUI)~~ The Director, Program Executive Office, Services, agreed, stating that DISA currently has [redacted].

(U) Our Response

~~(CUI)~~ Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once DISA provides documentation verifying that it has implemented [redacted].

h. (U) Revise existing or develop new classified mobile device training programs that include information on all 23 Office of the Secretary of Defense memorandum requirements.

(U) Defense Information Systems Agency Comments

(U) The Director, Program Executive Office, Services, agreed, stating that DISA is updating the training documentation to include the 23 requirements. The Director expects the updated training to be in place by June 30, 2025.

(U) Our Response

(U) Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once DISA provides documentation verifying that the revised classified mobile device training includes all 23 OSD Memorandum requirements.

i. (U) Provide all existing classified mobile device users with the updated training that includes all 23 Office of the Secretary of Defense memorandum requirements.

(U) Defense Information Systems Agency Comments

(U) The Director, Program Executive Office, Services, agreed, stating that once their updated training is in place, DISA will make it available to all existing classified mobile device users. The Director expects to have the updated training in place by September 30, 2025.

(U) Our Response

(U) Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once DISA provides documentation verifying that all of its classified mobile device users completed the revised training.

j. (U) Establish a mechanism to track the status of all classified mobile device user agreements and ensure that all users have acknowledged the most recent version of the user agreement.

(U) Defense Information Systems Agency Comments

(U) The Director, Program Executive Office, Services, agreed, stating that DISA will identify an automated solution as part of the device ordering process to track signed user agreements. The Director expects to develop a plan for compliance by June 30, 2025.

(U) Our Response

(U) Comments from the Director partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. DISA's proposed actions only address tracking the status of classified mobile device user agreements but not having users acknowledge the most recent version of the user agreement. We

(U) request that the Director provide comments within 30 days of the final report that include actions to address the recommendation.

k. (U) Develop and implement procedures for retaining signed classified mobile device user agreements.

(U) Defense Information Systems Agency Comments

(U) The Director, Program Executive Office, Services, agreed, stating that DISA will identify an automated solution as part of the device ordering process to retain signed user agreements. The Director expects to develop a plan for compliance by June 30, 2025.

(U) Our Response

(U) Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once DISA provides documentation verifying that an automated solution to retain signed classified mobile device user agreements has been implemented.

l. ~~(CUI)~~ Develop and implement procedures to verify that their classified mobile device users [redacted] as required by Committee on National Security Systems Directive No. 520.

(U) Defense Information Systems Agency Comments

(U) The Director, Program Executive Office, Services, agreed, stating that DISA will identify an automated solution as part of the device ordering process to track annual training status. The Director expects to develop a plan for compliance by June 30, 2025.

(U) Our Response

~~(CUI)~~ Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once DISA provides documentation of the procedures it implemented [redacted].

m. ~~(CUI)~~ [redacted]

(U) Defense Information Systems Agency Comments

~~(CUI)~~ The Director, Program Executive Office, Services, agreed, stating that DISA will establish [redacted].

~~(CUI)~~ The Director also stated that [redacted]. The Director expects to develop a plan for compliance by June 30, 2025.

(U) Our Response

~~(CUI)~~ Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once DISA provides documentation verifying that it implemented a process [redacted].

(U) Recommendation 4

(U) We recommend that the DoD Chief Information Officer direct the DoD Component heads to review their classified mobile device programs for the issues identified in this report, take corrective actions as applicable, and report the results of their review and any corrective actions taken to the DoD Chief Information Officer. At a minimum, DoD Component heads should ensure that their classified mobile device programs,

- **a. (U) maintain complete and accurate inventory records,**
- **b. ~~(CUI)~~ [redacted],**
- **c. ~~(CUI)~~ [redacted],**
- **d. ~~(CUI)~~ [redacted],**
- **e. (U) include all requirements in their classified mobile device training,**
- **f. (U) include all requirements in their classified mobile device user agreements,**
- **g. ~~(CUI)~~ [redacted], and**
- **h. (U) annually review and approve incident response plans.**

(U) Acting DoD Chief Information Officer Comments

~~(CUI)~~ [redacted].

(U) Our Response

(U) Comments from the Acting DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the DoD CIO provides the issued guidance that includes all

(U) elements of the recommendation and documentation verifying that the DoD CIO is tracking the status of the DoD Components' reviews and corrective actions taken with respect to their classified mobile device programs.

(U) Recommendation 5

~~(CUI)~~ We recommend that the DoD Chief Information Officer immediately issue a memorandum affirming that DoD policies are [redacted] and supporting classified mobile device program managers to enforce their policies against [redacted].

(U) Acting DoD Chief Information Officer Comments

~~(CUI)~~ [redacted].

(U) Our Response

(U) Comments from the Acting DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the DoD CIO provides the issued guidance that includes all elements of the recommendation.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from August 2021 to September 2024, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We concluded that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

(U) Although we initiated this audit in 2021, the COVID-19 pandemic operationally impacted the DoD Components, resulting in delays to our requests for classified information. In addition, we suspended the audit from December 2021 to May 2022 while we completed a statutorily required audit and from December 2022 to January 2023 due to limited staffing availability. Because of those delays, we requested updated information for some of the controls tested, which the DoD Components provided between June 2023 and June 2024. Although these circumstances extended the time needed to complete this audit, the findings and recommendations in this report remain relevant to current operations.

(U) We selected and reviewed the implementation of security controls from the following security control families.

- (U) Configuration Management
- (U) Access Control
- (U) Awareness and Training
- (U) Physical and Environmental Protection
- (U) Continuous Monitoring
- (U) Incident Response

~~(CUI)~~ We also interviewed officials at the Office of the DoD CIO and at the NSA to determine their roles and responsibilities for implementing and protecting classified mobile devices. In addition, we interviewed officials at DISA, USEUCOM, USSOCOM, and the U.S. Strategic Command (USSTRATCOM) responsible for monitoring their classified mobile device programs; managing assets, user agreements, and training; and responding to cybersecurity incidents to determine how they protect classified mobile devices and the data accessed, transferred, and stored on them. However, [redacted]

~~(CUI)~~ [redacted]. Therefore, this report does not include findings related to USSTRATCOM. We conducted site visits to the following locations.

- (U) DISA Headquarters at Fort Meade, Maryland, and the Columbus–Network Assurance Mobility Operations Facility in Columbus, Ohio
- (U) USEUCOM at U.S. Army Garrison Stuttgart-Patch Barracks in Stuttgart, Germany
- (U) USSOCOM Headquarters at MacDill Air Force Base, Tampa, Florida
- (U) SOCCENT at MacDill Air Force Base, Tampa, Florida

(U) In addition, we reviewed the DoD Components' policies related to training, user agreements, access management, user account management, incident response, continuous monitoring, device configurations, and inventory management to determine whether they developed and implemented cybersecurity controls to protect classified mobile devices and the information stored on them, in accordance with Federal and DoD guidance.

(U) This report was reviewed by the DoD Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. In preparing and marking this report, we considered any comments submitted by the DoD Components about the CUI treatment of their information. If the DoD Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

(U) Audit Universe and Sample Selection

~~(CUI)~~ The scope of the audit included classified mobile devices that were active from January 2020 to December 2021. We focused on Mobile Access with DAR capability packages because these capability packages allow users to access, transmit, and store classified information outside of a secure facility. We nonstatistically selected DISA, USEUCOM, USSOCOM, and USSTRATCOM for review because they were the only Components [redacted].

~~(CUI)~~ In November 2023, [redacted]. Therefore, this report does not include findings related to USSTRATCOM-owned devices.

(U) User Agreement and Interview Sample Selection

(U) We requested a sample of classified mobile device user agreements from the four DoD Components to determine whether the Components retained signed user agreements and verified the classified mobile device information and the user mission need. We also attempted to interview classified mobile device users from the four DoD Components to determine whether the user was still in possession of the classified mobile device and their awareness of cybersecurity requirements.

~~(CUI)~~ For DISA and USEUCOM, we received assistance from the DoD OIG Quantitative Methods Division to select a nonstatistical sample of classified mobile users and their devices from the Component's inventories, as of January 2022. We selected a sample of 42 of [redacted] users from DISA and 21 of [redacted] users from USEUCOM to verify user agreements and conduct user interviews. DISA was unable to provide us with any of the 42 user agreements due to corrupt data files and personnel turnover. However, we were able to interview 26 of the 42 DISA users. We received 21 USEUCOM user agreements and were able to interview 12 USEUCOM users.

~~(CUI)~~ During our site visit to USSOCOM HQ, officials provided a list of [redacted] classified mobile devices in their on-hand inventory. We selected every [redacted] device for testing, for a total of 15 devices. We selected a nonstatistical sample of 4 of the 15 USSOCOM HQ devices. We also requested user agreements for the four USSOCOM HQ devices, but USSOCOM HQ provided only three of the four agreements. We attempted to interview the three users for whom we received user agreements, but we were able to interview only one.

~~(CUI)~~ SOCCENT officials provided a list of [redacted] classified mobile devices with user information during our site visit in December 2022. We selected a nonstatistical sample of 10 of [redacted] devices from the list and requested the corresponding user agreements while onsite. SOCCENT officials produced 5 of the 10 requested user agreements. We requested interviews with the five users for whom we received user agreements, but we were able to interview only three of them.

(U) Onsite Inventory Sample Selection

(U) During our site visits to the four DoD Components we reviewed, two Components (USEUCOM and USSOCOM HQ) provided an inventory of classified mobile devices on hand. DISA did not have classified mobile devices on hand at the facilities we visited and SOCCENT issued all their devices to users at the time of our site visit in December 2022.

~~(CUI)~~ During our site visit in October 2022, USEUCOM officials provided a list of [redacted] devices that had been returned or ready for issuance stored in an office and [redacted] unconfigured devices stored in the warehouse. USEUCOM officials located [redacted] of the

~~(CUI)~~ [redacted] devices stored in the office because a USEUCOM official inaccurately input the serial number for a device into the inventory system, resulting in a duplicate entry. We determined that the correct serial number associated with that device was assigned to a device in the inventory. We also identified all [redacted] of the unconfigured devices on hand in the warehouse.

~~(CUI)~~ USSOCOM HQ officials provided a list of [redacted] classified mobile devices on hand during our December 2022 site visit. USSOCOM HQ officials had 10 hand receipts for classified mobile devices that were issued but not updated in the inventory system, revising the expected number on-hand devices to [redacted]. In addition, USSOCOM HQ officials reviewed their property management systems and identified that they had issued four additional devices, but they had not updated their inventory records accordingly. This further revised the expected number of on-site devices from [redacted] to [redacted]. We then selected a nonstatistical sample of 15 from the list of [redacted] devices and requested that USSOCOM HQ officials locate the device and provide the corresponding inventory record. USSOCOM HQ officials located 11 of the 15 devices with matching inventory records. USSOCOM HQ officials stated that four of the missing devices had been issued to users.

(U) Universe of Disabled User Accounts

~~(S)~~ We requested lists of user login data from the four DoD Components. However, the information DISA and USEUCOM provided was unreliable for determining whether they disabled or removed inactive user accounts in accordance with guidance because [redacted], or did not differentiate between desktop and mobile device Secret Internet Protocol Router Network accounts.

~~(CUI//NF)~~ USSOCOM HQ provided login data as of December 2022 for [redacted]. We reviewed the data for all [redacted] to determine whether USSOCOM HQ disabled and removed inactive users in accordance with their access control policy.

~~(CUI//NF)~~ SOCCENT provided a login data as of February 2024 for [redacted].[44] We reviewed the data for all [redacted] to determine whether SOCCENT disabled and deleted inactive user accounts in accordance with the required timeframe established in the USSOCOM HQ access control policy.

[44] ~~(CUI//NF)~~ [redacted].

(U) Internal Control Assessment and Compliance

(U) We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed the controls for classified mobile devices related to the:

- (U) control environment,
- (U) risk assessment,
- (U) control activities,
- (U) information and communication, and
- (U) monitoring.

(U) However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

(U) Use of Computer-Processed Data

(U) We obtained inventory Excel spreadsheets from four DoD Components to determine the universe classified mobile devices and select a nonstatistical sample of users of classified mobile devices. We performed random inventory checks to determine whether the DoD Components' inventory records were accurate. In addition, we interviewed asset management officials to discuss inventory records and requested supporting documentation. We used the differences as the basis for our findings, conclusions, and recommendations. We determined that the data were sufficiently reliable for the purpose of this audit.

(U) In addition, we obtained classified mobile device configuration settings to determine whether the DoD Component established and documented its classified mobile device configuration settings. We also obtained user account authentication spreadsheets to determine whether DoD Components developed and implemented access control procedures. We used the data as the basis for our findings, conclusions, and recommendations. We determined that the data were sufficiently reliable for the purpose of this audit.

(U) Use of Technical Assistance

(U) The DoD OIG Quantitative Methods Division helped us develop the nonstatistical sampling methodology that we used to select the users of the classified mobile devices from the four DoD Components reviewed.

(U) Prior Coverage

(U) No prior coverage has been conducted on the security and use of classified mobile devices during the last 5 years.

(U) Appendix B

(U) Classified Mobile Devices Training Program Requirements

(U) The OSD memorandum requires DoD Components to develop training specific to using and protecting classified mobile devices that includes 23 technical and administrative requirements.[45] Table 4 identifies the 23 requirements and whether DISA, USEUCOM, and USSOCOM Components complied with them.

(U) Table 4. DoD Components' Compliance with Classified Electronic Device Training Requirements

~~(CUI)~~ OSD Training Requirements	DISA WINDAR	DISA NGD	USEUCOM M-CLASS	USSOCOM CSfC
Technical Training Requirements				
1. Device storage	[redacted]			
2. Physical security of the device verification				
3. Evidence of tampering checks				
4. Device authentication				
5. Device wiping				
6. Keyboard and function keys operational				
7. Classified email operation				
8. Classified video/voice capabilities operation				
9. Personal organizer functions operation				
10. How to change domain, user, and multi-layer encryption passwords				
11. Airplane mode use				
12. Use of camera to take geo-tagged photos				~~(CUI)~~

[45] ~~(CUI)~~ [redacted].

(U) Table 4. DoD Components' Compliance with Classified Electronic Device Training Requirements (cont'd)

~~(CUI)~~ OSD Training Requirements	DISA WINDAR	DISA NGD	USEUCOM M-CLASS	USSOCOM CSfC
13. Voice and video recorders usage	[redacted]			
14. Email signing and encrypting				
15. Procedures for operating in a security conscious manner				
16. Procedures for physically securing the device				
17. Procedures for reporting a lost or stolen device				
18. Discussion of requirement to not install/remove applications without approval				
19. Email auto signature configuration				
20. Security incidents and reporting requirements				
21. General security information and information handling procedures				
22. Required processes described in Component or local site concept of operations				
23. Proper password storage and use				~~(CUI)~~

(U) Legend

(U) CCM Commander's Classified Mobility
(U) CSfC Commercial Solutions for Classified
(U) DISA Defense Information System Agency
(U) OSD Office of the Secretary of Defense
(U) NGD Next-Generation Device
(U) USEUCOM U.S. European Command
(U) USSOCOM U.S. Special Operations Command
(U) WINDAR Windows Data-at-Rest

(U) Source: The DoD OIG.

(U) Appendix C

(U) Classified Mobile Device User Agreement Requirements

(U) CNSSD No. 520 requires DoD Components to develop user agreements that include 11 requirements defining the rules of use for the device. Table 5 identifies the 11 user agreement requirements and whether DISA, USEUCOM, and USSOCOM Components complied with them.

(U) *Table 5. DoD Components' Compliance with Federal User Agreement Requirements*

~~(CUI)~~ CNSSD No. 520 Requirements	DISA 1	DISA 2	DISA 3	DISA 4	DISA 5*	DISA 6	DISA 7	DISA 8	USEUCOM	USSOCOM
1. Approved working environment	[redacted]									
2. Responsibility to adhere to Operations Security when using device										
3. Consent to monitoring										
4. Classification level of information stored, processed, or transmitted cannot exceed user's classification level										
5. User has been trained and will only connect to authorized accessories										~~(CUI)~~

(U) Table 5. DoD Components' Compliance with Federal User Agreement Requirements (cont'd)

~~(CUI)~~ CNSSD No. 520 Requirements	DISA 1	DISA 2	DISA 3	DISA 4	DISA 5*	DISA 6	DISA 7	DISA 8	USEUCOM	USSOCOM
6. User's responsibility to maintain physical control of device and store properly	[redacted]									
7. Responsibility to report incidents										
8. Forbidding to alter device software or hardware										
9. Procedures for bringing device into secure spaces										
10. Procedures for returning device for updates and end of life procedures										
11. Requirements for periodic user training										~~(CUI)~~

* (U) DISA updated user agreements based on changes to the capability package, user needs, and response to cybersecurity incidents. During the audit, DISA developed eight different user agreements for WINDAR and NGD—DMCC-S WINDAR-Secret user agreement Version 1.0 (DISA 1); DMCC-S WINDAR user agreement Version 2.3 (DISA 2); DMCC-S NGD user agreement Version 1.0 (DISA 3); DMCC-S NGD and WINDAR Secret user agreement Version 1.0 (DISA 4); and DMCC-S Windows 10 Surface Book Pilot user agreement Version 1.0 (DISA 5).

(U) Source: The DoD OIG.

(U) The NSA Mobile Access capability package requires DoD Components to develop user agreements that include 11 additional requirements defining the rules of use for the device. Table 6 identifies the 11 NSA user agreement requirements and whether DISA, USEUCOM, and USSOCOM complied with them.

(U) *Table 6. Compliance with NSA User Agreement Requirements*

~~(CUI)~~ NSA Requirements	DISA 1	DISA 2	DISA 3	DISA 4	DISA 5	DISA 6	DISA 7	DISA 8	USEUCOM	USSOCOM
1. Consent to monitoring	[redacted]									
2. Operations Security Guidance										
3. Physical protections when operating and storing device										
4. When, where, and under what conditions the device may be used										
5. Responsibility to report incidents										
6. Verification of Information Assurance training										
7. Verification of appropriate clearance										
8. Justification for access										
9. Requestor information and organization										~~(CUI)~~

(U) *Table 6. Compliance with NSA User Agreement Requirements (cont'd)*

~~(CUI)~~ NSA Requirements	DISA 1	DISA 2	DISA 3	DISA 4	DISA 5	DISA 6	DISA 7	DISA 8	USEUCOM	USSOCOM
10. Account expiration date	[redacted]									
11. User Responsibilities										~~(CUI)~~

(U) Source: The DoD OIG.

(U) Management Comments

(U) DoD Chief Information Officer Comments

~~CONTROLLED UNCLASSIFIED INFORMATION~~

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

CHIEF INFORMATION OFFICER

OCT 23 2024

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General "Audit of Cybersecurity of DoD Classified Mobile Devices" Draft Report (D2021-D000CU-0131.000).

(U) This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Draft Report, "Audit of Cybersecurity of DoD Classified Mobile Devices" Report (D2021-D000CU-0131.000)."

~~(CUI)~~ DoD IG RECOMMENDATION: The Department of Defense Chief Information Officer (DoD CIO) will direct the DoD Component heads to review their classified mobile device programs for the issues identified in this report, take corrective actions as applicable, and report the results of their review and any corrective actions taken to the DoD Chief Information Officer.

~~(CUI)~~ DoD CIO RESPONSE: DoD CIO agrees with the DoD IG recommendation. [redacted]

~~(CUI)~~ DoD IG RECOMMENDATION: The DoD Chief Information Officer immediately issue a memorandum affirming that DoD policies are [redacted] and supporting classified mobile device program managers enforce their policies against [redacted]

~~(CUI)~~ DoD CIO RESPONSE: [redacted]

(U) The point of contact for this matter is [redacted]

Leslie A. Beavers
Acting

~~Controlled by: DoD CIO~~
~~Controlled by: Audit~~
~~CUI Category: ISVI, OPSEC~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC: Audit Program Director, Cyberspace Operations~~ [redacted]

~~CONTROLLED UNCLASSIFIED INFORMATION~~

(U) U.S European Command Comments

~~CUI~~

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400
APO AE 09131

ECJ6 24 October 2024

MEMORANDUM FOR RECORD

SUBJECT: (U) Audit of Cybersecurity of DoD Classified Mobile Devices, Project No. D2021-D000CU-0131.000, HQ EUCOM Acknowledgement

1. ~~(CUI)~~ In August 2021 the DoD Office of Inspector General (DOD OIG) initiated an audit of HQ EUCOMs [redacted]. The objective of the audit was to determine whether DoD Components implemented cybersecurity controls to protect classified mobile devices and classified information accessed, transferred, and stored on those devices in accordance with Federal and DoD guidance.

2. (U) The DOD OIG inspection team sampled twenty-one (21) of HQ EUCOMs Data at Rest (DAR) classified laptops and identified eleven (11) recommendations aimed at improving the compliance posture of US EUCOM's CSfC program.

3. (U) USEUCOM acknowledges the recommendations issued in the Inspector General, US. Department of Defense Project No. D2021-D000CU-0131.000 Report "(U) Audit of Cybersecurity of DoD Classified Mobile Devices" dated September 30, 2024. USEUCOM has taken the following actions below, that will address the recommendations.

4. ~~(CUI)~~ The POC for this action is [redacted]

MYERS.KAY.AN N.[redacted] Digitally signed by MYERS.KAY.ANN[redacted] Date: 2024.10.24 16:35:24 +02'00'

KAY A. MYERS
Authorizing Official (AO)
HQ EUCOM C4/Cyber Directorate

Enclosure:
a. US EUCOM CSfC DoD IG Audit Findings

~~Controlled by: USEUCOM~~
~~Controlled by: ECJ65/Cybersecurity~~
~~CUI Category: Basic~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC:~~ [redacted]

~~CUI~~

Page 1 of 2

(U) U.S European Command Comments (cont'd)

US EUCOM CSfC DoD IG Audit Recommendations

RECOMMENDATIONS	EUCOMs MITIGATION /FIX ACTION
(U) Update inventory records for all classified mobile devices to include information for the six elements required in an accountable property system of record.	(U) USEUCOM will update the Inventory for all classified mobile devices to include information for the six elements required in an accountable property system of record. Completion projected for Q1 CY2025.
~~(CUI)~~ [redacted]	~~(CUI)~~ [redacted]
~~(CUI)~~ [redacted]	~~(CUI)~~ [redacted]
(U) Immediately revalidate and document the user justification for the devices and recall the device if the user no longer has a valid mission need, revise existing access policies to require detailed written justifications for obtaining classified mobile devices, and establish processes to periodically, at least annually, revalidate the need for continued access to the devices.	(U) USEUCOM CSfC team has taken immediate action to revalidate, documented the user justification for the devices, and recalled the device if the user no longer has a valid mission need. The team has also revised existing access policies to require detailed written justifications for obtaining classified mobile devices, and will establish processes to periodically, at least annually, revalidate the need for continued access to the devices.
(U) [redacted]	(U) USEUCOM J63 HQ IT team has [redacted]
~~(CUI)~~ [redacted]	~~(CUI)~~ [redacted]
(U) Provide all existing classified mobile device users with the updated training that includes all 23 Office of the Secretary of Defense Memorandum requirements.	(U) US EUCOM will provide all existing classified mobile users with the updated training that includes all 23 Office of the Secretary of Defense Memorandum requirements. Completion projected for Q1 CY2025.
(U) Revise existing or develop new classified mobile device training programs that include information on all 23 Office of the Secretary of Defense Memorandum requirements.	(U) USEUCOM has begun revising existing classified mobile device training programs that include information on all 23 Office of the Secretary of Defense Memorandum requirements. Completion projected for Q1 CY2025.
(U) Update the classified mobile device user agreement to include all Committee on National Security Systems Directive No. 520 requirements and ensure that all users have acknowledged the updated user agreements.	(U) USEUCOM has begun updating the classified mobile device user agreement to include all Committee on National Security Systems Directive No. 520 requirements and ensure that all users have acknowledged the updated user agreements. Completion projected for Q1 CY2025.
~~(CUI)~~ [redacted]	~~(CUI)~~ [redacted]
~~(CUI)~~ [redacted]	~~(CUI)~~ [redacted]

* *Highlighted cells indicate CUI classification*

~~Controlled by: USEUCOM~~
~~Controlled by: ECJ65/Cybersecurity~~
~~CUI Category: Basic~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC:~~ [redacted]

(U) Defense Information Systems Agency Comments

~~CUI~~

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

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

SUBJECT: (U) Response to DoD IG Draft Audit of Cybersecurity of DoD Classified Mobile Devices, Project No. D2021-D000CU-0131.000

Reference: (U) U.S. Department of Defense Inspector General's draft, "Audit of Cybersecurity of DoD Classified Mobile Devices," Project No. D2021-D000CU-0131.000, September 30, 2024

(U) The Defense Information Systems Agency (DISA) has reviewed the referenced draft audit and is providing responses to the recommendations. Thank you for your diligence in performing the audit and the important recommendations therein. DISA partially concurs with the report and below are the actions directed in response to your recommendations.

(U) Recommendation 3.A: (U) We recommend that the Director of the Defense Information Systems Agency's Joint Enterprise Services Directorate: Update inventory records for all classified mobile devices to include information for the six elements required in an accountable property system of record.

(U) DISA partially concurs with this recommendation. As a service provider, DISA does not maintain the inventory records for all classified mobile devices across the enterprise as devices themselves (i.e., hardware) are owned and operated by mission partners. The enterprise standard is for the mission partner's equipment/property custodians to maintain its inventory records, including key data elements mandated by governing regulations.

(U) Recommendation 3.B: (U) We recommend that the Director of the Defense Information Systems Agency's Joint Enterprise Services Directorate: Develop and implement a process to ensure inventories are conducted periodically and records are updated in a timely manner; immediately reconcile all issued and on-site classified mobile devices; update inventory records; and take appropriate action if you are unable to properly reconcile a classified mobile device.

(U) DISA partially concurs with this recommendation. As a service provider, DISA does not maintain the inventory records for all classified mobile devices across the enterprise as devices themselves (i.e., hardware) are owned and operated by mission partners. The enterprise standard is for the mission partner's equipment/property custodians to maintain its inventory records, including key data elements mandated by governing regulations.

(U) Recommendation 3.C: ~~(CUI)~~ [redacted]

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

DISA Memo, (U) Response to DoD IG Draft Audit of Cybersecurity of DoD Classified Mobile Devices, Project No. D2021-D000CU-0131.000

(U) DISA concurs with this recommendation. DISA determines [redacted] and takes action based on a monthly report that is pulled manually. DISA will identify an automated solution and devise a plan for compliance by 3Q FY2025.

(U) Recommendation 3.D: ~~(CUI)~~ Develop and implement [redacted]

(U) DISA concurs with this recommendation. DISA is exploring technical solutions for all form factors to automate [redacted] for all classified mobile devices. DISA will identify an automated solution and devise a plan for compliance by 3Q FY2025.

(U) Recommendation 3.E:(U) Immediately revalidate and document the user justification for the devices and recall the device if the user no longer has a valid mission need, revise existing access policies to require detailed written justifications for obtaining classified mobile devices, and establish processes to periodically, at least annually, revalidate the need for continued access to the devices.

(U) DISA concurs with this recommendation. DISA will investigate an automated solution that is consistent with the device ordering process to capture validated need and annual revalidation. DISA will devise a plan for compliance by 3Q FY2025.

(U) Recommendation 3.F: (U) [redacted]

~~(CUI)~~ DISA concurs with this recommendation. [redacted]

(U) Recommendation 3.G: (U) [redacted]

(U) DISA concurs with this recommendation. The current process enforces [redacted] per DISA policy guidance for all DMCC users, to include [redacted]

(U) Recommendation 3.H: (U) Revise existing or develop new classified mobile device training programs that include information on all 23 Office of the Secretary of Defense memorandum requirements.

(U) DISA concurs with this recommendation. DISA is updating training documentation to include the required 23 items. Updated training will be in place by Q3 FY2025.

(U) Recommendation 3.I: (U) Provide all existing classified mobile device users with the updated training that includes all 23 Office of the Secretary of Defense memorandum requirements.

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

DISA Memo, (U) Response to DoD IG Draft Audit of Cybersecurity of DoD Classified Mobile Devices, Project No. D2021-D000CU-0131.000

(U) DISA concurs with this recommendation. Once updated training is in place, DISA will make it available to all existing classified mobile device users. Expected completion is Q4 FY2025.

(U) Recommendation 3.L: ~~(CUI)~~ Develop and implement procedures to verify that their classified mobile device users [redacted] *as required by Committee on National Security Systems Directive No. 520.*

(U) DISA concurs with this recommendation. DISA will identify an automated solution that is consistent with the device ordering process to track annual training status and devise a plan for compliance by 3Q FY2025.

(U) Recommendation 3.J: (U) Establish a mechanism to track the status of all classified mobile device user agreements and ensure that all users have acknowledged the most recent version of the user agreement.

(U) DISA concurs with this recommendation. DISA will identify an automated solution that is consistent with the device ordering process to track signed user agreements and devise a plan for compliance by 3Q FY2025.

(U) Recommendation 3.K: (U) Develop and implement procedures for retaining signed classified mobile device user agreements.

(U) DISA concurs with this recommendation. DISA will identify an automated solution that is consistent with the device ordering process to retain signed user agreements and devise a plan for compliance by 3Q FY2025.

(U) Recommendation 3.M: ~~(CUI)~~ [redacted]

(U) DISA concurs with this recommendation. DISA will establish a [redacted] DISA will devise a plan for compliance by 3Q FY2025.

(U) We appreciate the opportunity to review and comment on the report and recommendations. The point of contact for this audit is [redacted]

BEAN.CAROLIN E.G. [redacted]
Digitally signed by BEAN.CAROLINE.G [redacted]
Date: 2024.10.21 15:35:47 -04'00'

CAROLINE G. BEAN
Director
PEO Services

(U) Annex: Sources of Classified Information

(U) The following documents are sources used to support the classification of information in this report.

(U) **Source 1**: DISA's DMCC-S Removed Users from Directory Service Spreadsheet (Document is Secret).

(U) Declassification date: November 8, 2033
(U) Generated date: November 8, 2023

(U) **Source 2**: USSOCOM Insider Threat Program Briefing Slides (Document is Secret).

(U) Declassification date: December 31, 2047
(U) Generated date: December 5, 2022

(U) **Source 3**: USEUCOM Incident Response Process Playbook, Version 1.4 (Document is Secret).

(U) Declassification date: May 24, 2041
(U) Generated date: May 24, 2021

(U) **Source 4**: DISA Mobility Portfolio Security Classification Guide (Document is CUI)

(U) Declassification date: February 01, 2026
(U) Generated date: October 17, 2016

(CUI) **Source 5**: [redacted] (Document is CUI).

(U) Generated date: August 26, 2021

(U) Acronyms and Abbreviations

(U) CIO	Chief Information Officer
(U) CPEDM	Classified Portable Electronic Device Manager
(U) CNSSD	Committee on National Security Systems Directive
(U) CNSSP	Committee on National Security Systems Policy
(U) CSfC	Commercial Solutions for Classified
(U) DAR	Data-at-Rest
(U) DISA	Defense Information Service Agency
(U) DMCC-S	DoD Mobility Classified Capability – Secret
(U) EUD	End-User Device
(U) HQ	Headquarters
(U) NGD	Next-Generation Device
(U) NIST SP	National Institute of Standards and Technology Special Publication
(U) NSA	National Security Agency
(U) OSD	Office of the Secretary of Defense
(U) SOCCENT	U.S. Special Operations Command Central
(U) USEUCOM	U.S. European Command
(U) USSOCOM	U.S. Special Operations Command
(U) USSTRATCOM	U.S. Strategic Command
(U) WINDAR-S	Windows Data-at-Rest – Secret

(U) Glossary

(U) Authorizing official. A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations, organizational assets, or individuals.

(U) Directory Service. A directory service stores information about objects on a network, such as information about user accounts, and makes the information available to network users and administrators.

(U) Encryption. The process of changing plain text to an unreadable format for the purpose of security or privacy.

(U) Subscriber Identity Module Card. A removable hardware token that provides data storage and cellular access.

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:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

Twitter
www.twitter.com/DoD_IG

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~~