



U.S. Department of Defense

July 11, 2024



DOD OIG (b)(6)

[illegible]

~~SECRET~~





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

July 11, 2024

(U) MEMORANDUM FOR COMMANDER, U.S. AIR FORCES IN EUROPE

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

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

(U) The Commander of U.S. Air forces in Europe agreed to address the recommendations of the management advisory or proposed alternative corrective actions that met the intent of the recommendations. Therefore, we consider the recommendations resolved and open. We will close the recommendations when you provide us documentation showing that all agreed-upon actions to implement the recommendations 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 **DOD OIG (b)(6)**, (DSN **DOD OIG (b)(6)**) **DOD OIG (b)(6)**.

FOR THE INSPECTOR GENERAL:

Bryan Clark

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

(U) Introduction

(U) Executive Summary

(U) Since Russia's full-scale invasion of Ukraine on February 24, 2022, the United States and its allies have transferred defense items to the Ukrainian Armed Forces (UAF) to support their war effort. Within the U.S. European Command (USEUCOM), U.S. Air Forces in Europe (USAFE) personnel assigned to the Logistics Enabling Node Romania (LEN-R) are responsible for overseeing the transfer of a portion of the defense items to the UAF through Romania. The United States uses locations such as LEN-R to transfer equipment by truck, rail, or air for onward movement to Ukraine. At LEN-R, USAFE personnel handle customs clearance, accountability, and reporting for the delivery of contracted defense items on behalf of the U.S. Government. LEN-R personnel report on the results of these transfers to the Security Assistance Group Ukraine (SAG-U).

(U) In January 2024, during our ongoing evaluation of LEN-R, we identified operational and information security vulnerabilities that created a risk of inadvertently revealing sensitive or classified DoD information, which could impact the overall success of the LEN-R mission.¹ Specifically, USAFE personnel provided our team with documentation that was not properly marked in accordance with USEUCOM and USAFE security classification guidance or supplemental documentation. Additionally, USAFE personnel violated DoD Instruction (DoDI) 8170.01, DoD Manual (DoDM) 5200.01, and Secretary of Defense guidance by transmitting official DoD information over public networks using personal electronic devices (PEDs) and third-party messaging services.²

(U) These situations occurred for two reasons. Specifically, USAFE did not provide LEN-R personnel with:

- (U) mission-specific classification guidance or instruction on the application of limited existing theater guidance regarding the appropriate classification of mission-related information, or
- (U) the equipment necessary to conduct their mission through approved communications platforms.

(U) If an adversary or strategic competitor compromises the operational details contained within the documentation and communications, it could result in serious damage to U.S. national security interests by providing information sufficient to disrupt

¹ (U) DoD OIG Project No. D2023 DEVOPC 0027.000, "Evaluation of Security and Accountability Controls for Defense Items Transferred to Ukraine Through Romania."

² (U) DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019, incorporating Change 1 effective August 24, 2021. DoD Manual 5200.01, Volume 3, "DoD Information Security Program," February 24, 2012, Effective July 28, 2020.

(U) ongoing operations and cause harm to personnel, property, the mission, and Ukraine's sovereignty and territorial integrity.

(U) We recommend that the Commander of USAFE conduct a review of USAFE security classification guidance to determine whether the guidance is sufficient for USAFE personnel to properly mark, store, and disseminate information related to USAFE missions in support of Ukraine and provide direction for USAFE units on existing or updated guidance following the sufficiency review. We also recommend that the Commander provide the necessary equipment to enable personnel stationed at LEN-R to transmit and receive classified information securely. Further, we recommend that the Commander incorporate guidance and lessons learned from this management advisory into annual trainings and security refreshers for USAFE subordinate commands.

(U) The USAFE Commander agreed with two of the recommendations and disagreed with one recommendation. The Commander agreed to conduct a review and determine whether the current USAFE security classification guidance is sufficient for USAFE personnel to properly mark, store, and disseminate information. The Commander also agreed to incorporate guidance and lessons learned from this management advisory into annual trainings and security refreshers for USAFE subordinate commands. The Commander disagreed with the recommendation to provide the necessary equipment to enable personnel stationed at LEN-R to transmit and receive official information securely, stating that due to the complexity of communications needed to meet mission requirements, he authorized an exception to policy in DoDI 8170.01. According to DoDI 8170.01, Component heads have the authority to approve official use of non-DoD controlled and non-federal controlled electronic messaging services. Although it does not mitigate the risk, the USAFE Commander's authorization of the exception listed in DoDI 8170.01 minimally meets the intent of the recommendation because it documents the USAFE Commander's acceptance of risk. Therefore all three of the recommendations are resolved but remain open pending DoD OIG verification of the Commander's actions.

(U) Objective

(U) The objective of this ongoing evaluation is to determine the effectiveness and efficiency of the DoD's security and accountability controls for U.S. defense items transferred to the UAF through LEN-R. This management advisory addresses urgent security concerns we discovered with operational and information security of documents and communications used to manage, track, and coordinate the movement of U.S. defense items to Ukraine through LEN-R.

(U) Background

(U) Since Russia's full-scale invasion of Ukraine on February 24, 2022, the United States and its allies have transferred defense items to the UAF to support their war effort. The DoD transports U.S. defense items by air or sea from the United States to aerial and sea ports of debarkation, as well as specified LENs in the USEUCOM area of responsibility, for onward movement to Ukraine. Once defense items are in USEUCOM's area of responsibility, the DoD transports the items through a LEN and transfers the defense items to Ukrainian trains or trucks for onward movement to Ukraine.

~~(S)~~ One transport location within USEUCOM is LEN-R. USAF (b)(1)(1.4a), (b)(1)(1.4g)

[REDACTED]

(U) DoD Policy and USEUCOM and USAFE Guidance on Security Classification

(U) DoDM 5200.01 volume 3 identifies the roles and responsibilities for the protection of classified national security information.³ Specifically, DoDM 5200.01 implements policy and provides procedures for the safeguarding, storage, destruction, transmission, and transportation of classified information. DoDM 5200.01 volume 2 states that: the proper marking of a classified document is the specific responsibility of the original or derivative classifier, and derivative classifiers shall refer to the source documents, Security Classification Guides (SCGs), or other guidance issued by the original classification authority when determining the markings to apply.⁴

³ (U) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, Incorporating Change 3, Effective July 28, 2020.

⁴ (U) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Marking of Information," February 24, 2012, Incorporating Change 4, Effective July 28, 2020.

(U) DoDM 5200.01 volume 3 states that an SCG is the authoritative document for derivative classification. Volume 3 also states that DoD personnel must transmit classified information over secure communications circuits approved for transmission of information at the specified level of classification. This includes communication by telephone, email, and other forms, such as messages or websites. DoDM 5200.01 volume 3 also provides procedures for the safeguarding, storage, destruction, transmission, and transportation of classified information. According to the manual, DoD personnel must transmit classified information over secure communications circuits approved for transmission of information at the specified level of classification. This includes communication by telephone, email, and other forms, such as messages or websites.

(U) To implement DoDM 5200.01, USEUCOM developed an SCG that establishes the basic policies for proper classification and release of information relevant to USEUCOM, including vulnerabilities, capabilities, systems, projects, and programs that pertain to operations, exercises, and training events during normal and emergency periods. The USEUCOM SCG provides both original and derivative classifiers with guidance on the required classification level and duration of classification based on the types of information or documentation created. USAFE also developed their own SCG that references and incorporates the USEUCOM SCG, but provides additional guidance specific to USAFE missions.

(U) Additionally, the DoD regulates how DoD personnel may use electronic devices to communicate official DoD information. Specifically, DoDI 8170.01, states, "DoD personnel must not use personal email or other nonofficial accounts to exchange official information."⁵ The DoDI also states, "Personal, nonofficial accounts may not be used to conduct official DoD communications for personal convenience or preferences."

⁵ (U) DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019, incorporating Change 1 effective August 24, 2021.

(U) USAFE Personnel at LEN-R Mishandled Classified and Sensitive Mission Data

(S) USAFE personnel at LEN-R did not properly mark, store, or disseminate classified and sensitive mission data in accordance with the USEUCOM or USAFE Security Classification Guides (SCGs) or supplemental guidance. USAF (b)(1)(1.4a), (b)(1)(1.4g)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(S) Additionally, USAFE personnel at LEN-R violated DoD information security policies by using unauthorized PEDs and a third-party electronic messaging application to transmit official DoD information. USAF (b)(1)(1.4a), (b)(1)(1.4g)

[REDACTED]

[REDACTED]

[REDACTED]

(U) These conditions occurred because USAFE did not provide LEN-R personnel with:

- (U) mission-specific classification guidance or instruction on the application of limited existing theater guidance regarding the appropriate classification of mission-related information, or
- (U) the equipment necessary to conduct their mission through approved communications platforms.

(U) As a result, the DoD risks serious damage to U.S. national security interests, operational security, and the success of the DoD's mission to provide Ukraine defense items through Romania.

(S) This is the second management advisory we have issued on information security concerns related to Ukraine operations within the USEUCOM area of responsibility. Previously, the DoD OIG issued Report No. DODIG-2024-002, a management advisory discussing the protection of sensitive mission data by SAG-U and its subordinate commands on November 2, 2023. That advisory identified that DoD personnel at a LEN in Poland transmitted sensitive DoD logistics information over PEDs using the public third-party electronic messaging application and did not use authorized secure systems to store and transmit sensitive information.⁷

⁶ (U) We requested information for the ongoing DoD OIG Project No. D2024 DEVOPC 0027.000, "Evaluation of Security and Accountability Controls for Defense Items Transferred to Ukraine Through Romania."

⁷ (U) The DoD OIG is currently conducting Project No. D2024 DEVOPC 0083.000, "Follow up Evaluation of Management Advisory: The Protection of Sensitive Mission Data by the Security Assistance Group Ukraine and Its Subordinate Commands," to follow up on the results of the management advisory.

(U) USAFE Personnel at LEN-R Did Not Handle Classified and Sensitive Mission Data in Accordance with DoD Requirements

{S} We identified that USAFE personnel at LEN-R did not properly mark, store, or disseminate classified and sensitive mission data in accordance with the USAFE or USEUCOM SCGs or supplemental guidance. USAF (b)(1)(1.4a), (b)(1)(1.4g)

[REDACTED]

{S} As part of an ongoing evaluation, USAFE officials at LEN-R responded to a request for information on LEN-R operations by providing a number of documents, including USAF (b)(1)(1.4a), (b)(1)(1.4g) and other documentation containing operational details through NIPRNet. The classification markings on these documents were inconsistent; some carried CUI markings, others were unmarked.

{S} USAF (b)(1)(1.4a), (b)(1)(1.4g)

[REDACTED]

(U) The USEUCOM SCG identifies the following classification guidance for these types of information.

- (U) USAF (b)(1)(1.7e) should be classified as SECRET until 1 year after operation completion.

⁸ (U) Joint Operations Directives summarize current operations in space and time, provide commander's intent and guidance, and establish tasks resulting from decision boards. These messages, typically drafted as orders, allow staffs to quickly gain and share situational awareness and understanding.

- (U) Participating units, including types, vulnerabilities, locations, quantities, readiness status, deployments, redeployments, or details of movement of U.S. friendly forces in operations, should be classified as SECRET until mission completion.
- (U) Movement of ammunition, aircraft, and other equipment should be treated as Confidential and may be classified higher at the direction of the USEUCOM Logistics Directorate.
- (U) Host nation participation should be classified as SECRET until plan execution.
- (U) Specific locations of temporarily deployed communications nodes supporting contingency or exercise-related command and control networks should be classified as SECRET until redeployment.

~~(CUI)~~ The USAFE SCG identifies a number of similar elements consistent with the requirements of the USEUCOM SCG. Specifically, the USAFE SCG mirrors language regarding classification as a minimum of SECRET for information on participating units, including types, vulnerabilities, locations, quantities, readiness status, deployments, redeployments, and details of movement of U.S. friendly forces. The USAFE SCG also includes language stating that the specifics of communications security hardware requires classification as SECRET, similar to the USEUCOM SCG's language regarding the locations of deployed communications nodes.

~~(S)~~ Following our review of the SCGs, we contacted the USEUCOM Special Security Office (J24) and the USAFE IP Office to request clarification on the proper classification of the information we received. We provided USEUCOM J24 [REDACTED], and other documents to review. USEUCOM J24 officials stated that [REDACTED] [REDACTED]. However, the J24 officials recommended that we contact the USAFE IP Office, as the owners of the information with subject matter experts, who could review the documents and make definitive classification determinations. We therefore provided [REDACTED], and other document to the USAFE IP office and similarly asked for guidance on the proper classification of the information. The USAFE IP Office Director reviewed the information and stated that at least one element in each of the three documents we provided contained classified information.

~~(S)~~ An official from the USAFE IP office stated on March 20, 2024, that the [REDACTED] would need to conduct an official inquiry into the spillage of classified information, which began on March 27, 2024. The [REDACTED] completed their inquiry on June 10, 2024, and concluded that an inadvertent spillage of classified information and controlled unclassified information did occur.

(U) USAF Personnel at LEN-R Used PEDs and Third-Party Electronic Messaging Services to Communicate Official Information

{S} USAF personnel at LEN-R violated DoD information security policies by using PEDs and a third-party electronic messaging application to transmit official DoD information.

USAF (b)(1)(1.4a), (b)(1)(1.4g)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) DoDI 8170.01 states, "DoD personnel must not use personal email or other nonofficial accounts to exchange official information." The DoDI also states, "Personal, nonofficial accounts may not be used to conduct official DoD communications for personal convenience or preferences." Specifically, the Instruction states, "DoD personnel may not use personal, nonofficial accounts to conduct official DoD communications." On April 17, 2023, the Secretary of Defense issued a memorandum emphasizing cybersecurity protocols that references the requirements of DoDI 8170.01.⁹ The memorandum states that DoD Components must immediately review and assess their adherence to standards for protecting classified National security information. Additionally, USEUCOM issued a memorandum, on April 17, 2023, reinforcing DoD policy prohibiting the use of non-DoD controlled electronic messaging systems, except when specific conditions are met.¹⁰

{S} USAF (b)(1)(1.4a), (b)(1)(1.4g)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Although DoD policy generally prohibits the use of PEDs to conduct official DoD business, DoDI 8170.01 does provide for limited exceptions to the

⁹ (U) "Memorandum for all Department of Defense Personnel: Immediate Review and Assessment of Department of Defense Information Security Procedures," April 17, 2023.

¹⁰ (U) "Memorandum for Distribution: Use of Non DoD controlled Electronic Messaging Systems," April 17, 2023.

~~(S)~~ policy under three conditions. The three conditions for using personal PEDs are: 1) Emergencies or other critical mission needs; 2) When official communication capabilities are unavailable, impractical, or unreliable; and 3) It is in the interests of DoD or other U.S. Government missions. However, USAFE personnel we interviewed were not aware of any documentation requesting or granting an exception to the policy under the three conditions allowed.

(U) USAFE Did Not Provide Mission-Specific Classification Guidance or Approved Communications Equipment to Mission Personnel

(U) The conditions occurred because USAFE did not provide LEN-R personnel with:

- (U) mission-specific classification guidance or instruction on the application of limited existing theater guidance regarding the appropriate classification and protection of mission related information, or
- (U) the equipment necessary to conduct their mission through approved communications platforms.

(U) USEUCOM and USAFE SCGs Did Not Provide Clear Guidance on the Classification of Ukraine-Specific Information

~~(S)~~ We reviewed the USEUCOM and USAFE SCGs and previous DoD OIG reports. We also interviewed USAFE IP, ~~(U) USAF (b)(1), (b)(4), (b)(5), (b)(6), (b)(7)(C), (b)(7)(D), (b)(7)(F), (b)(7)(G), (b)(7)(H), (b)(7)(I), (b)(7)(J), (b)(7)(K), (b)(7)(L), (b)(7)(M), (b)(7)(N), (b)(7)(O), (b)(7)(P), (b)(7)(Q), (b)(7)(R), (b)(7)(S), (b)(7)(T), (b)(7)(U), (b)(7)(V), (b)(7)(W), (b)(7)(X), (b)(7)(Y), (b)(7)(Z), (b)(7)(AA), (b)(7)(AB), (b)(7)(AC), (b)(7)(AD), (b)(7)(AE), (b)(7)(AF), (b)(7)(AG), (b)(7)(AH), (b)(7)(AI), (b)(7)(AJ), (b)(7)(AK), (b)(7)(AL), (b)(7)(AM), (b)(7)(AN), (b)(7)(AO), (b)(7)(AP), (b)(7)(AQ), (b)(7)(AR), (b)(7)(AS), (b)(7)(AT), (b)(7)(AU), (b)(7)(AV), (b)(7)(AW), (b)(7)(AX), (b)(7)(AY), (b)(7)(AZ), (b)(7)(BA), (b)(7)(BB), (b)(7)(BC), (b)(7)(BD), (b)(7)(BE), (b)(7)(BF), (b)(7)(BG), (b)(7)(BH), (b)(7)(BI), (b)(7)(BJ), (b)(7)(BK), (b)(7)(BL), (b)(7)(BM), (b)(7)(BN), (b)(7)(BO), (b)(7)(BP), (b)(7)(BQ), (b)(7)(BR), (b)(7)(BS), (b)(7)(BT), (b)(7)(BU), (b)(7)(BV), (b)(7)(BW), (b)(7)(BX), (b)(7)(BY), (b)(7)(BZ), (b)(7)(CA), (b)(7)(CB), (b)(7)(CC), (b)(7)(CD), (b)(7)(CE), (b)(7)(CF), (b)(7)(CG), (b)(7)(CH), (b)(7)(CI), (b)(7)(CJ), (b)(7)(CK), (b)(7)(CL), (b)(7)(CM), (b)(7)(CN), (b)(7)(CO), (b)(7)(CP), (b)(7)(CQ), (b)(7)(CR), (b)(7)(CS), (b)(7)(CT), (b)(7)(CU), (b)(7)(CV), (b)(7)(CW), (b)(7)(CX), (b)(7)(CY), (b)(7)(CZ), (b)(7)(DA), (b)(7)(DB), (b)(7)(DC), (b)(7)(DD), (b)(7)(DE), (b)(7)(DF), (b)(7)(DG), (b)(7)(DH), (b)(7)(DI), (b)(7)(DJ), (b)(7)(DK), (b)(7)(DL), (b)(7)(DM), (b)(7)(DN), (b)(7)(DO), (b)(7)(DP), (b)(7)(DQ), (b)(7)(DR), (b)(7)(DS), (b)(7)(DT), (b)(7)(DU), (b)(7)(DV), (b)(7)(DW), (b)(7)(DX), (b)(7)(DY), (b)(7)(DZ), (b)(7)(EA), (b)(7)(EB), (b)(7)(EC), (b)(7)(ED), (b)(7)(EE), (b)(7)(EF), (b)(7)(EG), (b)(7)(EH), (b)(7)(EI), (b)(7)(EJ), (b)(7)(EK), (b)(7)(EL), (b)(7)(EM), (b)(7)(EN), (b)(7)(EO), (b)(7)(EP), (b)(7)(EQ), (b)(7)(ER), (b)(7)(ES), (b)(7)(ET), (b)(7)(EU), (b)(7)(EV), (b)(7)(EW), (b)(7)(EX), (b)(7)(EY), (b)(7)(EZ), (b)(7)(FA), (b)(7)(FB), (b)(7)(FC), (b)(7)(FD), (b)(7)(FE), (b)(7)(FF), (b)(7)(FG), (b)(7)(FH), (b)(7)(FI), (b)(7)(FJ), (b)(7)(FK), (b)(7)(FL), (b)(7)(FM), (b)(7)(FN), (b)(7)(FO), (b)(7)(FP), (b)(7)(FQ), (b)(7)(FR), (b)(7)(FS), (b)(7)(FT), (b)(7)(FU), (b)(7)(FV), (b)(7)(FW), (b)(7)(FX), (b)(7)(FY), (b)(7)(FZ), (b)(7)(GA), (b)(7)(GB), (b)(7)(GC), (b)(7)(GD), (b)(7)(GE), (b)(7)(GF), (b)(7)(GG), (b)(7)(GH), (b)(7)(GI), (b)(7)(GJ), (b)(7)(GK), (b)(7)(GL), (b)(7)(GM), (b)(7)(GN), (b)(7)(GO), (b)(7)(GP), (b)(7)(GQ), (b)(7)(GR), (b)(7)(GS), (b)(7)(GT), (b)(7)(GU), (b)(7)(GV), (b)(7)(GW), (b)(7)(GX), (b)(7)(GY), (b)(7)(GZ), (b)(7)(HA), (b)(7)(HB), (b)(7)(HC), (b)(7)(HD), (b)(7)(HE), (b)(7)(HF), (b)(7)(HG), (b)(7)(HH), (b)(7)(HI), (b)(7)(HJ), (b)(7)(HK), (b)(7)(HL), (b)(7)(HM), (b)(7)(HN), (b)(7)(HO), (b)(7)(HP), (b)(7)(HQ), (b)(7)(HR), (b)(7)(HS), (b)(7)(HT), (b)(7)(HU), (b)(7)(HV), (b)(7)(HW), (b)(7)(HX), (b)(7)(HY), (b)(7)(HZ), (b)(7)(IA), (b)(7)(IB), (b)(7)(IC), (b)(7)(ID), (b)(7)(IE), (b)(7)(IF), (b)(7)(IG), (b)(7)(IH), (b)(7)(II), (b)(7)(IJ), (b)(7)(IK), (b)(7)(IL), (b)(7)(IM), (b)(7)(IN), (b)(7)(IO), (b)(7)(IP), (b)(7)(IQ), (b)(7)(IR), (b)(7)(IS), (b)(7)(IT), (b)(7)(IU), (b)(7)(IV), (b)(7)(IW), (b)(7)(IX), (b)(7)(IY), (b)(7)(IZ), (b)(7)(JA), (b)(7)(JB), (b)(7)(JC), (b)(7)(JD), (b)(7)(JE), (b)(7)(JF), (b)(7)(JG), (b)(7)(JH), (b)(7)(JI), (b)(7)(JJ), (b)(7)(JK), (b)(7)(JL), (b)(7)(JM), (b)(7)(JN), (b)(7)(JO), (b)(7)(JP), (b)(7)(JQ), (b)(7)(JR), (b)(7)(JS), (b)(7)(JT), (b)(7)(JU), (b)(7)(JV), (b)(7)(JW), (b)(7)(JX), (b)(7)(JY), (b)(7)(JZ), (b)(7)(KA), (b)(7)(KB), (b)(7)(KC), (b)(7)(KD), (b)(7)(KE), (b)(7)(KF), (b)(7)(KG), (b)(7)(KH), (b)(7)(KI), (b)(7)(KJ), (b)(7)(KK), (b)(7)(KL), (b)(7)(KM), (b)(7)(KN), (b)(7)(KO), (b)(7)(KP), (b)(7)(KQ), (b)(7)(KR), (b)(7)(KS), (b)(7)(KT), (b)(7)(KU), (b)(7)(KV), (b)(7)(KW), (b)(7)(KX), (b)(7)(KY), (b)(7)(KZ), (b)(7)(LA), (b)(7)(LB), (b)(7)(LC), (b)(7)(LD), (b)(7)(LE), (b)(7)(LF), (b)(7)(LG), (b)(7)(LH), (b)(7)(LI), (b)(7)(LJ), (b)(7)(LK), (b)(7)(LL), (b)(7)(LM), (b)(7)(LN), (b)(7)(LO), (b)(7)(LP), (b)(7)(LQ), (b)(7)(LR), (b)(7)(LS), (b)(7)(LT), (b)(7)(LU), (b)(7)(LV), (b)(7)(LW), (b)(7)(LX), (b)(7)(LY), (b)(7)(LZ), (b)(7)(MA), (b)(7)(MB), (b)(7)(MC), (b)(7)(MD), (b)(7)(ME), (b)(7)(MF), (b)(7)(MG), (b)(7)(MH), (b)(7)(MI), (b)(7)(MJ), (b)(7)(MK), (b)(7)(ML), (b)(7)(MM), (b)(7)(MN), (b)(7)(MO), (b)(7)(MP), (b)(7)(MQ), (b)(7)(MR), (b)(7)(MS), (b)(7)(MT), (b)(7)(MU), (b)(7)(MV), (b)(7)(MW), (b)(7)(MX), (b)(7)(MY), (b)(7)(MZ), (b)(7)(NA), (b)(7)(NB), (b)(7)(NC), (b)(7)(ND), (b)(7)(NE), (b)(7)(NF), (b)(7)(NG), (b)(7)(NH), (b)(7)(NI), (b)(7)(NJ), (b)(7)(NK), (b)(7)(NL), (b)(7)(NM), (b)(7)(NN), (b)(7)(NO), (b)(7)(NP), (b)(7)(NQ), (b)(7)(NR), (b)(7)(NS), (b)(7)(NT), (b)(7)(NU), (b)(7)(NV), (b)(7)(NW), (b)(7)(NX), (b)(7)(NY), (b)(7)(NZ), (b)(7)(OA), (b)(7)(OB), (b)(7)(OC), (b)(7)(OD), (b)(7)(OE), (b)(7)(OF), (b)(7)(OG), (b)(7)(OH), (b)(7)(OI), (b)(7)(OJ), (b)(7)(OK), (b)(7)(OL), (b)(7)(OM), (b)(7)(ON), (b)(7)(OO), (b)(7)(OP), (b)(7)(OQ), (b)(7)(OR), (b)(7)(OS), (b)(7)(OT), (b)(7)(OU), (b)(7)(OV), (b)(7)(OW), (b)(7)(OX), (b)(7)(OY), (b)(7)(OZ), (b)(7)(PA), (b)(7)(PB), (b)(7)(PC), (b)(7)(PD), (b)(7)(PE), (b)(7)(PF), (b)(7)(PG), (b)(7)(PH), (b)(7)(PI), (b)(7)(PJ), (b)(7)(PK), (b)(7)(PL), (b)(7)(PM), (b)(7)(PN), (b)(7)(PO), (b)(7)(PP), (b)(7)(PQ), (b)(7)(PR), (b)(7)(PS), (b)(7)(PT), (b)(7)(PU), (b)(7)(PV), (b)(7)(PW), (b)(7)(PX), (b)(7)(PY), (b)(7)(PZ), (b)(7)(QA), (b)(7)(QB), (b)(7)(QC), (b)(7)(QD), (b)(7)(QE), (b)(7)(QF), (b)(7)(QG), (b)(7)(QH), (b)(7)(QI), (b)(7)(QJ), (b)(7)(QK), (b)(7)(QL), (b)(7)(QM), (b)(7)(QN), (b)(7)(QO), (b)(7)(QP), (b)(7)(QQ), (b)(7)(QR), (b)(7)(QS), (b)(7)(QT), (b)(7)(QU), (b)(7)(QV), (b)(7)(QW), (b)(7)(QX), (b)(7)(QY), (b)(7)(QZ), (b)(7)(RA), (b)(7)(RB), (b)(7)(RC), (b)(7)(RD), (b)(7)(RE), (b)(7)(RF), (b)(7)(RG), (b)(7)(RH), (b)(7)(RI), (b)(7)(RJ), (b)(7)(RK), (b)(7)(RL), (b)(7)(RM), (b)(7)(RN), (b)(7)(RO), (b)(7)(RP), (b)(7)(RQ), (b)(7)(RR), (b)(7)(RS), (b)(7)(RT), (b)(7)(RU), (b)(7)(RV), (b)(7)(RW), (b)(7)(RX), (b)(7)(RY), (b)(7)(RZ), (b)(7)(SA), (b)(7)(SB), (b)(7)(SC), (b)(7)(SD), (b)(7)(SE), (b)(7)(SF), (b)(7)(SG), (b)(7)(SH), (b)(7)(SI), (b)(7)(SJ), (b)(7)(SK), (b)(7)(SL), (b)(7)(SM), (b)(7)(SN), (b)(7)(SO), (b)(7)(SP), (b)(7)(SQ), (b)(7)(SR), (b)(7)(SS), (b)(7)(ST), (b)(7)(SU), (b)(7)(SV), (b)(7)(SW), (b)(7)(SX), (b)(7)(SY), (b)(7)(SZ), (b)(7)(TA), (b)(7)(TB), (b)(7)(TC), (b)(7)(TD), (b)(7)(TE), (b)(7)(TF), (b)(7)(TG), (b)(7)(TH), (b)(7)(TI), (b)(7)(TJ), (b)(7)(TK), (b)(7)(TL), (b)(7)(TM), (b)(7)(TN), (b)(7)(TO), (b)(7)(TP), (b)(7)(TQ), (b)(7)(TR), (b)(7)(TS), (b)(7)(TT), (b)(7)(TU), (b)(7)(TV), (b)(7)(TW), (b)(7)(TX), (b)(7)(TY), (b)(7)(TZ), (b)(7)(UA), (b)(7)(UB), (b)(7)(UC), (b)(7)(UD), (b)(7)(UE), (b)(7)(UF), (b)(7)(UG), (b)(7)(UH), (b)(7)(UI), (b)(7)(UJ), (b)(7)(UK), (b)(7)(UL), (b)(7)(UM), (b)(7)(UN), (b)(7)(UO), (b)(7)(UP), (b)(7)(UQ), (b)(7)(UR), (b)(7)(US), (b)(7)(UT), (b)(7)(UU), (b)(7)(UV), (b)(7)(UW), (b)(7)(UX), (b)(7)(UY), (b)(7)(UZ), (b)(7)(VA), (b)(7)(VB), (b)(7)(VC), (b)(7)(VD), (b)(7)(VE), (b)(7)(VF), (b)(7)(VG), (b)(7)(VH), (b)(7)(VI), (b)(7)(VJ), (b)(7)(VK), (b)(7)(VL), (b)(7)(VM), (b)(7)(VN), (b)(7)(VO), (b)(7)(VP), (b)(7)(VQ), (b)(7)(VR), (b)(7)(VS), (b)(7)(VT), (b)(7)(VU), (b)(7)(VV), (b)(7)(VW), (b)(7)(VX), (b)(7)(VY), (b)(7)(VZ), (b)(7)(WA), (b)(7)(WB), (b)(7)(WC), (b)(7)(WD), (b)(7)(WE), (b)(7)(WF), (b)(7)(WG), (b)(7)(WH), (b)(7)(WI), (b)(7)(WJ), (b)(7)(WK), (b)(7)(WL), (b)(7)(WM), (b)(7)(WN), (b)(7)(WO), (b)(7)(WP), (b)(7)(WQ), (b)(7)(WR), (b)(7)(WS), (b)(7)(WT), (b)(7)(WU), (b)(7)(WV), (b)(7)(WW), (b)(7)(WX), (b)(7)(WY), (b)(7)(WZ), (b)(7)(XA), (b)(7)(XB), (b)(7)(XC), (b)(7)(XD), (b)(7)(XE), (b)(7)(XF), (b)(7)(XG), (b)(7)(XH), (b)(7)(XI), (b)(7)(XJ), (b)(7)(XK), (b)(7)(XL), (b)(7)(XM), (b)(7)(XN), (b)(7)(XO), (b)(7)(XP), (b)(7)(XQ), (b)(7)(XR), (b)(7)(XS), (b)(7)(XT), (b)(7)(XU), (b)(7)(XV), (b)(7)(XW), (b)(7)(XZ), (b)(7)(YA), (b)(7)(YB), (b)(7)(YC), (b)(7)(YD), (b)(7)(YE), (b)(7)(YF), (b)(7)(YG), (b)(7)(YH), (b)(7)(YI), (b)(7)(YJ), (b)(7)(YK), (b)(7)(YL), (b)(7)(YM), (b)(7)(YN), (b)(7)(YO), (b)(7)(YP), (b)(7)(YQ), (b)(7)(YR), (b)(7)(YS), (b)(7)(YT), (b)(7)(YU), (b)(7)(YV), (b)(7)(YW), (b)(7)(YZ), (b)(7)(ZA), (b)(7)(ZB), (b)(7)(ZC), (b)(7)(ZD), (b)(7)(ZE), (b)(7)(ZF), (b)(7)(ZG), (b)(7)(ZH), (b)(7)(ZI), (b)(7)(ZJ), (b)(7)(ZK), (b)(7)(ZL), (b)(7)(ZM), (b)(7)(ZN), (b)(7)(ZO), (b)(7)(ZP), (b)(7)(ZQ), (b)(7)(ZR), (b)(7)(ZS), (b)(7)(ZT), (b)(7)(ZU), (b)(7)(ZV), (b)(7)(ZW), (b)(7)(ZX), (b)(7)(ZY), (b)(7)(ZZ)~~ and LEN-R personnel, and determined that USEUCOM and USAFE officials did not provide mission-specific guidance or instruct LEN-R personnel in the proper application of existing guidance regarding classification marking, storage, or dissemination of mission-related information. We reviewed the USEUCOM and USAFE SCGs for information related to missions in support of Ukraine security assistance and did not find any specific guidance. Additionally, a previous DoD OIG management advisory found that the USEUCOM SCG only “includes generic guidance and may not include sufficient detail for making classification decisions about the DoD’s Ukraine security assistance mission.”¹¹ That management advisory recommended that the Commander of USEUCOM review existing classification guidance and determine whether the guidance was sufficient to enable personnel within USEUCOM to conduct proper derivative classification. Depending on the outcome of that review, the management advisory also recommended either updating the USEUCOM SCG with additional guidance specific to Ukraine assistance operations or providing clarifying guidance to officials on how to perform derivative classification with the existing guidance. While USEUCOM concurred with those recommendations, officials indicated that the review would not be complete until May 2024. According to

¹¹ (U) DoD OIG Report No. DODIG 2023 105, “Management Advisory: U.S. European Command Security Classification Guidance for Ukraine Assistance,” August 11, 2023.

~~(S)~~ USAFE officials, as of March 2024, USEUCOM had not provided any additional guidance.

~~(S)~~ Officials at LEN-R and the ~~USAF (b)(1)(1.4a), (b)(1)(1.4g)~~ were unsure of the classification level of their mission and documentation. During our interviews with ~~USAF (b)(1)(1.4a), (b)(1)(1.4g)~~ personnel, including current and former LEN-R commanders, some of these personnel stated that they believed portions of their mission information should be CUI at a minimum and potentially classified due to compilation and aggregation. However, current and former LEN-R commanders also stated that while they were aware of SCGs, they did not know whether USEUCOM had developed an SCG for the mission to transfer defense articles to Ukraine and that no one from their leadership chain provided them with security classification guidance related to their mission. Additionally, the ~~USAF (b)(1)(1.4a), (b)(1)(1.4g)~~ personnel, including the ~~USAF (b)(1)(1.4a), (b)(1)(1.4g)~~ Commander, stated that they did not know whether SAG-U or USAFE issued specific guidance regarding the classification of the LEN-R mission and documentation created from it. The ~~USAF (b)(1)(1.4a), (b)(1)(1.4g)~~ Commander also stated that they understood the information related to transfers of defense items to be unclassified or CUI.

~~(S)~~ During an interview with the USAFE IP Office Director, we asked whether the USEUCOM staff had provided any additional supplementary guidance to USAFE on conducting derivative classification for Ukraine-related activities. The USAFE IP Office Director was aware of USEUCOM and USAFE Night Orders and the USEUCOM and USAFE SCGs but stated that they were unaware of any SCG or guidance regarding classification of cargo movement information related to Ukraine or the LEN-R mission.

~~(CUI)~~ We previously identified and highlighted security concerns related to insufficient SCG guidance for USEUCOM personnel. Specifically, on August 11, 2023, we issued a management advisory on USEUCOM SCGs for Ukraine assistance due in part to the receipt of information that U.S. Army Europe and Africa personnel did not properly mark as classified.¹² The August 2023 management advisory also identified that the USEUCOM SCG includes generic guidance and may not include sufficient detail for making classification decisions about the DoD's Ukraine security assistance mission. The management advisory emphasized that the absence of sufficient guidance regarding the proper classification of activities in support of the DoD's Ukraine security assistance missions creates a risk that personnel within multiple commands in the USEUCOM area of responsibility may not mark documents with the appropriate level of classification. That management advisory recommended that the Commander of USEUCOM determine whether current SCGs were sufficient to provide USEUCOM personnel with guidance related to the classification of Ukraine mission-related information. As of April 2024, a USEUCOM official stated indicated they were still in the process of addressing the recommendation, with an estimated completion in May 2024.

¹² (U) DoD OIG Report No. DODIG 2023 105 "Management Advisory: U.S. European Command Security Classification Guidance for Ukraine Assistance," August 11, 2023.

~~(U)~~ USEUCOM is already working on resolving the above recommendation, and we are not recommending additional action by the Commander of USEUCOM at this time.

(U) USAFE Officials Did Not Provide LEN-R with Necessary Communications Equipment

~~(S)~~ USAFE officials did not provide LEN-R personnel with necessary equipment to conduct their mission through approved communications platforms and in accordance with DoD policy. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- ~~(S)~~ [REDACTED]
[REDACTED]
- ~~(S)~~ [REDACTED]
[REDACTED]
- ~~(S)~~ [REDACTED]
[REDACTED]

~~(S)~~ [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

~~(S)~~ [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

~~(S)~~ [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

~~(S)~~ The [REDACTED] Commander at [REDACTED] stated that they did not have any current plans to provide additional equipment to the [REDACTED] personnel stationed at LEN-R. Specifically, the Commander stated that the [REDACTED]

~~(S)~~ USAF (b)(1)(1.4a), (b)(1)(1.4g) and USAFE have several ongoing projects for upgrades to communications infrastructure.. USAF (b)(1)(1.4a), (b)(1)(1.4g)

~~(S)~~ We previously identified similar instances of personnel using public third-party messaging applications on PEDs to transmit official DoD information elsewhere within the USEUCOM area of responsibility. In a management advisory released on November 2, 2023, we found that U.S. Army Europe and Africa personnel stationed in Poland transmitted sensitive equipment movement data on their PEDs over public networks, using public messaging applications and public online document editors.¹³ That management advisory recommended that the Commander of the Poland mission issue sufficient government information systems to personnel performing the mission in order to comply with DoD policy.

(U) The DoD Risks Serious Damage to U.S. National Security Interests and Capabilities in USEUCOM

~~(S)~~ Due to these operational and information security vulnerabilities, the DoD risks serious damage to U.S. national security interests, operational security, and the success of the DoD's mission to provide Ukraine additional defense items through Romania.

~~(S)~~ If personnel do not follow proper procedures for derivative classification or communication of classified information regarding the USAF (b)(1)(1.4a), (b)(1)(1.4g) activities or those of DoD contractors or subcontractors to facilitate the transfer of defense items to Ukraine may become compromised. An unauthorized disclosure could increase the risk of harm to DoD, contractor, or partner nation personnel and property.

~~(S)~~ Additionally, the DoD risks disruption to its mission providing security assistance to Ukraine due to the lack of clear guidance on security classification. As a result of a security inquiry into the appropriate level of classification for the LEN-R mission that began following our outreach to the USAFE IP Office, LEN-R personnel stated that they

USAF (b)(1)(1.4a), (b)(1)(1.4g)

¹³ (U) DoD OIG Report No. DODIG 2024 002, "Management Advisory: The Protection of Sensitive Mission Data by the Security Assistance Group – Ukraine and Its Subordinate Commands," November 2, 2023.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the U.S. Air Forces in Europe Commander:

- a. **(U) Conduct a review of U.S. Air Forces in Europe security classification guidance and determine whether existing guidance is sufficient for U.S. Air Forces in Europe personnel to properly mark, store, and disseminate information related to U.S. Air Forces in Europe missions in support of Ukraine, such as those at Logistics Enabling Node–Romania.**
 1. **(U) If the Commander determines that existing guidance is insufficient, the Commander should update the U.S. Air Forces in Europe security classification guide and provide notification to squadron information protection officers informing them of the new guidance.**
 2. **(U) If the Commander determines that existing guidance is sufficient, the Commander should issue coordinating instructions to squadron information protection officers on how to apply existing guidance for U.S. Air Forces in Europe missions in support of Ukraine.**

(U) Commander, U.S. Air Forces in Europe Comments

(U) The USAFE Commander agreed with the recommendation. The Commander stated that the USAFE Information Protection Office reviewed the current security classification guidance and determined that the guidance is in accordance with DoD policy and sufficient for USAFE personnel to properly mark, store, and disseminate information related to USAFE missions in support of Ukraine, such as those at LEN-R. The Commander further stated that the USAFE IP Office has provided additional instructions to ~~USAF (b)(1)(1.7e)~~ IP officers on how to apply existing guidance for USAFE mission in support of Ukraine. Lastly, the Commander stated that at the completion of the formal investigation, the USAFE IP Office will provide all subordinate units lessons learned captured in the investigation to ensure units are trained to standards.

(U) Our Response

(U) Comments from the USAFE Commander addressed all specifics of the recommendation; therefore the recommendation is resolved but will remain open. We will close the recommendation once we verify that the USAFE IP Office has provided the additional guidance and lessons learned specified in the recommendation to subordinate units.

- b. (U) Provide necessary communications equipment and gear to the Logistics Enabling Node–Romania team to allow the squadron to perform its security assistance mission in accordance with DoD Instruction 8170.01, DoD Manual 5200.01, and the Secretary of Defense memorandum on DoD information security procedures, dated April 17, 2023.

(U) Commander, U.S. Air Forces in Europe Comments

(S) The USAFE Commander disagreed with the recommendation, (b)(1)(4a), (b)(1)(4g)

[REDACTED]

[REDACTED], the Commander stated that the LEN-R mission meets all three conditions for an exception to utilize non-DoD communication methods outlined in DoDI 8170.01. The USAFE Commander also stated that he will ensure USAFE creates a memorandum to memorialize the exception to the DoDI 8170.01 requirement to permit LEN-R personnel to utilize non-DoD communication methods.

(U) Our Response

(U) Although the USAFE Commander disagreed with the recommendation, the Commander's response addressed the specifics of the recommendation; therefore the recommendation is resolved and but will remain open. We acknowledge that according to DoDI 8170.01, component heads have the authority to approve official use of non-DoD controlled and non-federal controlled electronic messaging services and that the Commander believes justification for an exception exists because alternative solutions are impractical. Although it is not optimal because it does not mitigate the risk, the USAFE Commander's authorization of the exception listed in DoDI 8170.01 minimally meets the intent of the recommendation because it documents the USAFE Commander's acceptance of risk. We will close the recommendation once we verify that USAFE has issued the memorandum documenting the exception to policy granted by the USAFE Commander under DoDI 8170.01.

- c. (U) Develop guidance and lessons learned from the improper classification and use of third-party electronic messaging services identified in this management advisory into U.S. Air Forces in Europe annual trainings and security refreshers on proper derivative classification and operational security.

(U) Commander, U.S. Air Forces in Europe Comments

(U) The USAFE Commander agreed with the recommendation and stated that USAFE would incorporate lessons learned from security incidents in required annual refresher training, in accordance with DoD Information Security Training policy. The Commander stated that USAFE will continue to incorporate guidance on direct support to national-level mission sets, such as LEN-R, in annual training and security refresher courses.

(U) Our Response

(U) Comments from the USAFE Commander addressed the specifics of the recommendation; therefore the recommendation is resolved but will remain open. We will close the recommendation once we verify that USAFE has incorporated the lessons learned from the security incident into its annual refresher training for USAFE personnel.

(U) Appendix

(U) Scope and Methodology

(U) We conducted this management advisory in March and April 2024 as part of an evaluation of security and accountability controls for defense items transferred to Ukraine through Romania in accordance with the “Quality Standards for Inspection and Evaluation,” published in December 2020 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the evaluation to ensure that objectives are met and that we perform the evaluation to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent, and relevant to lead a reasonable person to sustain our evaluation findings.

(U) We identified and reviewed policies, directives, and DoD guidance. Specifically, we reviewed the following criteria.

- (U) USEUCOM Guide 5201.02A, “USEUCOM Security Classification Guide (SCG),” April 12, 2021
- (U) USAFE Guide UA-SCG-21 “Headquarters United States Air Forces In Europe United States Air Forces Africa Security Classification Guide,” January 31, 2021
- (U) DoDM 5200.01, Volume 3, “DoD Information Security Program: Protection of Classified Information,” February 24, 2012 (Incorporating Change 3, July 28, 2020)
- (U) DoDI 8170.01, “Online Information Management and Electronic Messaging,” January 2, 2019 (Incorporating Change 1, August 24, 2021)
- (U) Secretary of Defense Memorandum, “Immediate Review and Assessment of Department of Defense Information Security Procedures,” April 17, 2023

(U) We interviewed personnel from the following DoD organizations.

- (S) USAF (b)(1)(1.4a), (b)(1)(1.4g)
- (U) USAFE
- (U) USEUCOM
- (U) SAG-U

(S) We travelled to the aerial port of debarkation known as LEN-R at ~~USAF (b)(1)(1.4a), (b)(1)(1.4g)~~ At

LEN-R, we accompanied ~~USAF (b)(1)(1.4a), (b)(1)(1.4g)~~ personnel as they conducted a customs and accountability mission for a shipment of U.S.-procured defense items being transferred to Ukraine at a border transfer point in ~~USAF (b)(1)(1.4a), (b)(1)(1.4g)~~. There, we observed the customs and accountability processes performed by LEN-R personnel. At both

(S) locations, we interviewed LEN-R and [REDACTED] personnel regarding their mission details as well as the classification of information and use of PEDs to conduct DoD business.

(U) We also submitted requests for information and obtained documentation from LEN-R personnel regarding operational security controls and information security of their mission. We interviewed personnel from USAFE and USEUCOM regarding proper classification of information related to LEN-R.

(U) This report was reviewed by USAFE to identify whether any of its 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 USAFE about the CUI treatment of its information. If USAFE failed to provide any sufficient comments about the CUI treatment of its information, we marked the report based on our assessment of the available information.

(U) Management Comments

(U) Commander, U.S. Air Forces in Europe

SECRET



DEPARTMENT OF THE AIR FORCE
UNITED STATES AIR FORCES IN EUROPE
UNITED STATES AIR FORCE S AFRICA

19 June 2024

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: HQ USAF-AF/AFRICA/CC
Unit 3281
APOAE 09094

SUBJECT: (U) United States Air Forces in Europe - Air Forces Africa Response to DoD Office Inspector General Draft Report, "Management Advisory--USAFE-AFACRICA Handling of Sensitive Information at 1 EN-R DRAFT 0516.24" Recommendations 1.a.1, 1.a.2, 1.b, and 1.c

1. (U) This memorandum establishes the United States Air Forces in Europe - Air Forces Africa (USAFE-AFAFRICA) response to the 1.1 IG Draft Report, "Management Advisory - USAFE Handling of Sensitive Information at LENO DRAFT 051624" Recommendations 1.a.1, 1.a.2, 1.b, and 1.c.

2. (U) HQ USAFE-AFAPRICA concurs with DoD IG recommendations with comments to recommendations 1 a.1, 1 a.2, and 1.c. below:

a. (U) Recommendation 1.a.1: We recommend that the U.S. Air Forces in Europe Commander conduct a review of U.S. Air Forces in Europe security classification guidance and determine whether existing guidance is sufficient for U.S. Air Forces in Europe personnel to properly mark, store, and disseminate information related to U.S. Air Forces in Europe missions in support of Ukraine, such as those at Logistics Enabling Node-Romania. If the Commander determines that existing guidance is insufficient, the Commander should update the U.S. Air Forces in Europe security classification guide and provide notification to squadron information protection officers informing them of the new guidance.

(U) **USAFE-AF AFRICA RESPONSE (1.1.1):** Concur with comments USAFE-AFAFRICA Information Protection reviewed the current security classification guidance and I have determined that the guidance is in accordance with DoD policy and is sufficient for U.S. Air Forces in Europe personnel to properly mark, store, and disseminate information related to U.S. Air Forces in Europe missions in support of Ukraine, such as those at Logistics Enabling Node-Romania.

SECRET (S)

[illegible]

~~CONFIDENTIAL - NOFORN~~
~~CONFIDENTIAL - NOFORN~~
 Distribution of ~~CONFIDENTIAL~~
 [REDACTED] (b)(7)(G)

SECRET

SECRET

(U) USAFE-AF AFRICA RESPONSE (1.a.2): Concur with comments. USAFE-AF AFRICA Information Protection reviewed the current security classification guidance and I have determined that the guidance is in accordance with DoD policy and is sufficient for U.S. Air Forces in Europe personnel to properly mark, store, and disseminate information related to U.S. Air Forces in Europe missions in support of Ukraine, such as those at Logistics Enabling Node-Romania.

c. (U) Recommendation 1c: Develop guidance and lessons learned from the improper classification and use of third-party electronic messaging services identified in this management advisory into U.S. Air Forces in Europe annual trainings and security refreshers on proper derivative classification and operational security.

(C) USAFE-AFACRICA RESPONSE (1.c): Concur with comments. In accordance with DoD Information Security Training policy, lessons learned from security incidents are included in required annual refresher training. USAFE-AFACRICA will continue to incorporate guidance on direct support to national-level mission sets, such as IEN-R, in annual training and security refresher courses.

3. (U) HQ USAFE-AF AFRICA non-concurs with DoD IG recommendations with comments to recommendation 1 b. below:

a. (U) Recommendation 1.b: Provide necessary communications equipment and gear to the Logistics Enabling Node-Romania team to allow the squadron to perform its security assistance mission in accordance with DoD Instruction 8170.01, DoD Manual 5200.01, and the Secretary of Defense memorandum on DoD information security procedures dated April 17, 2023.

SECRET

(U) Acronyms and Abbreviations

USAF (b)(1)(1.7e)

DoDI Department of Defense Instruction

DoDM Department of Defense Manual

IP Information Protection

LEN-R Logistics Enabling Node - Romania

USAF (b)(1)(1.7e)

NIPRNet Non-Classified Internet Protocol Router Network

PED Personal Electronic Device

SAG-U Security Assistance Group – Ukraine

SCG Security Classification Guide

USAF (b)(1)(1.7e)

UAF Ukrainian Armed Forces

USAFE U.S. Air Forces in Europe

USEUCOM U.S. European Command

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

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

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

Congressional Liaison
703.604.8324

Media Contact
publicaffairs@dodig.mil; 703.604.8324

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



www.twitter.com/DoD_IG

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

DoD Hotline
www.dodig.mil/hotline



~~SECRET~~



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~~