DEPARTMENT OF THE ARMY
UNITED STATES ARMY GARRISON ITALY
UNIT 31401 BOX 42
APO AE 09630

AMIM-ITO-S

25 August 2023

MEMORANDUM FOR All U.S. Army Garrison (USAG) Italy Units and Supported Units

SUBJECT: U.S. Army Garrison Italy Command Policy, Security Program

1. References. This policy will be used in conjunction with the below listed references, specifically Army Regulation (AR) 380-5 and 380-67. Conflicts between these SOPs or any other higher Headquarters publication will be resolved in favor of the higher-level publication.

a. Department of Defense Manual (DODM) 5200.01, Vol. 1 - 3, DOD Information Security Program, 24 February 2012

b. DODM 5200.02, Procedures for the DOD Personnel Security Program (PSP), 03 April 2017

c. DOD Instruction (DODI) 5200.48, Controlled Unclassified Information (CUI), 06 March 2020

d. AR 380-5, Information Security Program, 22 October 2019

e. AR 380-67, Personnel Security Program, 24 January 2014

f. AR 380-49, Industrial Security Program, 20 March 2013

g. AR 15-6, Procedures for Administrative Investigations and Boards of Officers, 01 April 2016

h. HQDA G2 Memorandum, Army Implementation of Security Executive Agent Directive (SEAD) 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position, 21 June 2022

i. USAG Italy Memorandum, USAG Italy Emergency Destruction and Evacuation Plan for Classified Materials, 16 June 2023

j. USAG Italy Memorandum, Standard Operating Procedure for Closed Storage, 20 June 2023

2. Authorities: This policy is applicable to all personnel assigned, attached, or detailed for duty within USAG Italy and will be strictly adhered to.

3. Purpose. This policy establishes procedures for collateral security programs within

USAG Italy. It is designed to ensure classified and Controlled Unclassified Information (CUI) are properly controlled, accounted for, safeguarded, and destroyed.

4. Responsibilities. The Garrison Commander (GC) is responsible for the effective administration of the Information Security, Personnel Security, and Security Education Training and Awareness (SETA) programs within the Garrison. This includes appointing primary and alternate Command Security Managers, in writing, to implement the security programs and ensure compliance with established directives and regulations.

a. Primary Security Manager (PSM) and Alternate Security Manager (ASM) will-

(1) Advise and represent the commander on matters related to the classification, downgrading, declassification, safeguarding, and destruction of national security information.

(2) Establish and implement an effective security education program.

(3) Conduct in/out-processing briefings for all USAG Italy personnel (military, civilian, and U.S. contractors).

(4) Conduct security inspections and report findings to the commander.

(5) Ensure that personnel who handle classified material are appropriately cleared, have a valid need for access, and are properly trained on marking, safeguarding, transmission, transportation, reproduction, and destruction procedures.

(6) Prepare a Security Clearance Access Roster (SCAR) and make it available, as applicable, for verification of individual security clearances.

(7) Ensure security violations are properly investigated and reported in accordance with reference d.

(8) Establish and maintain visit control procedures when visitors require authorized access to classified information.

(9) Ensure that end-of-day security checks are conducted using Standard Form (SF) 701 *(Activity Security Checklist).* Retain SF 701 forms for a minimum of 90 days.

(10) Coordinate annual cleanout with Garrison Directorates to review electronic and hardcopy CUI and classified documents and oversee proper destruction of all documents that no longer require retention.

b. Individuals will—

(1) Access classified information on a need-to-know basis only to the extent required to perform official duties.

(2) Protect and handle classified information to prevent compromise or unauthorized access.

(3) Ensure classified information is retained within USAG Italy spaces only as long as necessary for official use and secured in a General Services Administration (GSA) container approved for the specific level of classified being secured.

(4) Ensure classified information is not discussed with or accessed by visitors until their identification, authorization, classified access level, and need-to-know has been validated.

(5) Never remove any classified from the office to work on at a personal residence.

(6) Destroy classified documents as necessary using only National Security Agency (NSA) approved crosscut shredders.

(7) Report security violations to the USAG Italy Security Office.

(8) Ensure Controlled Unclassified Information (CUI) held within USAG Italy offices is protected per applicable regulations.

(9) Complete all required security training.

(10) Self-report any issues that may affect security clearance eligibility IAW reference e and h.

(11) Report all foreign travel, in advance, to the USAG Italy Security Office IAW references d and h.

5. Personnel Security. AR 380-67, *Personnel Security Program,* governs all aspects of the Personnel Security program and will be used as guidance for submitting investigations, granting interim access, and reporting derogatory information.

a. All newly assigned military, civilian, and contractor personnel, whether or not they have a security clearance, are required to in-process through the USAG Italy Security Office and receive an initial security awareness briefing. Refresher briefings will be accomplished annually by all personnel.

b. Prior to departure, all personnel scheduled to Permanent Change of Station (PCS), Expiration Term of Service (ETS), terminate assignment, or retire, will report to the USAG Italy Security Office with a copy of their orders to out-process from the installation. The Security Manager will conduct security debriefings using the Standard Form (SF) 312 for personnel who are retiring, separating, discharged, revocation of clearance, or no longer require access to classified material. The organization will maintain these completed forms for 2 years.

c. The access to classified information orally, in writing, or by any other means is limited to persons whose official duties (not title or grade) require the proper security clearance, need-to-know, and a signed nondisclosure agreement utilizing SF 312.

(1) All personnel must have a signed SF 312 and date uploaded in the Defense Information System for Security (DISS) before being granted access to classified information and debriefed when access to classified information has been terminated.

(2) Individuals refusing to sign the SF 312 will not be granted access to classified information. Individuals will be given up to five (5) calendar days to re-evaluate their decision not to sign. At the end of the five (5) day period, refusal to sign the SF 312 will be reported as an incident report to the Defense Counterintelligence and Security Agency Consolidated Adjudication Services (DCSA CAS).

d. Personnel Security Investigations (PSI) and/or Standard Form 86 updates will be submitted in a timely manner using the Personnel Security Investigation Portal (PSIP).

(1) Applicants must complete the required paperwork within the allotted time provided by PSIP to avoid termination of the background investigation request. After a second termination, the Security Manager will request a memorandum from the applicant's supervisor prior to submitting a third PSIP request.

(2) PSIs will be initiated for volunteers requiring access to government information systems. The USAG Italy Security Office will coordinate with the volunteer's sponsoring unit, Trusted Agent (TA), and the USAG Italy Central Processing Facility (CPF) ID Card section to ensure all requirements are met prior to issuance of a Volunteer Common Access Card (VOLAC).

e. The Security Manager will coordinate with the Civilian Personnel Advisory Center (CPAC) to review Position Descriptions (PDs) and ensure the position sensitivity for civilian positions are properly designated.

6. Information Security. AR 380-5, *Information Security Program*, is the primary reference for the protection of U.S. Government Classified and Controlled Unclassified Information within the Army.

a. Classified material received, created, and stored will be protected and handled at all times to prevent compromise and inadvertent or unauthorized access.

b. Information processing equipment used to process classified information will only be moved by the Information Management Office (IMO) Chief or USAG Italy Security Manager. Personnel will adhere to the USAG Italy Memorandum for Closed Storage (reference j) to prevent unauthorized access.

c. All classified material will be marked IAW applicable regulations.

(1) The USAG Italy Security Office will review the markings on classified

documents during Staff Assistance Visits (SAV) and annual Command Inspections (CI).

(2) Cleared personnel will notify the USAG Italy Security Office if they believe information is improperly or unnecessarily classified. The Security Manager will address the issue and provide additional guidance if a formal challenge is warranted.

(3) Foreign government classified information shall be protected in the same way as U.S. classified information of comparable classification.

d. Reproduction of classified material will be held to a minimum and strictly controlled.

(1) Every machine authorized to reproduce classified material will have a sign conspicuously posted on or near it indicating the highest classification it is allowed to reproduce.

(2) Copies of classified documents reproduced for any purpose, including those incorporated in a working paper, are subject to the same controls prescribed for the original document from which copies were made.

e. All classified material will be secured in a GSA-approved security container when not being used. Materials of different classification levels will be segregated to preclude unintentional disclosure and to facilitate emergency destruction.

(1) Each security container shall bear no markings as to indicate the level of classified material stored therein. The only external documentation authorized on a GSA-approved security container are:

(a) SF 702 *(Security Container Checklist)* - annotated each time it is open and closed. Containers not opened during a workday will still be checked and the recorded on the SF 702. Retain SF 702 forms for at least ninety (90) days following the last entry.

(b) Reversible OPEN and CLOSED/SECURED signs

(c) GSA certification label

(2) A SF 700 *(Security Container Information)* will be used to record combinations and emergency points of contact. The envelope portion of SF 700 (Part 2 and Part 2A) will be stored in the USAG Italy Security Office.

(3) The USAG Italy Security Office will change combinations IAW reference d. Any individual requiring access must coordinate with the USAG Italy Security Office. Providing combinations to anyone without the approval of the Security Manager is strictly prohibited.

(4) Requests for maintenance and/or repairs of containers will be routed through the USAG Italy Security Office. Only DOD-certified lock technicians are authorized to

conduct maintenance and repairs on GSA-approved containers.

(5) USAG Italy personnel will consult the USAG Italy Security Office prior to purchasing equipment that will be used to store classified material to ensure regulatory compliance.

(6) Security equipment, to include containers, must be thoroughly inspected prior to turn-in IAW reference d.

(a) Units will coordinate the inspection with the USAG Italy Security Office.

(b) Combinations will be reset to the standard combination (50-25-50).

(c) The inspector/s will remove each container drawer to ensure no classified material remains.

(d) A memorandum of the inspection certifying that no classified material is present will be provided to the USAG Italy Security Office and maintained on file for two (2) years.

f. All disposal and destruction of paper classified materials will be accomplished using an approved NSA cross-cut shredder or other device outlined in reference d.

(1) Disposal of classified media that cannot be properly destroyed via crosscut shredder must be coordinated with IMO and the Security Office.

(2) CUI documents should be considered sensitive in nature and destroyed in the same manner as classified material. Shredding is the preferred method of destruction.

(3) Records of destruction are not required for SECRET material, except for North Atlantic Treaty Organization (NATO) and foreign government documents.

(4) In the event of an emergency or natural disaster, USAG Italy personnel will follow the Emergency Destruction Evacuation Plan (EDEP) outlined in reference i.

g. The preferred method of transmitting classified information is electronically via Secret Internet Protocol Router Network (SIPRNET) or Joint Worldwide Intelligence Communications System (JWICS).

h. The second best method of transmitting classified information is via official registered mail (up to Secret level classification).

(1) Personnel transmitting classified information via official registered mail will coordinate with the USAG Italy Security Office to ensure they are properly trained on the shipping/handling requirements.

(a) Under no circumstances shall the United States Postal Service Express

Mail label 11-B "Waiver of Signature and Indemnity" be used.

(b) Classified material must be mailed at the post office. Use of street mail collection boxes is prohibited.

(c) Shipment of bulk classified material will be coordinated through the USAG Italy Security Office to ensure regulatory compliance.

i. When receiving classified material, if a discrepancy is found (e.g., improper packaging or addressing, incorrect classification markings on the wrappers) the receiver will account for the material received, take all necessary measures to secure, and immediately report it to the USAG Italy Security Office.

j. Incoming official mail is handled via the USAG Italy Central Mail Room that separates normal mail from certified or registered mail which may contain classified information.

(1) Only authorized personnel with the appropriate clearance that are listed on Postal Service (PS) Form 3801 *(Standing Delivery Order)* may pick up mail from the certified or registered mail area.

(2) Registered or certified official mail will be opened by a cleared individual in a discrete location outside of view of non-cleared personnel. The USAG Italy Security Office will be contacted if the contents are classified.

k. Personnel hand carrying classified must have a Department of Defense (DD) Form 2501 *(Courier Authorization)* in their possession.

(1) Couriers must read and sign a courier brief prior to hand carrying classified.

(2) Courier cards are issued for no more than two (2) years or DEROS date, whichever is earlier.

(3) Classified material must remain under the control of the courier at all times during transportation. Leaving classified material unattended in locked vehicles, car trunks, or government conveyance is strictly prohibited and in violation of security regulations.

(4) Hand carrying classified material outside the Vicenza, Italy area requires courier orders, provided by the Security Manager, in addition to the courier card.

l. Security Violations. Anyone discovering a possible compromise (unauthorized access to classified) or violation of security procedures for collateral material will immediately report the incident to the USAG Italy Security Office.

(1) Submit an initial report of any collateral violation, in writing, to the USAG Italy Security Office within 48 hours. The initial report will include the following information.

(a) The date, title, and classification of the information involved.

(b) The office of primary interest and the originator.

(c) 5Ws; Who, What, When, Where, Why and How.

(d) Under no circumstance will classified information be included in the initial report.

(2) In the case of a suspected compromise, the Garrison Commander will appoint an investigating officer to conduct a Preliminary Inquiry (PI). The appointee will meet with the USAG Italy Security Office to receive training and guidance prior to the start of the inquiry. The PI will be conducted IAW reference g and establish one of the following:

(a) That a compromise did not occur.

(b) That a compromise may have occurred and, when appropriate, support the administrative sanctions listed in reference d.

(c) That a compromise of classified information did occur, but there is no reasonable possibility of damage to the national security.

(3) Final results of the PI will be provided to the USAG Italy Security Office. In the event of a compromise, the Security Manager will report the findings to HQDA G2 and the Original Classification Authority IAW reference d.

(4) Contractor-related security incidents involving classified information and/or CUI will be reported to the Contracting Officer's Representative (COR). The COR will ensure the USAG Italy Security Office, Facility Security Officer (FSO), and Defense Security Service (DSS) Industrial Security Representative are informed. A damage assessment will be conducted by the U.S. Government.

m. USAG Italy personnel sponsoring or hosting classified briefings or conferences are responsible for the proper protection and dissemination of classified information and verification of security clearances.

(1) Classified meetings must be coordinated with the Security Manager to ensure all necessary measures are in place to safeguard classified information.

(2) Verification of visitor security clearances can be accomplished by submission of a Visit Access Request (VAR) via DISS by the owning SM to the Security Management Office (SMO) code W6E7AA.

(3) USAG Italy Security Office will prepare a security clearance roster of attendees after verifying security clearances and a need-to-know.

(4) The Security Manager and/or designated cleared personnel will walk through

meeting spaces during extended breaks and end of day to ensure no classified material has been left unsecured.

n. All secure working areas and containers must be checked by cleared personnel at the end of every duty day.

(1) The last person leaving the office each day will complete the SF 701 Activity Security Checklist posted near the office door exit.

(2) He/she will ensure that all classified material is properly secured, to include classified waste, computer disks, classified hard drives and laptops. Security containers will be locked, checked, and the top of furnishings cleared of items which might conceal classified material.

(3) He/she will ensure the SF 702 has been properly annotated for all classified security containers.

(4) Any noticeable tampering or suspicious markings will be reported to the USAG Italy Security Office.

(5) Retain SF 701 for a minimum of ninety (90) days following the last entry.

7. Industrial Security. The AR 380-49, governs all aspects of the Army's Industrial Security Program and will be used as guidance for requirements, restrictions, and other safeguards to prevent the unauthorized disclosure of classified information and CUI released to current, prospective, or former Army contractors.

a. Contractors requiring a CAC to perform their official duties must in-process with the USAG Italy Security Office. Contractors will provide a copy of their Letter of Authorization (LOA) and receive an initial security briefing tailored to their official duties.

b. For contractor personnel performing on a classified contract and requiring classified access, the Security Manager must verify that the contractor has a signed SF 312 recorded in DISS. If the contractor is performing under an unclassified contract, no access to classified information is authorized even if the individual has clearance eligibility in DISS.

c. All contractors requiring access to classified information must have a Visit Access Request (VAR) sent to the USAG Italy Security Office (SMO: W6E7AA) via DISS.

d. The Security Manager will initiate a PSI for any contractor who does not have the appropriate investigation on file. The USAG Italy Security Office is not authorized to process investigations on contractor personnel for security eligibility, only for CAC credentialing.

8. Security Education.

a. All newly assigned personnel, whether military, civilian, or contractor with or without security clearance will receive an initial briefing from the USAG Italy Security Office.

b. Periodic training bulletins, instructions, and changes to regulations published by the Deputy Chief of Staff Intelligence (DCSINT), USAG Italy, IMCOM, or higher headquarters will be disseminated for mandatory reading by all assigned or attached personnel.

c. All assigned cleared personnel will receive annual refresher training on basic security policies, principles, practices, regulations and criminal, civil, and administrative penalties. Refresher training will be conducted throughout the year by utilizing visual aids, emails, or classroom briefings, as applicable.

d. USAG Italy personnel are responsible for completing security training through the Center for Development Security Excellence (CDSE) website.

(1) Initial "DOD Initial Orientation and Awareness Training is required for all military, civilian, and contractors. The "DOD Annual Security Awareness Refresher" is required annually thereafter.

(2) All cleared personnel requiring access to classified information systems must complete "Derivative Classification" training annually. The training certificate will be uploaded in the Army Training & Certification and Tracking System (ATCTS).

(3) All personnel will complete "DOD Mandatory Controlled Unclassified Information (CUI)" training annually.

9. Proponent. The Office of Primary Responsibility for this action is USAG Italy S3/5/7 Security Office at 314-646-5720/5722 or email: usarmy.usag-italy.id-europe.list.security-office@army.mil.

10. Expiration. This Command Policy supersedes any previous USAG Italy Security Program Command Policy or SOP and will remain in effect until superseded or rescinded.

SCOTT W. HORRIGAN
COL, IN
COMMANDING