DEPARTMENT OF THE ARMY
UNITED STATES ARMY GARRISON ITALY
OPC 427 BOX 36
APO AE 09630

AMIM-ITO-O 09 July 2025

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

SUBJECT: U.S. Army Garrison Italy Operations Security (OPSEC) Policy

1. References:

a. Army Regulation (AR) 530-1, (Operations Security).

b. DoD Directive (DoDD) 5205.02E, (DoD Operations Security (OPSEC) Program),

2. Applicability. This policy applies to all USAG Italy Soldiers, Department of the Army (DA) Civilians and contractors, Family Members, and personnel supporting USAG Italy's mission.

3. Responsibility: AR 530-1 states, "OPSEC is everyone's responsibility". The operations security responsibility rests with each member of the organization to protect Critical Information (CI). Likewise, every member of the USAG Italy team must make every effort to protect critical and sensitive information essential to the success of our missions and for the protections of our Soldiers, Civilians, and their Families. This requires you to become familiar with the type of information I have identified as CI.

4. The following list identifies the type of information I expect you to protect from potential threat exploitation. Critical Information can be exploited to impact mission accomplishment. This is my approved Critical Information List (CIL):

a. Locations, capabilities, activities, requirements, and vulnerabilities, of Mission Essential Vulnerable Area (MEVAs) or High-Risk Targets (HRTs).

b. Schedules, itineraries, or purposes of travel of distinguished visitors or key personnel within the USAG Italy footprint.

c. Plans of present or future deployments and training exercises of USAG Italy supported units.

d. Changes in operations or security postures of USAG Italy, and the Random Antiterrorism Measure (RAM) schedule to support protection.

e. Budget allocations or shortfalls affecting Installation missions and operations. Security measures used to protect USAG Italy personnel, MEVAs, and HRTs (i.e. alarm systems, patrol frequencies, and security camera zones).

f. Details of agreements (i.e. Memorandums of Agreement (MOAs) or Memorandums of Understanding (MOUs)) between USAG Italy and our Host Nation.

g. Times, locations, attendees, and security plans of non-public major events.

h. Personal Identifiable Information (PII) of USAG Italy Soldiers, DA Civilians, contractors, and Family Members.

5. OPSEC considerations must be part of USAG Italy planned activities, especially those including out foreign partners. Adhering to the mandates of foreign disclosure review, complying with established security policies and security procedures also supports the overall OPSEC objective. I expect all USAG Italy personnel at each level to protect sensitive and critical information that potentially could be exploited by our adversaries. This will minimize unauthorized access to information important to mission success. The following OPSEC measures support the protection of the types of information identified on the USAG Italy CIL and should be implemented in day-to-day activities:

a. Do not discuss your work in public places or where others can overhear your conversation.

b. All papers, either handwritten or printed, must be destroyed by using an approved crosscut shredder before being discarded in the trash.

c. Do not send CI or PII via unencrypted e-mail messages.

d. Do not send CI or PII on unsecure telephones.

e. Ensure all information for public release receives an OPSEC review by OPSEC Level 2 trained personnel.

f. Remove Common Access Card (CAC) when away from your workstation.

g. Do not display access badges or CAC outside your workplace (i.e. outside your building or facility).

h. Only disclose CI or PII on a need-to-know basis.

i. Control access to your respective building or facility, and escort personnel not assigned.

j. Limit the number of indicators to the greatest extent possible, which could highlight increased operational activity.

6. OPSEC is a continuous process and an inherent part of military culture. We must take into consideration the changing nature of CI, the threat, known and unknown vulnerabilities concerning USAG Italy's operations and fully integrate OPSEC into the execution of all our operations and supporting activities. Our adversaries are monitoring our activities, conversations, and communications using a variety of methods in an attempt to gain information they can use against us. Therefore, everyone must carefully consider whether their actions, activities, or coordination processes used to accomplish the mission adequately protect CI from our adversaries' collection efforts. The security of our Nation, success to the mission, and the lives of our Soldiers, Civilians, and their Families depend on everyone's awareness and practicing good OPSEC.

7. Point of contact for this memorandum is USAG Italy S-3 Operations Branch at DSN: 314-646-5700/5732. CIV: 0444-71-5700/5732, Email: usarmy.usag-italy.id-europe.mbxinstallation-operations@army.mil.

STRONG.VAUGHN.DOUGLAS.JR.1089658191

Digitally signed by STRONG.VAUGHN.DOUGLAS.JR.1089658191
Date: 2025.07.15 11:23:45 +02'00'

VAUGHN D. STRONG JR.
COL, IN
Commanding