



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

IMIT-PL

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: United States Army Garrison (USAG) Italy Command Policy Letter #37,
Operations Security (OPSEC)

1. References:

- a. DoD Directive 5205.2, DoD Operations Security Program
- b. AR 530-1, Operations Security, 26 September 2014
- c. AER 530-1, Operations Security, 15 September 2008
- d. U.S. Army Garrison (USAG) Italy Operations Security (OPSEC) SOP

2. This policy applies to all USAG Italy Soldiers, DA Civilians and contractors, Family members, and personnel supporting USAG Italy's mission.

3. Army Regulation 530-1 states that "OPSEC is everyone's responsibility". That 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 the critical and sensitive information essential to the success of our missions and for the protection 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; information which could be used 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 from USAG Italy and/or our tenant units.
- c. Plans of present or future deployments and training exercises of USAG Italy tenant units.

IMIT-PL

SUBJECT: United States Army Garrison (USAG) Italy Command Policy Letter #37,
Operations Security (OPSEC)

- 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 effecting Installation missions and operations.
- f. Security measures used to protect USAG Italy personnel, MEVAs, and HRTs (i.e. alarm systems, patrol frequency, security camera zones).
- g. Details of agreements (i.e. Memorandums of Agreement (MOAs) or Memorandums of Understanding (MOUs)) between USAG Italy and our host nation.
- h. Times, locations, attendees, and security plans of non-public major events.
- i. Personal Identifiable Information (PII) of USAG Italy Soldiers, DA Civilians and contractors, and Family members.

5. OPSEC considerations must be part of USAG Italy planned activities, especially those including our foreign partners. Adhering to the mandates of foreign disclosure review and complying with established security policies and security systems procedures also supports the overall OPSEC objective. I expect all USAG Italy personnel at each level to protect sensitive and critical information that could potentially 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 paper, 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 personally identifiable information (PII) via unencrypted e-mail messages.
- d. Do not discuss 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. building or facility).

IMIT-PL

SUBJECT: United States Army Garrison (USAG) Italy Command Policy Letter #37,
Operations Security (OPSEC)

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 critical information, the threat, and 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 our critical information from our adversaries' collection efforts. The security of our Nation, success of 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 Directorate of Plans, Training, Mobilization, and Security (DPTMS) Operations Branch at DSN: 314-637-8035/8007, CIV: 0444-61-8035/8007, usarmy.vicenza.imcom.mbx.ops@mail.mil

STEVEN M. MARKS
COL, SF
Commanding

DISTRIBUTION:
Electronic