DEPARTMENT OF THE ARMY
UNITED STATES ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, US ARMY GARRISON, PRESIDIO OF MONTEREY
1759 LEWIS ROAD, SUITE 210
MONTEREY, CA 93944-3223

REPLY TO
ATTENTION OF

AMIM-PMG-ZA (530-1a) 30 January 2023

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy #47, Garrison Operations Security

1. Every member of United States Army Garrison, Presidio of Monterey (USAG POM) is responsible for Garrison Operations Security (OPSEC) and the protection of our mission. Our success requires your active involvement.

2. The threat is real! We are involved in an information war. Adversaries monitoring our activities, conversations, and communications use various methods to collect information that can be used against us. We must maintain a constant awareness of our actions, limit what we say over the phone, encrypt emails to the maximum extent possible, and cease "shop talk" in environments where individuals without the need to know might overhear.

3. OPSEC is our first line of defense against intelligence collection methods. OPSEC security measures are fundamental actions for preventing, detecting, and subverting an adversary's indirect actions on our mission. OPSEC awareness and countermeasures must continue to evolve as our information operations and technology advance. OPSEC training is mandatory for all members of the USAG POM workforce.

4. USAG POM follows the five-step OPSEC process - Identify critical information, analyze threat, analyze vulnerability, assess risk, and apply countermeasures—to maximize our potential for successful operation in the information age. Refer to the Garrison OPSEC SOP for additional details. Furthermore, the garrison-level OPSEC working group (OPSEC WG) uses the five-step OPSEC process to develop the Organization Critical Information List (CIL). The CIL is not all-encompassing and includes only the top 10 specific facts about activities, capabilities and activities needed by adversaries to disrupt mission accomplishment. The CIL is approved by the GC annually. A copy of the CIL is available on the POM SharePoint site at:

https://armyeitaas.sharepoint-mil.us/sites/IMCOM-ID-T-USAG-PoM/DPTMS%20OPSEC%20Library/Forms/AllItems.aspx?viewid=bdae7e5d%2Ddf1d%2D4249%2Db9e6%2Dd5f16848833a

5. USAG POM OPSEC Program Manager will establish an OPSEC Working Group (OPSEC WG) that stays abreast of changes within the OPSEC program while collaborating to ensure the success of the program. The OPSEC WG is an important

feeder board to the Protection Executive Committee (PEC). The OPSEC WG is responsible for conducting the following activities:

-Meet quarterly
-Dumpster inspections
-Spot-inspections throughout the organization
-Review OPSEC violations and make recommendations for corrective actions
-Validate CIL
-Conduct OPSEC Assessment
-Make recommendations for additions / deletions to the CIL
-Brief PEC on OPSEC findings involving two or more organizations and associated recommendations.

6. The responsibility to support the USAG POM OPSEC program rests with everyone assigned to USAG POM.

7. An OPSEC review will be mandatory for (1) Information on the CIL, (2) Information owner determines information is sensitive that is not on the CIL, and (3) Information owner is unsure if information is sensitive and seeks review by OPSEC Program Manager. The process for requesting an OPSEC review is to send an email, with the document(s) requiring an OPSEC review, to the Garrison OPSEC Program Manager at: darryl.e.powe3.civ@army.mil

8. For further information, contact the USAG POM OPSEC Program Manager, Dr. Darryl E. Powe Sr. at (831) 242-4030 or darryl.e.powe3.civ@army.mil

SAMUEL W. KLINE
COL, SF
Commanding

DISTRIBUTION:
G