



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

OCT 20 2020

IMPM-ZA

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy #44, Facility Entry Control on POM and OMC

1. References:

- a. AR 190-13, The Army Physical Security Program, 27 Jun 2019
- b. AR 190-51, Security of Unclassified Army Resources (Sensitive and Nonsensitive), 27 Jun 2019
- c. AR 380-67, Personnel Security Program, 24 Jan 2014
- d. AR 380-5, Department of the Army Information Security Program, 29 Sep 2000
- e. AR 25-2, Cybersecurity, 4 Apr 2019
- f. DA PAM 25-2-13, Army Identity, Credential and Access Management and Public Key Infrastructure Implementing Instructions, 8 Apr 2019
- g. POM Installation Protection Plan, Annex N (Physical Security Plan), 27 Jul 2018
- h. Command Policy #17, Installation Access Procedures for Visitors, 25 Jan 2015

2. Purpose: To establish policy and procedures derived from regulations, which provide security guidance to mitigate threats to facilities housing Unclassified Information System assets that are connected to the Defense Information Systems Network within the POM area of responsibility.

3. Applicability: This policy applies to all persons entering, traveling through, assigned to, in temporary duty status at or employed on POM and OMC. Violation of this policy may subject the individual to adverse administrative action and punishment under the UCMJ. Individuals found violating this policy may be barred from further entry onto the installation.

4. Proponent: The proponent for this policy is Directorate of Plans, Training, Mobilization and Security (DPTMS) with coordination from the Directorate of Emergency Services (DES).

IMPM-ZA

SUBJECT: Command Policy #44, Facility Entry Control on POM and OMC

5. Controlled Areas: Access to POM and OMC facilities will be controlled at all times with a system to identify and validate entry into the facility. Controlling facility access is accomplished through the actions listed below.

a. Mission Essential Vulnerable Areas (MEVA). MEVAs are essential to the accomplishment of the installation's mission and are vulnerable to a threat intent on destroying, damaging or tampering with property and/or equipment which includes removing sensitive items and equipment or property and acts of terrorism. These facilities require additional protection through application of increased physical measures, procedures and equipment.

b. Restricted Areas (RA). RAs are either classified vaults/message centers (managed per AR 600-8-14), AA&E or pharmacy storage areas, and require additional protection through application of increased physical security measures, procedures and equipment. Commanders/Directors of RAs will designate access rosters (unaccompanied and accompanied) in memorandum format, and will post Restricted Area signs in conspicuous and appropriate places to identify the site as a restricted area. Announcement of the site as restricted will include posting signs at each entrance to the site.

c. Communications Closets or Computer Rooms. Communications closets or computer rooms will be secured at all times in accordance with reference 1.b. The Network Enterprise Center (NEC) will maintain custody of keys or combinations used to secure communication server rack(s) and room(s), and is the approval authority for access. Visitors conducting maintenance in communication closets or computer rooms must coordinate their visit with the NEC in advance to gain access.

d. Entry Control Point (ECP) for facilities designated in paragraphs 5.a.- c.

(1) These facilities should have only one main ECP into the critical portion of their facility and must have a process to monitor who and when personnel access and exit the facility. The ECP may be controlled with either an automated access system, trained staff or both. If it is not feasible or logical to establish an facility ECP, then a designated ECP can serve as the initial point of access at auxiliary or special purpose buildings.

(2) Access Control Systems (ACS). These ECPs will be equipped with an ACS in order to validate personnel access into the facility using either automated or manual verification. An automated ACS uses a combination (two-factor verification) of pin codes, passwords, ID card, and biometrics to validate a person's right of entry into the facility. Manual ACS includes keypad and keyed lock systems and may require a staff member to view a person's valid credential against an access roster for the facility.

6. Free Access Facilities: Free Access Facilities are buildings, which host various services available to authorized visitors, intentionally do not have ECPs, and allow

IMPM-ZA

SUBJECT: Command Policy #44, Facility Entry Control on POM and OMC

sufficient access in order to receive installation support services with minimum interference. Examples on POM include (but are not limited to) Headquarters Bldg., Tin Barn, Taylor Hall and DLIFLC academic institutions. Examples on OMC include (but are not limited to) DFMWR Stillwell Center, AAFES Main PX and DECA Commissary.

a. Offices or workspaces. Whenever an individual permanently assigned to the activity is not present, offices or work spaces in which government equipment is located will be secured (i.e. after duty hours or when otherwise unoccupied).

b. Visitors are not allowed to remain within office or workspaces while the primary occupants are vacant. During working hours, the assigned staff to an office or workspace provide security for offices for which they work in.

c. Security will consist of closing and locking appropriate doors and windows, as a minimum.

7. Locks and Keys: Lock and key control procedures are accomplished in accordance with AR 190-11, Chapter 3 and AR 190-51, Appendix D. It is incumbent on the unit to administer regulatory inspections of the keys (required every six months) and to update the Access/Sign-Out Roster when appropriate.

a. Keys are stored inside a container, which has been locked and sealed with an access/sign out roster memorandum signed by the commander and attached to the container.

b. Only GSA approved locks (www.navfac.navy.mil), such as 5200 series or high security locks, with solid hardened steel body and positive key retention will be used for the security of government weapons and equipment.

8. Visitor Control Program: Commanders and Directors will comply with the installation access procedures to ensure only authorized individuals enter the installation. Commanders and directors will not grant visitors unescorted installation access without the required identity proofing, vetting against the National Crime Information Center Interstate Identification Index (NCIC-III), the Terrorism Screening Data Base (TSDB) and determination of a valid purpose for entry for all personnel who do not possess a CAC, another Federal personal identity verification card, or other DOD ID card (reference 1.h.).

a. Specific Visitor types include: Media, DOD Contractors, POM Housing Residents, Gold Star Family members, patrons of Continuing Development Incorporated (CDI), sponsored guests for special event or Family Care Plans, and vetted deliver drivers for commercial or food delivery/vendors, taxies, tow trucks, repossessions and movers.

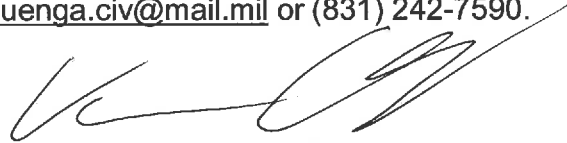
IMPM-ZA

SUBJECT: Command Policy #44, Facility Entry Control on POM and OMC

b. All visitors will coordinate with the appropriate staff section to gain further access into the government facilities. If visitors require access to controlled areas (listed in paragraph 5), their host will make arrangements ahead of time and be properly escorted at all times during their visit.

9. Common Access Card (CAC): CACs enable access to the Army's Non-Secure Internet Protocol Router network (NIPRnet) may also be used as an ACS credential to access POM/OMC facilities. Personnel will maintain positive control of their issued Common Access Card at all times to prevent unauthorized access to computers and facilities. Positive control of these CACs is defined as having direct line of sight from the authorized hold of the card to its location.

10. POC for this memorandum is Ms. Janice Quenga, POM Antiterrorism Officer (ATO) and may be reached via email at janice.l.quenga.civ@mail.mil or (831) 242-7590.



VARMAN S. CHHOEUNG
COL, SF
Commanding

DISTRIBUTION:

G