



DEPARTMENT OF THE ARMY
10TH ARMY AIR AND MISSILE DEFENSE COMMAND
UNIT 25357
APO AE 09067

AECG-AMD

8 November 2019

MEMORANDUM FOR All Personnel Assigned, Attached, or OPCON to 10th Army Air and Missile Defense Command (AAMDC), Rhine Ordnance Barracks, Germany 09067

SUBJECT: Policy Letter #6, Foreign Military Exchange Policies, Procedures, and Requirements

1. References:

- a. Army Regulation (AR) 600-20, Army Command Policy
- b. AR 614-10, Army Military Personnel Exchange Program with Military Services of Other Nations
- c. AR 11-31, Army International Security Cooperation Policy
- d. AR 380-5, Department of the Army Information Security Program
- e. AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives
- f. 10th AAMDC Restricted Area Security Identification Badge Policy

2. Purpose. This memorandum establishes the policies, procedures, and requirements for hosting foreign military personnel at any echelon within 10th AAMDC either as part of an informal exchange or in support of the Army's Military Personnel Exchange Program (MPEP). All formations within 10th AAMDC are required to understand and adhere to these policies.

3. Definitions.

a. Controlled Unclassified Information (CUI): Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies (i.e., For Official Use Only [FOUO]).

b. Classified Military Information (CMI): Information originated by or for the Department of Defense or its agencies—or is under their jurisdiction or control—which requires protection in the interests of national security. It is designated TOP SECRET, SECRET, and CONFIDENTIAL, as described in Executive Order 12356. Classified military information may be in oral, visual, or material form and has been subdivided further into the eight categories described below.

c. Personally Identifiable Information (PII): Unique information about an individual that can be used to distinguish or trace his or her identity. It includes, but is not limited to: name, social security number, date and place of birth, mother's maiden name, home address and phone number, personal e-mail address, biometric records, financial transactions, medical history, criminal or employment history, and other information to which a security manager may have

AECG-AMD

SUBJECT: 10th AAMDC Command and Policy Letter #6, Foreign Military Exchange Policies, Procedures, and Requirements

access. PII does not include an individual's name when it is associated with work elements, such as duty phone number, duty address, and U.S. Government e-mail address.

d. Disclosure: Conveying classified information, in any manner, to an authorized representative of a foreign government.

e. Compromising Emanations: Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment.

f. Military Personnel Exchange Program (MPEP): A reoccurring foreign military officer assigned to 10th AAMDC or a subordinate command on a permanent tour of duty status.

4. Requirements pursuant to foreign military exchanges:

a. Contact Officer: Units hosting foreign military personnel will appoint in writing an officer or NCO of equivalent or higher rank as the personnel being hosted to serve as the contact officer.

(1) Temporary Exchange: The assigned contact officer will receive a brief from their respective command special security officer (SSO)—typically the S2 at the battalion and brigade levels—or from the 10th AAMDC, SSO. The contact officer must have contact with the foreign exchange officer at least twice daily. The contact officer must be familiar with AR 614-10 paragraph 6-7, and adhere to all stated requirements.

(2) MPEP: The assigned contact officer must receive a foreign disclosure brief from the United States Army Europe Foreign Disclosure Officer; and brief the foreign exchange officer on relevant Department of the Army and local policies. The contact officer must have contact with the foreign exchange officer at least twice daily. Additionally, the contact officer will prepare assessments of the exchange for the USAREUR MPEP office on an annual basis, or as required. The contact officer must familiarize themselves with AR 614-10 paragraph 6-7, and adhere to all stated requirements.

b. Alternate Contact Officer: Units hosting foreign military personnel will likewise appoint in writing an officer or NCO of equivalent or higher rank as the personnel being hosted to serve as the alternate contact officer to. The alternate contact officer will fulfil all requirements of the primary contact officer if circumstances separate the contact officer from the foreign exchange officer.

c. Foreign Disclosure Requirements.

(1) The G2 or S2 of the hosting echelon must brief the foreign exchange officer about access to classified environments and documentation, with an emphasis on enabling participation. The G2 or S2 will also inform colleagues of the disclosure limitations on foreign military personnel access of classified military information.

AECG-AMD

SUBJECT: 10th AAMDC Command and Policy Letter #6, Foreign Military Exchange Policies, Procedures, and Requirements

(2) As needed, 10th AAMDC Datalink Operations Cell will facilitate foreign disclosure processes related to allowing an exchange officer to operate in or near sensitive systems, or to view data from sensitive systems.

d. MPEP Certification. MPEP exchange officers must sign a certification form provided by the USAREUR MPEP office within 15 days of arrival and before being formally assigned to their duty position. The 10th AAMDC G5 will facilitate this process.

e. Network Access. As needed, 10th AAMDC G6 must establish all network accounts and email services on Information Assurance Support Environment NIPR (IASE NIPR) and SIPR (IASE SIPR) that will enable an MPEP exchange officer to conduct business on behalf of the command. Email addresses will assume the following format: First.M.Last.fm@mail.mil. Network access is a requirement for MPEP exchanges. Network access is optional for temporary exchanges. It is the responsibility of the hosting unit to request 10th AAMDC G6 support to facilitate network access for temporary exchanges if the unit wants the exchange officer to have network access.

(1) The 10th AAMDC Information Assurance Manager (IAM), in coordination with the Contact Officer, will verify MPEP exchange officers have been trained on the appropriate security policies and consequences of not adhering to the security policies and responsibilities are fully explained. (2) The 10th AAMDC G6 Help Desk will ensure a signed acceptable use policy is on file for all MPEP exchange officers prior to having access to DoD information systems.

(3) The 10th AAMDC G6 Network Defense support personnel will ensure all 10th AAMDC Information Assurance Support Environment (IASE) users understand incident response and classified spill response plans.

(4) 10th AAMDC G6 is responsible for updating its Tenant Security Plan in order to reflect the IASE REL enclave.

f. Facilities Access. The G2 or S2 of the hosting echelon will ensure foreign military officers receive badges and access appropriate for their duties and clearance levels.

5. Security and Information Handling Procedures. All personnel assigned or attached to 10th AAMDC and its subordinate commands working in close proximity to foreign military personnel will:

a. Ensure all sensitive information (CUI, FOUO, PII) remain in locked drawers when not in use, and that all CMI is stored and secured according to regulations.

b. Ensure SIPR systems are locked in GSA-approved safes when not in use if not in an open storage area.

c. Ensure doors to open storage area rooms are closed if personnel inside them are working on SIPR or handling CMI. Such rooms must be locked when left unattended.

d. Ensure that exchange officers do not have unescorted access to any open storage area.

AECG-AMD

SUBJECT: 10th AAMDC Command and Policy Letter #6, Foreign Military Exchange Policies, Procedures, and Requirements

e. Ensure end-of-day security checks are completed as required and GSA containers are checked after the container is opened and closed throughout the duty day. Supervisors must verify SF 701s and 702s are properly filled out at the beginning of each duty day to ensure no security infraction/incidents occurred.

f. Not openly discuss sensitive and/or classified information while foreign officers are present. If required, find an empty room to do so, behind both a physical and auditory barrier.

g. When a foreign officer is escorted into a controlled access area, the escort will announce "red badge" to alert all personnel of the presence of an uncleared visitor or visitors. All uniformed, DA and contractor personnel will respond by sanitizing their areas of any CMI or CUI that has not previously been cleared by an FDR/FDO.

h. All products, media, presentations, conversations, etc. not properly vetted through a foreign disclosure representative for presentation to a foreign officer must be either shut off (e.g. SIPR systems, projectors, etc.) or moved out of eye-sight (e.g. to another room) when a foreign officer is present.

i. In a field environment, foreign officers will only be able to operate on systems and have information that is releasable to their respective country IAW intelligence sharing agreements (i.e. NATO, FVEY) and case-by-case approvals for foreign disclosure. US-only systems (JCR, appropriate air pictures) may have to be sanitized for command post operations to incorporate the foreign officer. All information is subject to the foreign disclosure process.

6. Required Reporting.

a. Any MPEP exchange officer must prepare a mid-tour and end-of-tour report for the USAREUR MPEP office.

b. There is no formal report required from foreign officers on temporary exchange. However, the contact officer and alternate contact officer must conduct an informal debriefing with the G2 or S2 SSO.

c. All personnel are required to immediately report suspicious behavior by exchange officers to their S2 or G2 SSO for further investigation.

7. Military Personnel Exchange Program (MPEP). At present, 10th AAMDC is pursuing a recurring MPEP exchange at the O-4 (NATO OF-3) level for up to two years' duration with the United Kingdom's 7th Air Defence Group to begin in winter 2020 or summer 2021. The information below will take effect upon approval of the exchange by both the UK General Staff and HQDA.

a. MPEP Exchange Officer Duty Position.

(1) Duty Title: G5 Plans Officer

(2) Location: 10th AAMDC Headquarters, Rhine Ordnance Barracks, Germany

AECG-AMD

SUBJECT: 10th AAMDC Command and Policy Letter #6, Foreign Military Exchange Policies, Procedures, and Requirements

(3) Duty Description: Serves as G5 plans officer with primary responsibility for organizing, executing, and assessing the command's outreach and engagements with Allies, Partners, and NATO entities. Assists G5 in developing new concepts and initiatives for testing and implementation, with a particular emphasis on concepts and initiatives that enable and prepare the command to operate effectively against emerging and future threats.

b. Certification: The MPEP Exchange Officer must sign a certification statement prepared by the USAREUR FDO responsible for MPEP within fifteen (15) days of arrival. This certification is derived from a USAREUR memorandum of agreement with the United Kingdom, and serves as a contract of responsibility between the two parties.

c. Conditions and Limitations.

(1) MPEP Exchange Officers cannot be assigned to serve as the sole representative of the 10th AAMDC to any conference, training exercise, or activity. They will not serve as contracting officers. They cannot hold any position that requires exercising responsibilities reserved by law or regulation to an officer of the United States Government, specifically the Uniformed Code of Military Justice.

(2) MPEP Exchange Officers will not have unescorted access to classified environments or documentation. They must be escorted through all environments/office space that has open storage of classified material, or operating SIPR computer systems.

d. MPEP Personnel Administration:

(1) Rating Scheme: The MPEP Exchange Officer will be rated annually on a DA Form 67-9 by the 10th AAMDC G5, and senior rated by the 10th AAMDC Deputy Commander. Any changes to this rating scheme must be approved by the USAREUR MPEP Office.

(2) Health Care: The MPEP Exchange Officer and his or her spouse and children will have access to DoD healthcare in accordance with North Atlantic Treaty Organization standards and AR 40-400.

(3) Misconduct: The MPEP Exchange Officer will adhere to all DoD, DA, and local command policies. If policy violations occur, the contact officer will provide a written report to the USAREUR MPEP Office and FDO, with a recommendation on whether to continue or terminate the exchange officer's tenure.


(4) Awards: Any awards will be processed through the 10th AAMDC G1 to the USAREUR G1, and ultimately through the HQDA G1. For foreign military personnel, any US Army award up to the Legion of Merit requires up to six months due to processing and counterintelligence investigation requirements. It is prudent to submit an end of tour award early, to satisfy this extensive time requirement.

(5) Deployment: 10th AAMDC will inquire with the USAREUR MPEP Office to ascertain HQDA's approval of the MPEP Exchange Officer's availability for deployment in the event of contingency operations.

AECG-AMD

SUBJECT: 10th AAMDC Command and Policy Letter #6, Foreign Military Exchange Policies, Procedures, and Requirements

8. The point of contact for this memorandum is MAJ Rory McGovern, 10th AAMDC Deputy G5, rory.m.mcgovern.mil@mail.mil.



GREGORY J. BRADY
Brigadier General, USA
Commanding