



REPLY TO
ATTENTION OF:

DEPARTMENT OF THE ARMY
HEADQUARTERS, 8TH ARMY
UNIT #15236
APO AP 96205-5236

EACG

03 NOV. 2011

MEMORANDUM FOR All 8th Army and Subordinate Command Personnel

SUBJECT: 8th Army Command Policy Letter #49, Operations Security (OPSEC) Policy

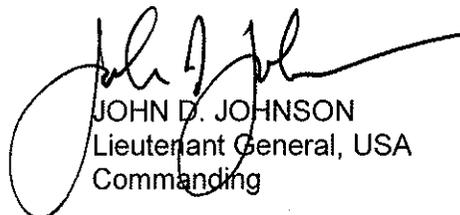
1. This policy, effective immediately, remains in effect until rescinded or superseded.
2. References:
 - a. Department of Defense (DoD) Directive 5205.02, DoD Operations Security (OPSEC), 6 March 2006.
 - b. DoD Manual 5205.02-M, DoD Operations Security (OPSEC) Program Manual, 3 November 2008.
 - c. Joint Publication 3-13.3, Operations Security, 29 June 2006.
 - d. Army Regulation 530-1, Operations Security, 19 April 2007.
 - e. Combined Forces Command Operations Publication 3-4.9, Operations Security, 1 January 2007.
 - f. United States Forces, Korea Command Policy Letter #24, Operations Security (OPSEC).
 - g. Army in Korea Regulation 530-1, Operations Security, 9 January 2010.
3. This policy applies to 8th Army military members, DoD civilian employees, contractors, 8th Army dependants, and all those supporting 8th Army operations.
4. The primary purpose of the OPSEC program is to ensure the Command practices OPSEC to deny critical information to adversaries. The OPSEC process is a proven means to protect operations and planning information and will support the 8th Army warfare mission and operations objectives. Proper use of the OPSEC process will minimize conflicts between operational and security requirements. The OPSEC process requires that each operation be individually analyzed to determine the level of acceptable risk. Therefore, commanders must actively participate in the program by providing guidance and decisions to ensure continuous and thorough attention by all staff levels to assure proper protection of critical information and OPSEC indicators. Within HQ 8th Army, subordinates, and supporting commands, OPSEC will—
 - a. Be used to deny enemy intelligence gathering organizations information about friendly capabilities, intentions, and operations. We will accomplish this by controlling or protecting indicators associated with planning and conducting military operations.

EACG

SUBJECT: 8th Army Command Policy Letter #49, Operations Security (OPSEC) Policy

- b. Be integrated into the planning and execution phases of all military operations.
 - c. Include frequent evaluations and identification of Essential Elements of Friendly Information (EEFI). Each OPLAN should be evaluated and refined annually in order to develop critical information specific to that plan.
 - d. Be a consideration in the day-to-day operations of each organization.
5. Securing classified information is well understood and enforced. However, everyone must understand that sensitive unclassified information must also be protected and denied to our adversaries. Small bits of information can be fused together to reveal a larger picture.
6. Each Soldier, DoD civilian employee and contractor, at all levels, must protect both classified and sensitive unclassified information that could potentially be exploited by our adversaries. We must make OPSEC a priority and integrate OPSEC practices into our daily activities.
7. The successful enforcement of OPSEC procedures will prevent serious injury and possibly death of 8th Army service members; damage to our key infrastructures; or loss of critical technological capabilities.
8. The point of contact for the policy is MAJ Yokeitha A. Ramey, 723-4831, 8th Army OPSEC Program Manager.

- 2 Encls
- 1. Critical Information List (CIL)
 - 2. 8th Army OPSEC Protective Measures



JOHN D. JOHNSON
Lieutenant General, USA
Commanding

DISTRIBUTION:
A

Enclosure 1

8th Army Critical Information List

1. General Officer and Civilian Equivalent Movements (Travel Itineraries and Schedules)
2. Exercise activities, scenarios, events and results
3. Force Compositions, Status, Movements, and Locations
4. Logistics movements and Locations
5. Presence or Employment of New/Improved Technology
6. Estimates in the Effectiveness of Operations
7. Telephone and Radio Communications Equipment, Procedures, Infrastructure and Computer Network IPs
8. Personal Information: SSN, Financial, Legal, Family

Enclosure 2

8th Army OPSEC Protective Measures

The following OPSEC measures should be integrated in daily operations by all 8th Army personnel. Through vigilance in these six areas, we can mitigate or reduce many disclosures of sensitive information and operational indicators. Based on unique mission requirements and activities, additional measures will likely be needed to fully protect command and unit critical information.

1. Computer Network Activities:

a. Use the appropriate secure network (i.e., SIPRNET, CENTRIXS-K) anytime you process classified information. This is also the preferred method when working on or transmitting sensitive unclassified information.

b. As a minimum, encrypt NIPRNET email using your Common Access Card (CAC) every time you pass sensitive unclassified information and unit Critical Information. This information should never be transmitted using commercial internet service providers, period.

c. To protect sensitive unclassified and potentially classified information, properly label and control removable computer media (i.e., CD/DVD, removable hard drive, etc).

2. Telephone and Radio Communications:

a. Use a secure telephone (STE, VoIP, or vIPer) or encrypted radio for passing sensitive information.

b. Do not attempt to "talk around" classified or sensitive information on an open line.

c. Announce "phone up/down" and use push-to-talk handsets properly.

d. If cellular phones are authorized in the facility, power down (remove the battery) and properly store them in designated area prior to entering a classified working area, command post/operations center, or where classified or sensitive discussions may take place.

3. Public Information Releases:

a. Get approval from your chain of command before talking with any media representative. Refer all requests for information to the Public Affairs Officer (PAO).

b. Do not post sensitive operational information or information that could be used to target friendly forces or family members to official publicly accessible or personal websites, weblogs, or chat rooms.

c. Keep sensitive discussions in the workplace.

d. Conduct periodic web content review in coordination with PAO IAW unit policies.

4. Document Disposal: Shredded papers are of no use to our adversaries. Shred all documents or paper that are work-related or contain personal information.

5. Know Command Critical Information: Know what to protect; post the command/unit Critical Information List (CIL) at all desks and workstations where information is processed and transmitted.

6. Immediately report all suspicious activities, persons, and objects to security manager and OPSEC officer.