



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY

2ND INFANTRY DIVISION

UNIT 15041

APO, AP 96258-5041

EAID-CG

JAN 23 2012

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Letter #7-1, Operations Security (OPSEC)

1. References.

- a. Department of Defense Directive (DoDD) 5205.02, DoD Operations Security, 6 March 2006.
- b. DoD Manual 5205.02-M, DoD Operations Security Program Manual, 3 November 2008.
- c. Joint Publication 3-13.3, Operations Security, dated 29 June 2006.
- d. Army Regulation 530-1, Operations Security, dated 19 April 2007.
- e. Army in Korea Regulation 530-1, Operations Security, 9 January 2010.
- f. USFK Command Policy Letter #24, Operations Security, 17 October 2011.
- g. 8th Army Command Policy Letter #49, Operations Security, 03 November 2011.

2. This policy is effective immediately and remains in effect until rescinded or suspended.

3. Applicability. This policy applies to all 2ID military members, DoD civilian employees, contractors and technical representatives, 2ID dependents and all those supporting 2ID operations.

4. OPSEC is a command responsibility. Every member of the Division must practice proper OPSEC procedures as a continuous disciplined habit. Lives and mission accomplishment are at risk and proper OPSEC reduces the risk – significantly. I charge commanders and leaders at every level to train your forces and organizations to enforce a disciplined application of OPSEC countermeasures in all your daily activities.

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. Sensitive or Critical Information that requires protection includes (but is not limited to):

- a. Privacy Act Information or personal information regarding unit personnel or families.

EAID-CG

SUBJECT: Policy Letter #7-1, Operations Security (OPSEC)

- b. Documents marked "For Official Use Only" or "Controlled Unclassified Information."
 - c. Unit status, capabilities, vulnerabilities, limitations, and force protection measures.
 - d. Installation maps indicating key nodes, critical facilities, and infrastructure.
 - e. Communications and information system/network procedures and vulnerabilities.
 - f. Detailed travel itineraries and agendas of senior leadership.
6. I direct each Soldier, Airman, DoD civilian employee and contractor, at all levels, to 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. Use secure communications whenever possible, minimize non-secure voice and digital, non CAC/PKI communications, and apply the general OPSEC protective measures listed in the enclosure and those developed and implemented within individual units.
7. The successful enforcement of OPSEC procedures will prevent serious injury and possibly death of 2ID service members, damage to our key mission essential equipment or logistics stocks, and loss of a critical technology capability to our adversary.
8. Report the loss of sensitive unclassified information to your unit OPSEC Officer.
9. The point of contact for this policy letter is 2ID G7 OPSEC Officer, DSN 732-9511.



EDWARD C. CARDON
Major General, USA
Commanding

Encl

A - 2ID OPSEC Protective Measures

B- Critical Information List (CIL)

DISTRIBUTION:

A

EAID-CG

SUBJECT: Policy Letter #7-1, Operations Security (OPSEC)

Enclosure A: 2ID OPSEC PROTECTIVE MEASURES

Incorporate the following OPSEC measures into daily operations. Through vigilance in these five areas, we can mitigate or greatly 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 a secure network (i.e., CENTRIXS, SIPRNET) anytime you process classified information. This is also the preferred method when working on or transmitting sensitive unclassified information.

b. As a minimum, digitally sign and encrypt NIPRNET email using your Common Access Card (CAC) every time you pass sensitive unclassified information and unit Critical Information. Do not transmit using commercial internet email service providers (e.g. Gmail, Hotmail, or Yahoo).

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

2. Telephone and Radio Communications:

a. Use a secure telephone or encrypted radio for passing sensitive information. When using a STE (Secure Terminal Equipment), activate the cryptographic card for secure communication.

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. Do not engage in non-secure phone calls in command posts during classified briefings and near classified or sensitive discussions.

e. If mobile phones are authorized in the facility, deactivate them prior to entering a classified work 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 Office.

EAID-CG

SUBJECT: Policy Letter #7-1, Operations Security (OPSEC)

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, blogs, chat rooms, photo sharing websites, or social media sites/social networking sites (SNS).

c. Keep sensitive discussions in the workplace.

4. Documents:

a. Shred any document or paper that is work-related or contains personal information. Limit the use of social security numbers to only what is required.

b. All documents classified SECRET, including REL-ROK, or higher must be shredded with a cross-cut shredder.

c. Secure sensitive unclassified documents (e.g. personally identifiable information).

d. Identification cards, common access cards, access badges, etc. must be safe guarded. Secure these items when departing the facility for which they were intended.

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

EAID-CG

SUBJECT: Policy Letter #7-1, Operations Security (OPSEC)

Enclosure B: 2ID CRITICAL INFORMATION LIST (CIL)

1. General Officer and Civilian equivalent movements (travel itineraries & schedules).
2. Exercise activities, scenarios, events, and results.
3. Force composition, movement and locations.
4. Logistics caches or resupply movement and locations.
5. Presence or employment of new or improved technology.
6. 2ID vulnerabilities and weaknesses.
7. Estimates in the effectiveness of operations.
8. Intelligence capabilities, purposes, or intent.
9. Communications equipment, procedures, & infrastructure:
 - a. UserID and passwords.
 - b. Frequencies and call signs.
 - c. Vulnerabilities.
10. Personal Information: SSN, Family, financial, legal, medical etc.