



DEPARTMENT OF THE ARMY  
2d ENGINEER BRIGADE  
724 POSTAL SERVICE LOOP #5000  
JOINT BASE ELMENDORF-RICHARDSON, ALASKA 99505-5000



REPLY TO  
ATTENTION OF

APVR-ENG-CO

26 September 2011

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Operations Security (OPSEC) Policy Letter #16

1. Reference:

- a. AR 530-1 Operations Security (OPSEC), 19 Apr 07
- b. USARPAC 530-1, OPSEC, Mar 07.
- c. USARAK 530-1, OPSEC, 30 Mar 04.
- d. USARAK Command Inspection Program, May 07.
- e. USARAK/USAG-AK Security SOP, Apr 04.
- f. USARAK CG Policy #0-16, United States Army Alaska (USARAK) Operations Security (OPSEC), dated 12 Aug 2010.

2. Purpose. The purpose of this memorandum is to provide Commanders and leaders with the 2d Engineer Brigade Commander's OPSEC Vision and Core OPSEC Program Requirements.

3. The 2d Engineer Brigade Commander's OPSEC Vision. Operational security is critical to our mission and I expect Commanders to remain engaged with their OPSEC programs. Commanders will integrate OPSEC into all operations, activities and events, ensuring Soldiers, Families, DA civilians, and DOD contractors receive the requisite education and guidance needed to actively participate in protecting unit critical and sensitive information at all times.

4. Commander's Core OPSEC Program Requirements.

a. Commanders will appoint primary and alternate unit OPSEC Officers in the appropriate grade and position IAW AR 530-1.

b. Commanders will develop and maintain a comprehensive and aggressive OPSEC plan IAW AR 530-1.

c. Commanders will annually approve and publish their Command Information List (CIL) and Essential Elements of Friendly Information (EEFI) to unit personnel.

d. Commanders will report OPSEC violations to the Brigade S2/S3, who will forward the reports to the USARAK G-3, utilizing the USARAK OPSEC report format.

e. Commanders will continuously evaluate the OPSEC threat and develop OPSEC countermeasures to protect critical information throughout all phases of operations.

f. Commanders will ensure newly assigned personnel receive reception and integration OPSEC training within 30 days of arrival. Areas addressed shall identify the unit OPSEC Officer, reporting suspect OPSEC violations, OPSEC threats, vulnerabilities, Commander's Critical Information Requirements (CCIR), CIL, EEFI, and unit OPSEC Counter Measures.

g. Commanders will ensure all personnel in their command receive Annual OPSEC Level I Awareness Training. Units develop functional and aggressive OPSEC training plans, ensuring all assigned personnel, Family Readiness Group members, and Families receive annual and quarterly OPSEC awareness training. Units ensure OPSEC training is incorporated into training calendars and schedules and that training records reflect this annual requirement.

h. Leaders, Soldiers, and Family members all have a responsibility to understand what operational information should be protected. With the prevalence of social networks and blogs on the web this is now a global vulnerability which requires our attention.

i. OPSEC Reporting. Submit OPSEC reports addressed IAW USARAK 530-1 and USARAK Annual Training Guidance to USARAK G-3, OPSEC Officer NLT 15 September each year.

j. OPSEC Violations. Suspected OPSEC violations will be reported to the unit OPSEC Officer, unit leadership, Installation Security Intelligence Office (ISIO), or USARAK OPSEC Officer.

k. Commanders develop and execute an aggressive OPSEC awareness campaign. Units can secure or request OPSEC training and awareness resources by visiting the USARAK OPSEC website at <https://portal.usarpac.army.mil/usarak/OPSEC/Default.htm>, or the Interagency OPSEC Support Staff at <http://www.iooss.gov/>.

5. Additional OPSEC information or comments can be sent to the Brigade S2 @ (907) 384-2725.

THOMAS J. ROTH  
COL, EN  
Commanding

**DISTRIBUTION:**

2d Engineer Brigade Command Teams