



HEADQUARTERS, UNITED STATES FORCES KOREA

UNIT #15237
APO AP 96205-5237

REPLY TO
ATTENTION OF:

FKCC

17 OCT. 2011

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: United States Forces Korea (USFK) Command Policy Letter #5, Operations Security (OPSEC)

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 This policy, effective immediately, remains in effect until rescinded or superseded.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, 6 March 2006.
 - b. Joint Publication 3-13.3, Joint Operations Security, 29 June 2006.
 - c. Combined Forces Command Operations Publication 3-4.9, Operations Security, 1 January 2007.
3. This policy applies to all USFK military members, DoD civilian employees, USFK-invited contractors, technical representatives, USFK dependants, and all those supporting USFK operations.
4. OPSEC is a command responsibility. Every USFK member must know and practice proper OPSEC procedures as a continuous, disciplined habit. Lives and mission accomplishment are at risk and proper OPSEC reduces the risk – significantly. 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.
 - 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.

This letter can be found at <http://www.usfk.mil>

FKCC

SUBJECT: United States Forces Korea (USFK) Command Policy Letter # 5, Operations Security (OPSEC)


5. Unclassified E-mail. All personnel must have the capability to digitally sign and encrypt official e-mail containing sensitive and/or critical information. A good rule of thumb is that unless you want to read it in the public media, you need to encrypt it. Refer to paragraph 4 for unclassified information that should be encrypted.

6. As the popularity of Social Networking Sites (SNS) continues to increase as a means of mass communication, they also pose significant OPSEC risks. Practicing good OPSEC when using SNSs will minimize these associated risks to our mission. Remember, think before you post. Once the information is out there, you can't get it back.

7. I direct each Soldier, Sailor, Airman, Marine, DoD civilian employee and contractor, at all levels, to protect both classified and sensitive unclassified information that could potentially be exploited by our adversaries.

8. The successful enforcement of OPSEC procedures will prevent serious injury and possibly death of USFK service members and our coalition partners; damage to our key mission essential facilities, equipment, or logistics stocks; or loss of a critical technology capability.

9. The point of contact for this policy letter is J39 Information Operations Division, OPSEC Branch, DSN 723-2149 or email, OPSEC@korea.army.mil.


JAMES D. THURMAN
General, U.S. Army
Commander

DISTRIBUTION:

A