HEADQUARTERS, UNITED STATES FORCES KOREA
UNIT #15237
APO AP 96205-5237

FKCC

02 JAN 2014

MEMORANDUM FOR SEE DISTRIBUTION

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

1. This policy applies to all USFK military members, DoD civilian employees, USFK-invited contractors, technical representatives, USFK dependants, and all those supporting USFK operations.

2. OPSEC is a shared responsibility. Every USFK member must know and practice OPSEC procedures as a continuous, disciplined habit. Lives and mission accomplishment are at risk, especially in a foreign environment, and good OPSEC reduces the risk – significantly. Every USFK organization must identify the specific critical information it must protect such as operational patterns, intentions, capabilities, vulnerabilities, and limitations. These friendly pieces of information can help an enemy, so we must protect them. The convenience, speed, and reach of cyber activities greatly benefit friendly forces; however, our adversaries are also able to leverage these capabilities to gather information from a distance.

3. I charge commanders and leaders at every level to identify your critical information, assess the threats and vulnerabilities, and train your forces to enforce disciplined application of daily countermeasures to protect those operations.

4. Securing classified information is well understood and enforced; however, 90% of intelligence gathering involves unclassified indicators. Everyone must understand the impact of lax information handling that can occur over time. Small pieces of information can be pieced together to reveal the larger picture. Sensitive or Critical Information that requires protection includes (but is not limited to):

- Privacy Act Information or personal information regarding unit personnel or families
- Documents marked "For Official Use Only" or "Controlled Unclassified Information"
- Unit status, capabilities, vulnerabilities, limitations, and force protection measures
- Installation maps indicating key nodes, critical facilities, and infrastructure
- Communications and information system/network procedures and vulnerabilities
- Detailed travel itineraries and agendas of senior leadership

5. Social Networking Sites (SNS) have become a part of daily life; they also pose significant OPSEC risks. Our adversaries are keenly interested in our information and monitor public-facing sites to glean sensitive information needed to disrupt our mission or cause harm. It is essential to inform our friends and significant others of sensitive

information they should avoid sharing on such sites. Practicing good OPSEC when using SNS will minimize vulnerabilities. Remember to think before you post.

6. This policy directs every Soldier, Sailor, Airman, Marine, DoD civilian employee and contractor to protect both classified and unclassified information against possible exploitation. Make OPSEC part of your thought process, and integrate mitigation measures into your daily activities. Apply the general OPSEC protective measures listed in the enclosure and those developed and implemented within individual units.

7. The successful implementation of OPSEC procedures will prevent serious injury and 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.

8. This policy remains in effect until rescinded or superseded.

9. Point of contact is J39 Information Operations Division, OPSEC Branch, DSN 723-2149.

//ORIGINAL SIGNED//
CURTIS M. SCAPARROTTI
General, U.S. Army
Commander

Encl
USFK OPSEC Protective Measures

DISTRIBUTION:
A

References.
a. DoD Directive 5205.02E, DoD Operations Security Program, 20 June 2012.
b. Joint Publication 3-13.3, Operations Security, 04 January 2012.
c. CFC Operations Publication 3-4.9, Operations Security, 30 June 2012.

USFK OPSEC Protective Measures

Implement the following OPSEC measures in daily USFK operations. Vigilance in these seven areas will substantially mitigate or reduce many unintended 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., CENTRIXS-K, SIPRNET) when processing classified information. This is also the preferred method when working on or transmitting sensitive unclassified information.

b. Encrypt NIPRNET email using your Common Access Card (CAC) every time you pass sensitive unclassified information and unit critical information. ***Never*** transmit sensitive unclassified information using commercial internet service providers.

c. Properly label and control removable computer media (e.g., CD/DVDs, disk, removable hard drives).

2. Telephone and Radio Communications:

a. Use a secure telephone (STE or VoIP) 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.

d. If cell phones are authorized in a facility, deactivate them (remove the battery) prior to entering a classified working area, command post/operations center, or where classified or sensitive discussions may take place. Cell phones can become listening devices.

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.

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

c. Keep sensitive discussions in the workplace.

4. Social Networking Sites:

a. Assess risk before posting information about you or your organization. Post in the past. Never post sensitive or critical information. Post information as if privacy or filtering settings do not exist within the site's functionality.

b. Set privacy settings to protect personal information and control how much is revealed about you and to whom it is revealed.

c. Before accepting a friend/connection request, directly confirm the request with them. This ensures that the involved accounts are neither compromised nor impersonated.

d. Be selective about which third-party applications to add to your profile. These applications could contain malicious code that can compromise your computer or your organization's network. Use location-aware applications with caution.

e. Follow computer security guidelines. Do not use official email addresses on these sites and secure your password.

5. Document Disposal: Properly shredded papers are of no use to our adversaries. Shred all documents and work-related paper that contains personal information.

6. Know your Commander's Critical Information: Know what to protect. Post command/ unit Critical Information List at all desks and workstations where information is processed and transmitted.

7. Immediately report all suspicious activities, persons, and objects.