



HEADQUARTERS, UNITED STATES FORCES KOREA

UNIT #15237
APO AP 96205-5237

REPLY TO
ATTENTION OF:

11 SEP 2008

FKCC

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: US Forces Korea (USFK) Command Policy Letter #13, Information Assurance

1. This letter supersedes USFK Command Policy #13, 26 Jun 06. It remains in effect until specifically rescinded or superseded.
2. References.
 - a. DoD 5200.1R, Information Security Program, Jan 1997.
 - b. CJCSM 6510.01 Information Assurance Computer Network Defense(CND), Mar 2005.
 - c. DoD 8500.1, Information Assurance, Oct 2002.
 - d. DoDI 8500.2, Information Assurance Implementation, Feb 2003.
 - e. CFC Operations Plan (OPLAN), Annex C, Appendix 11, Tab C, 31 May 2004.
3. This policy applies to all USFK military members, civilian employees, invited and local contractors, and technical representatives, whether assigned permanently, temporary duty, rotational duty, or on leave/pass status in Korea.
4. Component commanders must ensure that our information systems are protected and defended against exploitation, denial of service, and unauthorized access. This policy is designed to provide general guidance on IA, managing removable media (USB/Thumb Drives, CDs, DVDs, Diskettes, etc.) and managing unclassified E-mails.
5. All personnel are charged with adhering to the specific policy guidance below.
 - a. General Information Assurance.
 - (1) Protect Information. All personnel will safeguard data within the computing environment and ensure all data is appropriately labeled, handled, stored, transported and disposed of IAW ref 2a. Personnel and organizations will immediately notify their technical chain and Information Assurance support channels when irregular computer activity is suspected.
 - (2) Defend Systems and Networks. Everyone must recognize, react and respond to threats, vulnerabilities and deficiencies. Information Systems Service Providers will ensure that access is controlled, and all systems/networks incorporate defense-in-depth strategies and tools.

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

FKCC

SUBJECT: US Forces Korea (USFK) Command Policy Letter #13, Information Assurance

(3) Create an IA-Empowered Workforce. Organizational commanders will establish, resource, and implement Information Assurance training and certification programs.

b. Removable Storage Media (USB/Thumb Drives, CDs, DVDs, Diskettes, etc.). All personnel must mitigate the risk of compromising classified information stored on removable storage media. These media have multiple uses and their small size and adaptability can result in loss of accountability and inappropriate cross net (NIPR to SIPR, etc.). Recent revelations of this loss of accountability outside the gate in Baghram, Afghanistan highlight the requirement for focused command oversight. Commanders and Designated Approval Authorities will allow the specific use of removable media on an exception only basis, and institute rigid control mechanisms for accounting, handling, labeling, transporting and disposing of this classified media.

c. Unclassified E-mail. All personnel must have the capability to digitally sign and encrypt official E-mail containing sensitive and/or critical information, or other information that could potentially be exploited by unfriendly enterprises or an adversary. A good rule of thumb is that unless you want to read it in the public media, you need to encrypt it. Unclassified information which should be encrypted on our NIPRNET may include:

(1) Information under the Privacy Act, and the Health Insurance Portability and Accountability Act of 1996.

(2) Information for Official Use Only (FOUO).

(3) Unclassified unit status, capabilities, vulnerabilities (i.e., facilities, information systems, force protection).

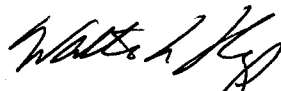
(4) Travel itineraries for key leadership personnel (i.e., GO's, SES's, or above).

(5) User names/passwords.

(6) Information found in routine DoD payroll, finance, logistics, and personnel management systems.

(7) All E-mail sent to and from the Commander, USFK will be digitally signed and encrypted. Encrypted E-mails received from the commander will not be forwarded to anyone unencrypted.

6. The POC for this policy is USFK, J6, IA Division at 723-3659 or j6sctry@korea.army.mil.


WALTER L. SHARP
General, U.S. Army
Commander

DISTRIBUTION:

A