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 #2, Antiterrorism and Force Protection

1. This policy applies to members of the U.S. Armed Forces when in the Republic of Korea (ROK), which includes personnel on permanent change of station (PCS), temporary duty (TDY), pass or leave status, DoD civilians, DoD invited contractors/technical representatives, and their family members and visiting guests.

2. The potential of antagonist behavior against USFK personnel requires everyone to be vigilant. Personnel associated with the U.S. Government are often targets for terrorist activity. One of the most important individual protective measures we can take is to develop personal habits and practices that frustrate terrorist attempts to determine our nationality, profession, individual job responsibilities, association, and overall importance to the Department of Defense.

3. Particularly in Korea with a complex threat environment, demands an added vigilance and discipline at all times. We must assume that there is high potential U.S. personnel and facilities are under periodic or continued surveillance. Additionally, there is potential for sudden violent demonstrations, which could result in direct contact with subversive agents of other countries or trans-national terror organizations. In other words, **be prepared for the unexpected!**

4. Force protection is a command responsibility. Our leaders will brief all personnel and family members on personal security and safety procedures on a routine basis, with particular importance placed on the first 30 days of arrival in Korea. Also, all personnel are the first line of defense for our force protection and anti-terrorism programs. With this in mind, report suspicious or overt activities to military police, unit intelligence officers, the Subversion and Espionage Directed Against the US Army (SAEDA) hotline (DN 723-3299), your local law enforcement office, or chain of command as soon as possible. Activities we should watch out for include: individuals observing or photographing installations and activities; attempts to circumvent physical security measures or gain access into our computer networks; or attempts to elicit information by questioning USFK personnel or their families. Always remain non-committal and immediately report contacts by suspicious persons or activities.

5. Strictly adhering to all published security measures can effectively enhance command anti-terrorism and force protection postures. For example, practicing good

Operations Security (OPSEC) and following Information Assurance (IA) guidelines are crucial in combating terrorist activities and other asymmetric and web-based threats. Know your security responsibilities and OPSEC protective measures to become a “hard target.” By using secure and encrypted communications, controlling access to USFK networks, destroying personal and work-related papers, concealing operational indicators, and varying routes and activities, USFK personnel can protect critical information the adversary requires to plan and execute terrorist activities.

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

7. Point of contact is USFK J34, Antiterrorism/Critical Infrastructure Protection Division, (DSN) 723-3691.

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

DISTRIBUTION:
A

2. References.
a. Department of Defense (DoD) Instruction 2000.16, DoD Antiterrorism (AT) Standards, December 8, 2006 (Change 2).
b. DoD Instruction 2000.12, DoD Antiterrorism (AT) Program, March 1, 2012.
c. DoD O-2000.12-H, DoD Antiterrorism Handbook, February 1, 2004.
d. USFK Operations Order 5050-11, Antiterrorism/Critical Infrastructure Protection, June 1, 2011.