



REPLY TO  
ATTENTION OF

DEPARTMENT OF THE ARMY  
HEADQUARTERS, III CORPS AND FORT HOOD  
1001 761ST TANK BATTALION AVENUE  
FORT HOOD, TEXAS 76544-5000

**COMMAND POLICY**  
**CBRNE-01**

AFZF-CBRNE

OCT 14 2011

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Commanding General's Policy Letter Operations Security (OPSEC)

1. **APPLICABILITY.** This policy applies to all III Corps and Fort Hood service members, Department of Defense civilians, and all contract personnel assigned to and under the operational control of Fort Hood, Texas. This policy applies to all subordinate commanders, units, and tenant activities across the Fort Hood Military Reservation.

2. **STATEMENT OF PURPOSE AND NECESSITY.**

a. The threat is real! We are involved in an information war. Adversaries monitoring our activities, conversations, and communications use various tactics to gain information that can be used against us. They are surfing the internet, reading web blogs, searching our social media and even talking to us to gain access to our critical information, photographs and structure. This enables the adversary to counter the Commanding General's military decision-making process and hinder his overall success. It also enables the adversary to manipulate photographs and data to further their cause. We must maintain a constant awareness of our actions, be aware of what we post on the public domain, use secure voice phones to the maximum extent possible, and cease "shop talk" in environments where individuals without the need to know might overhear.

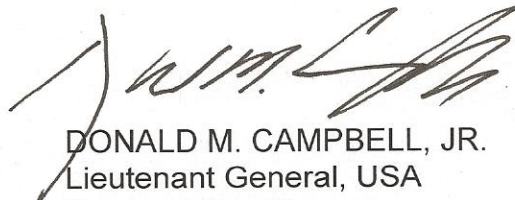
b. OPSEC is our first line of defense against hostile intelligence collection efforts. It provides commanders with a process to identify and evaluate issues that can negatively affect the outcome of their overall mission. Additionally, OPSEC provides a means to identify appropriate measures to mitigate the risks we are facing. The development and implementation of OPSEC measures provide an efficient review of our activities and how these activities may inadvertently provide critical information to our adversaries. OPSEC, therefore is the key means of preventing, detecting and subverting an adversary's indirect actions on our mission. OPSEC awareness and countermeasures must continue to evolve as our information operations and technology advance.

AFZF-CBRNE

SUBJECT: Commanders Policy Letter Operations Security (OPSEC)

3. POLICY. This policy letter, AR 530-1, and the III Corps OPSEC Program require that commanders at all levels are responsible for ensuring their units or organizations integrate and implement OPSEC measures to protect their critical information in every phase of all operations or activities. The III Corps OPSEC Program Manager will establish the III Corps OPSEC Program to include an OPSEC Working Group that will stay abreast of any changes within the OPSEC Program while working together with the Fort Hood Garrison and Fort Hood tenant organizations to ensure the success of the program. Each commander (battalion and above) will establish and maintain a documented OPSEC program that will support the III Corps OPSEC Program. It is also the responsibility of each individual assigned to III Corps to support the III Corps OPSEC Program.

4. EXPIRATION. This III Corps Command Policy Memorandum will remain in effect until superseded or rescinded.



DONALD M. CAMPBELL, JR.  
Lieutenant General, USA  
Commanding General

DISTRIBUTION:  
IAW FW Form 1853: A