



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
UNITED STATES ARMY FORCE MANAGEMENT SCHOOL
5500 21ST STREET, BUILDING 247, SUITE 1400
FORT BELVOIR, VIRGINIA 22060-5923

OCT 01 2015

DAMO-FMS

MEMORANDUM FOR Staff and Faculty of the Army Force Management School
(AFMS)

SUBJECT: AFMS Policy Letter #2 – Essential Elements of Friendly Information (EEFI)
Operational Security Program

1. References:

- a. ALARACT OPSEC Message, 221224Z May 2006, subject: Guidance on the Proper Use of Hardware and Software.
- b. AR 530-1, Operations Security, 19 Apr 2007.
- c. AR 380-5, DA Information Security Program, 29 Sep 2000.

2. With the advent of the computer, the picture cell phone, the internet and the frequent substitution of face to face meetings with email and electronic collaborations, the potential for inadvertent disclosure of sensitive information concerning our operations has greatly increased.

3. To more clearly define the information that we must protect from our adversaries, we have developed a number of EEFI for the school:

- a. Location, schedule, and security arrangements for senior leaders and visiting VIPs.
- b. Security, disposition, and location of information networks.
- c. Assets/VIPs deployed and the purpose, itinerary, and destination of the deployment.
- d. Location of mission essential vulnerable areas, high risk targets, and the measures employed to secure them.
- e. Measures to mitigate force protection vulnerabilities.
- f. Force Protection Condition Measures.
- g. Security measures planned or implemented for high visibility, high personnel concentration events.

DAMO-FMS

SUBJECT: AFMS Policy Letter #2 – Essential Elements of Friendly Information (EEFI)
Operational Security Program

4. EEFI are critical aspects of a friendly operation that, if known by our adversaries, could compromise, lead to failure, or limit success of that operation and therefore must be protected from enemy detection.

5. Effective immediately, information pertaining to our EEFI will be treated at a minimum as "For Official Use Only", meaning that such information will not be transmitted by non-secure means:

a. Data determined to be sensitive but unclassified will, at a minimum, be encrypted using CAC/PKI.

b. Classified information (e.g., CONFIDENTIAL, SECRET, etc.) will be transmitted over a network with a minimum security classification of SECRET (e.g., SIPERNET).

c. Unclassified critical and sensitive operational traffic over a secure network. For the purpose of this memorandum, unclassified critical and sensitive operational traffic will include, but is not limited to, correspondence containing General Officer and Senior Executive Service (SES) overseas travel schedules and all deployed and deploying troop information.

d. If, after reviewing the references and consulting with your security manager, it remains unclear whether the data is appropriate for an unclassified network, restrict transmission to a secure network until authoritative guidance is received. Even where CAC/PKI is used, the NIPRNET is not considered a "secure" network.

6. I expect all individuals at all levels to aggressively enforce this policy.



ALAN C. NOTGRASS
Colonel, U.S. Army
Commandant