



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 05 2017

DAMO-FMS

MEMORANDUM FOR All Army Force Management School (AFMS) Personnel

SUBJECT: AFMS Policy Letter #2 – Critical Information List (CIL) 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, 26 Sep 2014.
- c. AR 380-5, DA Information Security Program, 29 Sep 2000.
- d. AFMS Standard Operating Procedure (SOP), for Operations Security, 21 Sep 2017.

2. All AFMS personnel (staff, faculty and students) must prevent the inadvertent disclosure of sensitive information concerning our operations.

3. To more clearly define the information that we must protect from our adversaries, AFMS recognizes the following as its Critical Information List (CIL) (also contained in reference "d" above):

- a. Current/future operational activities for the Army (missions, strategies and strategic planning, plans, military decision-making products).
- b. Scope of specific operations (movement of forces, force capabilities and limitations, tactics/techniques/procedures and after action reviews).
- c. Critical infrastructure (detailed diagrams of installations, photos showing layouts of buildings, maps, geospatial data, telecommunications, power generation and distribution, banking and finance, transportation, emergency services, locations, control systems, backup systems, operating personnel/workers).
- d. Location, schedule, and security arrangements for senior leaders and visiting VIPs to AFMS and / or location, schedule and security arrangements for senior leader's enroute to forward (deployed) locations.

DAMO-FMS

SUBJECT: AFMS Policy Letter #2 – Critical Information List (CIL) Operational Security Program

e. Force Protection Condition Measures and / or associated vulnerability counter measures (Pentagon, Fort Belvoir and any other sensitive location).

f. Security measures taken or to be taken when visiting dignitaries, senior officials, or high profile/visibility persons.

g. Receipt, storage, transmittal and disposition of Personally Identifiable Information.

4. The CIL items, 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 CIL 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. 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.

7. My point of contact for this action is Mr. Robert Lebron, at comm: (703) 805-2878, email: Robert.lebron.civ@mail.mil


GEORGE LEWIS
Colonel, U.S. Army
Commandant