



DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT BELVOIR
9820 FLAGLER ROAD, SUITE 213
FORT BELVOIR, VIRGINIA 22060-5928

REPLY TO
ATTENTION OF

IMBV-PLO-B

8 August 2012

MEMORANDUM FOR US Army Fort Belvoir Personnel

SUBJECT: Fort Belvoir Policy Memorandum #18, Operations Security (OPSEC)

1. REFERENCE: AR 530-1, Operations Security (OPSEC), 19 April 2007.
2. PURPOSE: To provide guidance to all Fort Belvoir personnel on incorporation of OPSEC practices and procedures into daily activities.
3. APPLICABILITY: This policy applies to all Department of the Army military (active component, and reserve component), civilians and contract personnel at Fort Belvoir. All non-Army organizations or units on Fort Belvoir are encouraged to incorporate this policy into their own command policies in accordance with Department of Defense Directive 5205.02, Paragraph 2.
4. POLICY: Robust OPSEC practices and procedures will be integrated into the day-to-day operations of all Fort Belvoir activities. OPSEC is the only discipline that focuses primarily on unclassified information and activities. It is a security process that must be taken as seriously as the protection of classified information, one hinges on the other.
5. PROCEDURES.
 - a. All Army information products containing sensitive but unclassified information (Critical Information, For Official Use Only (FOUO), Privacy Act Information, etc.) should not be discarded with regular refuse or paper recycling, but should be destroyed with a standard office shredder, tearing, burning, or other method. Critical Information definition and examples are listed at Enclosure 1. All other information that is not considered sensitive but unclassified and is developed as part of our jobs, should be disposed of appropriately.
 - b. FOUO information should be the standard marking for all unclassified products determined to be Critical Information by each directorate in coordination with the OPSEC Program Manager.
 - c. Whenever available, use Secure Telephone Equipment (STE) for voice traffic of even the most innocuous information.

“LEADERS IN EXCELLENCE”

IMBV-PLO-B

SUBJECT: Fort Belvoir Policy Memorandum #18, Operations Security (OPSEC)

d. All Army personnel will consult with their immediate supervisor prior to publishing or posting in any public forum (including newspapers, journals, bulletin boards, the internet, such as email, web-based chat-rooms, logs or "blogs," or social websites, or other forms of dissemination or documentation) information that might contain Critical Information or its indicators. Supervisors will advise personnel to ensure that Critical Information and indicators of Critical Information are not released. Each unit's OPSEC Officer or Coordinator should advise supervisors on means to prevent the release of Critical Information.

e. Information Assurance (IA) is a crucial element of the OPSEC process. IA establishes policies and assigns responsibilities for all users and developers for achieving acceptable levels of IA in the engineering, implementation, operation, and maintenance for all information systems across the US Army Enterprise Info-structure. Do not store or transmit classified information on non-secure telecommunication systems. Official DoD telecommunication systems, including telephones, facsimile machines, computer networks, and modems are subject to monitoring at all times for telecommunications security purposes. All users will report security incidents to the Installation Security Manager (DPTMS) and the Information Assurance Program Manager USA Signal Network Enterprise Center – Fort Belvoir as appropriate.

6. PROPONENT: The Directorate of Plans, Training, Mobilization and Security (DPTMS), OPSEC Program Manager, (703) 805-4001.

Encl



GREGORY D. GADSON
Colonel, FA
Commanding

Critical Information

1. Identification of Critical Information: Critical Information consists of specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment. If we do not properly protect our critical information, someone who is interested in harming us or our operations may gather enough unclassified information to enable their plans. This information could be written documents or conversations overheard in social gatherings. The results could be devastating.

2. The following list includes examples of Critical Information topics, but does not represent an actual Critical Information List as defined in AR 530-1. This list is only to reinforce some types of information that OPSEC protects, including:

- Current and future operations
- Travel itineraries
- Usernames and passwords
- Access/Identification cards
- Operations planning information
- Personal identification information
- Entry/Exit (security) procedures
- Capabilities and limitations
- Address and phone lists
- Budget information, including procurement information or actions
- Building plans
- VIP/distinguished visitor schedules

3. Supervisors will provide unit specific Critical Information lists with each employee's initial 30-day OPSEC training. The Installation Critical Information List is outlined in the Installation OPSEC Plan.