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

11 August 2020

MEMORANDUM FOR US Army Fort Belvoir Personnel

SUBJECT: Fort Belvoir Policy Memorandum #8 – Operations Security (OPSEC) and Critical Information List (CIL)

1. REFERENCES.

a. DoDD 5205.02E (DoD Operations Security (OPSEC) Program), 20 June 2012

b. AR 530-1 (Operations Security), 26 September 2014

c. AR 360-1 (The Army Public Affairs Program), 25 May 2011

d. AR 25-2 (Army Cybersecurity), 4 April 2019

2. PURPOSE. This memorandum establishes OPSEC policy for United States Army Garrison-Fort Belvoir (USAG-FB) based on DoD and Army OPSEC regulations.

3. APPLICABILITY. This policy applies to ALL military personnel, civilian employees and contract personnel assigned or attached to USAG-FB, as well as USAG-FB satellite locations and other activities. All directorates will incorporate this policy into their OPSEC programs to support USAG-FB force protection responsibilities. Partner organizations on USAG-FB are encouraged to adopt this policy into their own command policies.

4. POLICY. Operations Security is everyone's responsibility. OPSEC is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information. It is a methodology that denies critical information to an adversary. Unlike security programs that seek to protect classified information, OPSEC measures identify, control, and protect generally unclassified information that is associated with sensitive operations and activities.

5. PROCEDURES.

a. OPSEC requirements for USAG-FB operational planning and execution.

(1) All USAG-FB staff elements, installations, and directorates responsible for planning missions, activities, or events will designate an OPSEC Coordinator to assist the OPSEC Program Manager with incorporating the OPSEC process into planning and coordination phases of operations. The OPSEC Coordinators will include an OPSEC Annex or Appendix into respective plans and orders with the assistance of the OPSEC Program Manager.

(2) Enclosed is the approved USAG-FB Critical Information List (CIL). Each Staff proponent will incorporate the listed Critical Information and identify what critical information their directorates, teams, sections, and/or detachments must protect to support the execution of the USAG-FB missions and tasks. Partner organizations are encouraged to incorporate USAG-FB CIL into their plans.

b. OPSEC requirements for USAG-FB personnel and day-to-day operations.

(1) Official work products (e.g., presentations not intended for the public, email printouts, electronic and recordable storage media, office correspondence, hand notes, any form of personal information, training schedules or calendars, or working papers) containing critical information **will not** be discarded as regular refuse or paper recycling. Any document containing operational or mission critical information not otherwise classified will be marked as "For Official Use Only" (FOUO) or "Controlled Unclassified Information" (CUI).

(2) Individuals will destroy these types of documents or information in a manner that defeats reconstruction by using a high-security or standard office shredder, tearing into small pieces, or utilizing your command's burn-bag program. Contact the Command Security Manager or OPSEC Program Manager for guidance on what types of documents should be destroyed.

(3) If Secure Telephone Equipment (STE) is available, operational based critical information should be communicated through secure means. When an encryption feature is available on unclassified networks, encrypt e-mail messages containing critical or FOUO information.

(4) All USAG-FB personnel will maintain annual OPSEC certification. In addition, all USAG-FB personnel will consult with their immediate supervisor, OPSEC Officer, or Public Affairs Office (PAO) for an OPSEC review prior to publishing or posting official information in public forums (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). Additionally, any office providing information to the PAO for public release will ensure an OPSEC review is conducted (AR 360–1, Paragraph 5-4).

(5) Prior to responding to Freedom of Information Act (FOIA) requests, an OPSEC review will be accomplished to ensure indicators of critical information are not released.

c. OPSEC coordination with other security programs.

(1) Coordination between OPSEC and traditional security programs helps ensure the protection of unclassified critical information, and classified national security information.

(2) OPSEC and Information Assurance (IA) work together to protect information through policies that achieve acceptable levels of IA in the engineering, implementation, operation, and maintenance of information systems. Official DoD telecommunication systems, including telephones and computer networks, are subject to monitoring at all times for security purposes. All users will immediately report network or cyber security incidents to the Information Assurance Program Manager.

d. Personnel will report any suspected OPSEC incident or violation to their organization OPSEC Officer or security manager for follow-up investigation. Other suspicious elicitation attempts should be reported to the 902d MI Group at (703) 805-3008, or the 1-(800) CALL-SPY hotlines, leaving a message with name and telephone number, and no further details.

6. PROPONENT: The Directorate of Plans, Training, Mobilization and Security (DPTMS) Antiterrorism Officer is the proponent for this policy at (703) 805-5205.

JOSHUA P. SEGRAVES
COL, IN
Commanding

USAG-FB CRITICAL INFORMATION LIST (CIL)

1. The Critical Information List (CIL) includes specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment. Critical information is susceptible to collection by adversaries through indicators (friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information), and vulnerabilities (conditions in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making).

2. The USAG-FB Critical Information List (CIL) is:

a. Information regarding deployment/redeployment of personnel and assets to support real-world missions (i.e. overseas contingency operations).

b. Travel Itineraries of employees and distinguished visitors.

c. Information pertaining to access control, physical security, and protection of installations and critical assets (e.g., personnel, facilities, equipment, or information).

d. Telephonic rosters, addresses and other contact information for employees Personal Identifiable Information (PII).

e. Emergency Response Capabilities.

f. Special Equipment Capabilities and Limitations.