



**DEPARTMENT OF THE ARMY**  
JOINT BASE MYER – HENDERSON HALL  
204 LEE AVENUE  
FORT MYER, VIRGINIA 22211-1199

REPLY TO  
ATTENTION OF

IMMH-BN

01 April 16

MEMORANDUM FOR all Soldiers Assigned and Attached to Headquarters Command Battalion (HQ CMD BN), Joint Base Myer-Henderson Hall, VA 22211-1199

SUBJECT: Commander's Operational Security Policy – Policy Memorandum #18

1. REFERENCE. AR 530-1, Operations Security (OPSEC), 26 Sep 14.
2. PURPOSE. To provide guidance to all HQ CMD BN personnel on incorporation of OPSEC practices and procedures into daily activities.
3. APPLICABILITY. This policy applies to all Department of the Army (DA) personnel, military and civilian, working in the HQ CMD BN community.
4. POLICY. OPSEC is the security of plans, operations and activities. OPSEC denies access to critical information by identifying, controlling, and protecting indicators and information sources associated with the planning and execution of actions, as well as the existence and capabilities of an activity. OPSEC practices and procedures will be integrated into day-to-day operations at all HQ CMD BN activities. It is a security process that must be taken as seriously as the protection of classified information.
5. PROCEDURES.
  - a. All products containing sensitive but unclassified information (Critical Information, For Official Use Only (FOUO), Privacy Act Information, etc.) should be destroyed as classified trash. Shredding is the principal method for destruction using GSA-approved shredders. All other information developed as part of the job should be disposed of appropriately.
  - b. "For Official Use Only" will be the standard marking for all unclassified products determined to be Critical Information by each directorate in coordination with the OPSEC Program Manager. Critical Information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and information needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment.
  - c. All unclassified official e-mail going outside of HQ CMD BN to higher headquarters will be sent encrypted and have the proper classified markings at the beginning and end of the message (e.g., Unclassified FOUO). All official e-mail sent within the HQ CMD BN containing privacy act information will also be sent encrypted.

IMMH-BN

SUBJECT: SUBJECT: Commander's Operational Security Policy – Policy  
Memorandum #18

d. Every effort should be made to keep work areas clear of classified documents, sensitive information and privacy information, including telephone numbers. Offices should use the Standard Form 701 to ensure work areas are OPSEC clean. The last individual leaving the office or work area is responsible for ensuring the area is cleared of classified, official use only documents, and privacy information. HQ CMD BN does not possess the required assets to store classified material. Soldiers needing to store classified material must coordinate with the Joint Base Myer-Henderson Hall Security Manager to ensure proper storage is conducted. At no time will classified material be stored in the HQ CMD BN area.

e. All HQ CMD BN personnel will consult with their immediate supervisor and/or the HQ CMD BN OPSEC program manager prior to publishing or posting information in any public forum to ensure no Critical Information or indicators are released. This includes but is not limited to letters, email, websites, web logs and information forums. Supervisors will review documents to ensure Critical Information and indicators of Critical Information are not released.

f. HQ CMD BN S-3 is responsible for appointing a representative to attend the OPSEC Working Group. HQ CMD BN OPSEC Manager will also annually review the Installation Critical Information List and develop an acceptable OPSEC risk for the Commander.

g. 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, operations, and maintenance for all information systems, including telephones, facsimile machines, computer networks, and modems. All government equipment is subject to monitoring for telecommunications security purposes at all times. All users will report security incidents to the Information Assurance Program Manager, Network Enterprise Center Fort Myer.

h. Annual training for OPSEC and Information Assurance is mandatory. OPSEC training can be scheduled through the DPTMS and will include Critical Information Awareness. Information Assurance training is an on-line course which personnel can access at <https://iaut.mdw.army.mil>.

IMMH-BN

SUBJECT: SUBJECT: Commander's Operational Security Policy – Policy  
Memorandum #18

6. PROPONENT. The Directorate of Plans, Training, Mobilization and Security is the proponent for this policy. POC is the OPSEC Program Manager, 703-696-0756.

*John M. Kupka*  
JOHNATHON M. KUPKA  
LTC, SF  
Commanding