



REPLY TO  
ATTENTION OF

**DEPARTMENT OF DEFENSE**  
**JOINT TASK FORCE GUANTANAMO**  
**U.S. NAVAL BASE, GUANTANAMO BAY, CUBA**  
**APO AE 09360**

JTF GTMO-CG

23 March 2004

MEMORANDUM FOR All Personnel Assigned or Attached to Joint Task Force Guantanamo Bay.

SUBJECT: General Order No. 2

1. **TITLE:** Operations Security (OPSEC) for Joint Task Force GTMO personnel serving in the Joint Operations Area (JOA).
2. **PURPOSE:** To prohibit conduct that is prejudicial to the good order and discipline of JTF GTMO, that may threaten the national security of the United States or its allies, and is of a nature likely to bring discredit upon the Armed Forces.
3. **APPLICABILITY:** This General Order is applicable to all U.S. military personnel assigned, attached, or under the operational control of JTF GTMO, and all U.S. civilian personnel serving with, employed by, or accompanying forces assigned or attached to JTF GTMO.
4. **AUTHORITY:** The Uniform Code of Military Justice (UCMJ), Title 10, United States Code, section 180 et. seq.
5. **PUNITIVE ORDER:** This order is punitive. Persons subject to the UCMJ who violate this order either negligently or intentionally may be punished under Article 92, UCMJ, for violating a lawful general order, or receive adverse administrative actions or both. Civilians serving with, employed by, or accompanying the U.S. Armed Forces in JTF GTMO are not only subject to all applicable federal laws, but may also face adverse administrative actions for violation of this General Order.
6. **PROHIBITED ACTIVITIES:**
  - a. Discussing matters of a personal or operational nature in the presence of detainees that need not be discussed in their presence.
  - b. Communicating with detainees (verbal or non-verbal) or assisting others and/or allowing others to communicate with detainees without the proper authorization. Failing to report unauthorized communications or attempted communications with a detainee, or failing to report a detainee's attempts to improperly communicate with a person subject to this Order.

JTF GTMO-CG

SUBJECT: General Order No. 2

c. Leaving any tools, keys, weapons or other work-related materials necessary to perform your mission unattended or within the reach of persons unauthorized to possess them, or bringing any materials not necessary for the performance of the mission into a sensitive area or detainee area.

d. Bringing cameras or other communication or recording devices without proper authority into one of the detainee camps, SCIF, or other areas where sensitive materials may be located.

e. Taking visual or audio recordings or drawings of the detainees, camp facilities, detainee operations, personnel working in and around detention facilities in Radio Range area, Camp X-Ray, or any other part of the NAVBASE that is a photography-prohibited area (this includes the coastline from Windmill Beach to the Cuban/American fence line). This prohibition also includes taking photographs or video recordings of personnel movements or operations at NAVBASE GTMO without the appropriate authorization, and transmitting or displaying any information relating to JTF GTMO operations on any website or other shared medium without the proper written authorization.

f. Communicating, discussing or disseminating classified information, or any other information relating to any JTF GTMO operations, including the information referenced in Policy Memorandum #8, subject: Essential Elements of Friendly Information (EEFI), without proper authorization.

g. Using non-secure means to discuss classified information or other information related to JTF GTMO operations.

h. Transferring classified information or discs to lower-classified or unclassified medium, network or computer.

i. Discussing classified matters, work related matters, or JTF operational matters with anyone who does not have either the appropriate clearance or the need to know said information or in the presence of anyone that does not have the appropriate clearance.

j. Transporting classified information without the proper locking containers or covers, leaving computer terminals or classified material unattended and unlocked.

k. The improper marking of information, taking classified materials to a housing unit, sharing or revealing computer access user names and passwords. Misplacing or leaving personnel rosters, access badges, or computer access user names and passwords, and classified materials unattended.

l. Failing to immediately disclose to the chain of command any information concerning

JTF GTMO-CG

SUBJECT: General Order No. 2

sabotage, terrorist activity, subversive activities that may pose a direct threat to U.S. personnel, requests by anyone for illegal or unauthorized access to classified or sensitive information, contact with an individual whom you have reason to believe is targeting you for exploitation, or other OPSEC violations.

m. Taking a person to any area for which they do not possess the required clearance without authorization or a mission related purpose, or leaving a person unattended in any area where they are not authorized to be unattended.

n. Wearing un-sanitized uniforms in the presence of detainees.

o. Accessing, downloading, installing, or storing unauthorized internet sites or other unauthorized materials, software, or programs on any JTF GTMO or MWR computer without the express written approval of the J6.

p. Leaving your computer system logged on and unattended without properly locking the terminal, using a private computer to process government related work, or plugging any privately owned computer (non-government computer) into the JTF GTMO or MWR networks without the express written approval of the J6.

q. Forwarding chain mail or virus warnings. Failing to immediately report the discovery of a virus or virus warning.

r. The improper use of another person's identity or computer account. Masking, or attempting to hide a user's identity while using the computer network system.

s. Connecting or allowing the connection of a modem to a JTF GTMO computer or printer/fax, which is directly connected to JTF GTMO computer networks. Connecting or allowing to be connected any hardware or software not provided or authorized by JTF GTMO, J6.

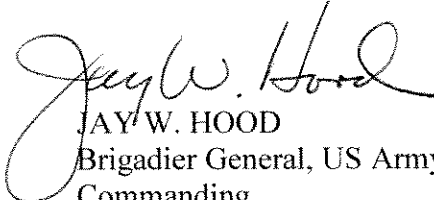
7. **INDIVIDUAL DUTY:** All persons subject to this General Order are charged with the duty to become familiar with this General Order. All personnel shall avoid action, whether or not specifically prohibited in this General Order, which might result in or reasonably be expected to create the appearance of a violation of this general Order or other law under the UCMJ, or which by its very nature might compromise the OPSEC of JTF GTMO.

8. **UNIT COMMANDER RESPONSIBILITIES:** Unit commanders and supervisors are to ensure that all personnel are briefed on the contents of this General Order, that personnel understand that they have a duty to report any violations of this order either to their supervisor or to the Staff Judge Advocate, and that it is posted on read boards in common areas throughout the unit.

JTF GTMO-CG

SUBJECT: General Order No. 2

9. EFFECTIVE DATE: This General Order is effective immediately.
10. EXPIRATION: This General Order will expire when rescinded by the Commander, JTF GTMO, or higher authority, or upon redeployment from JTF GTMO.
11. WAIVER REQUESTS: Requests to waive prohibitions of this General Order must be coordinated with the JTF Staff Judge Advocate and can only be approved by the Commander, JTF GTMO.
12. My point of contact for this General Order is the OPSEC Program Manager, x5022.

  
JAY W. HOOD  
Brigadier General, US Army  
Commanding