HQMC SECURITY ORIENTATION/AWARENESS BRIEFING

Because of the increased threat posed by terrorists and hostile intelligence operatives, it has become vitally important that we recognize that DoD employees, both military and civilian, are part of the first line of defense against those who wish to do us harm either physically or through the mishandling of classified information. With that in mind, it is critical that all employees receive basic security awareness information.

1. **Clearance and Access**: Only individuals with the appropriate clearance eligibility, a need-to-know, and billet requirements will have access to classified information. In addition, individuals requiring access to classified information who have a clearance based off of an out-dated personnel security investigation will be required to submit the Electronic Personnel Security Questionnaire (EPSQ) with fingerprint card to the HQMC Security Office.

2. **Classified information:** Classified information, as well as computers (including laptops) may not be removed from the DoD buildings (Pentagon/Annex, etc.) without a proper courier authorization and without proper packaging and protection. Requests for courier cards must be provided to the HQMC Security Office (room 1010) via the appropriate Security Manager (i.e., I&L, P&R, etc.). Property passes from the responsible officer are required in order for Government equipment to be taken outside of any building located on the Pentagon reservation (i.e. Annex/Pentagon). While inside a DoD building, no classified information may be carried outside office spaces unless it is also properly covered and safeguarded (i.e. use of colored coversheets).

3. **Disposal:** Controlled documents (classified information) may not be destroyed without proper authorization from your Security Manager and then only in an authorized manner.

4. **Classified storage:** All classified information must be stored in an approved GSA container (i.e. safe) or in an approved open storage office space.

5. **Telephones:** Classified discussion via telephone is authorized only by use of classified telephones (STU III/STE, etc.). Caution should be exercised when discussing classified information via classified phone to ensure that individuals cannot overhear the discussion.

6. **Faxes:** Faxes containing classified information may only be transmitted from a secure fax machine to a secure fax machine. Unclassified fax machines are not to be used as copiers for the purpose of copying classified information or for the transmission of classified information.

7. **Computers:** Classified information may only be processed on approved secure computers. All approved computers and diskettes must be clearly marked with the appropriate security labels, and personally owned computers

may never be used to process classified information. Transmission of classified information via computer may only be accomplished via SIPRNET.

8. **Photocopiers:** Classified information must be properly marked and may only be copied on approved (marked as classified) photocopiers and/or reproductive equipment.

9. **Security violations:** Security violations are to be reported to your Agency Security Manager. If unavailable, the security violation is to be reported to the HQMC Security Officer in room 1010 of the Annex.

10. **Discussion of classified information:** Discussion of classified information is only allowed in approved/secure areas. Discussion of classified information in DoD building passageways, dining areas, private vehicles, etc. is strictly prohibited.

11. **Checking out:** All personnel departing HQMC due to PCS/PCA, terminal leave, retirement/EAS, transfer, etc. are required to checkout with their Security Manager and with the HQMC Security Office in room 1010 of the Annex.

12. **Continuous Evaluation Program:** All personnel assigned to HQMC are subject to continuous evaluation. Information received by this office which may affect an individual's access to classified information will be forwarded to the Department of the Navy Central Adjudication Facility (DONCAF).

13. **Classified meetings/briefs:** DoD policy prohibits classified meetings and briefs from being conducted in non-government facilities (i.e., hotels).

14. **For Official Use Only (FOUO):** Information marked as FOUO should be destroyed by shredding or by placing in a burn bag. Official use means that only individuals with the U.S. Government are to be provided the information.

15. **Security Education Training:** Individuals are required to attend an annual CE brief. The brief is comprised of the required annual security refresher, anti-terrorism/force protection, and counter-intelligence briefs.

16. **HQMC/ARS/Security Website address is:** http://www2.hqmc.usmc.mil/ARS/ARSWebsi.nsf/arsmain?OpenView

---

Signature: _____

Witness: _____