

AR Division Check-In Checklist

Opened: _____

Closed: _____

In accordance with the Privacy Act of 1974 (Public Law 93-579), this notice informs you of the purpose for collection of information on this form. Please read it before completing the form.

AUTHORITY: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041. Headquarters, Marine Corps; and SORN NM05000-2.

PURPOSE: Information will be used to document completion of Check-In requirements.

RETENTION: This form will be maintained by AR Division for two years after final entry is made and then destroyed.

ROUTINE USES: Information will be accessed by AR Division personnel with a need to know to meet the purpose. Information will not be routinely disclosed outside of DoD. A complete list and explanation of the applicable routine uses is published in the authorizing SORN available at: <https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570436/nm05000-2/>.

DISCLOSURE: Voluntary; however, failure to provide the information requested may result in check-in requirements not being met and services not being provided in a timely manner.

Part I

New Join/Employee Info

Name Last, First MI _____

DOD ID (If Applicable)

Affiliation (Circle one): Marine (Active or Reserve), General Schedule, Contractor

Grade/Rank: _____ *All GS-12s and above will need to schedule time to meet with the Director*

Email (If no usmc.mil email, identify in Part III): _____ *Provide best email to contact you*

Contract # (If applicable): _____ *Provide contract when submitted to Front Office*

Contract Start Date: _____ End Date: _____

Date Joined/Hired: _____

Read HQMC Security Orientation Brief: Yes or No Initials: _____

Part II

Supervisor / Sponsor Information:

Rank/Grade Last, First MI _____ Email _____

Branch (circle one): ARD / ARE / ARF / ARH / ARI / ARS / Front Office

Part III

Administrative Requests

Email/Computer Access: (Circle One): Yes or No: *PII and Cyber Awareness Certificates completed (within 1 year) and complete required SAAR Forms*

Building Access Required (Circle One): Yes or No

PFAC ID Needed (Circle One): Yes or No *Only require access to the Pentagon but not a computer*

CAC Needed (Circle One): Yes or No If no, Expiration of CAC: _____

Parking (Circle One): Yes or No (Temporary or Permit)

Temp Parking dates: From: _____ To: _____

License Plate #: _____ State: _____

Swipe Request(s) Provide list of all room #s/SCIFs Rooms #s: _____

CANNOT be submitted until DD2249 is approved granting access to Pentagon

Part IV

-Date/Time emailed to SMB_HQMC_AR1@usmc.mil: _____ / _____ : _____

Remarks: _____

AR Division Check-In Checklist

(For Front Office Use)

Date Received: _____

BIC: _____

Date Request Submitted in ESSRP/ARS SMB: _____

Front Office Rep: _____

Action Requested/ Taken: ☐ Submitted via ESSRP / ARS SMB email ☐ Parking CAC/PFAC

☐ Building Access ☐ Swipe Access ☐ Investigation

☐ Other: _____

Remarks: _____

Front Office Verification

Date Received DD2249: _____

Date Swipe Access Approved: _____

Date Temp or Permit Parking Approved: _____

SAAR Forms Closed (Front Office IT Specialist): _____

Verified all action by (Front Office Rep): _____

Date Closed: _____

(Apr 2016)

Pentagon Access Acknowledgement Form

In accordance with the Privacy Act of 1974 (Public Law 93-579), this notice informs you of the purpose for collection of information on this form. Please read it before completing the form.

AUTHORITY: 10 U.S.C. 5041, Headquarters, Marine Corps;

PRINCIPAL PURPOSE: Information collected by this form will be used for sponsorship of access to the Pentagon and Pentagon Reservation.

RETENTION: The collected information will be maintained in the files of the HQMC Security Office. Issued Department of Defense (DoD) credentials are destroyed three months after return to issuing office. Records of sponsorships are destroyed two years after final entry or two years after date of document, whichever is later. Records in this file system will be retrieved by visitor name only.

ROUTINE USES: None other than the blanket routine uses established by the DoD Privacy Office and posted at <http://www.defenselink.mil/privacy/notices/blanket-uses.html>.

DISCLOSURE: Providing information on this form is voluntary. However, failure to provide may result in deny of Pentagon and Pentagon Reservation access.

Principal Purpose

To ensure that DoD and non-DoD personnel are informed of the Headquarters U.S. Marine Corps (HQMC) eligibility requirements and conditions associated with access to the Pentagon and Pentagon Reservation under HQMC sponsorship.

General

In accordance with DoD Administrative Instruction 30 (Force Protection of the Pentagon Reservation), you are being granted access to the Pentagon and Pentagon Reservation because an appropriate HQMC Staff Agency/Activity has chosen to sponsor you for access. In accepting this sponsorship, your signature on this document indicates your understanding that you have been granted access to the Pentagon and Pentagon Reservation for the sole purposes of conducting, participating in, or facilitating official U.S. Government business.

Misuse

Using your access to the Pentagon and Pentagon Reservation or any part thereof and to engage in activities outside the scope of the official business for which your access was granted, is grounds for the immediate confiscation of DoD credentials, withdrawal of HQMC sponsorship, and denial of continued and future access to the Pentagon and Pentagon Reservation.

Control

DoD credentials are U.S. Government property. The transfer or lending of your DoD credential to another individual or the alteration thereof is a violation of 18 United States Code section 499 and may result in prosecution or adverse administrative action.

Acknowledgement

I _____, have read, understand, and will comply with the provisions of this document and with the terms of DoD Administrative Instruction (AI) 30. Any questions I may have about this document or DoD AI 30 have been answered.

Signature

Date

BRIEFING/REBRIEFING/DEBRIEFING CERTIFICATE

SECTION A - GENERAL

1. NAME: _____
2. DUTY POSITION: _____ 3. PHONE NUMBER: _____
4. ORGANIZATION: _____ 5. ADDRESS: _____

SECTION B - BRIEFING

6. I certify that I have (read and been granted access to)(been briefed) and fully understand the procedures for handling (COSMIC)(ATOMAL)(NATO SECRET)(NATO CONFIDENTIAL) material and am aware of my responsibilities for safeguarding such information and that I am liable to prosecution under Sections 793 and 794 of Title 18, U.S.C., if either by intent or negligence I allow it to pass into unauthorized hands.

7. SIGNATURE OF INDIVIDUAL: _____ DATE: _____
8. SIGNATURE OF BRIEFER: _____ DATE: _____

SECTION C - ATOMAL REBRIEFING

9. I certify that I have been briefed and fully understand the procedures for handling ATOMAL material and am aware of my responsibility to safeguard such.

SIGNATURE AND DATE

SIGNATURE AND DATE

FILL OUT ONLY FOR ATOMAL ACCESS

SECTION D - DEBRIEFING

10. I have been debriefed for (COSMIC)(ATOMAL)(NATO SECRET)(NATO CONFIDENTIAL) and I understand that I must not disclose any classified information which I have obtained in my assignment to this organization or in connection therewith. I also understand that I must not make any such classified information available to the public or to any person not lawfully entitled to that information. I further understand that any unauthorized disclosure of such classified information, whether public or private, intentional or unintentional, will subject me to prosecution under applicable laws.

SIGNATURE OF INDIVIDUAL: _____ DATE: _____

SIGNATURE OF CONTROL OFFICER: _____ DATE: _____

CLASSIFIED INFORMATION ACCESS AUTHORIZATION (5521)

NAVMC HQ 512 (REV. 05-17) (EF) (Previous editions will not be used)

FOUO - Privacy sensitive when filled in

PRIVACY ACT STATEMENT

In accordance with the Privacy Act of 1974 (Public Law 93-579), this notice informs you of the purpose for collection of information on this form. Please read it before completing the form.

AUTHORITY: 5 U.S.C. 9101; 10 U.S.C. 137; DoD Directive 1145.02E; DoD 5200.01; DoD 5105.21; DoD Instruction (DoDI) 1304.26; DoDI 5200.02; DoDD 5220.6; DoDI 5220.22; Homeland Security Presidential Directive (HSPD) 12; E.O. 9397 (SSN), as amended; and SORN DMDC 12 DoD available at <http://dpclid.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570567/dmdc-12-dod/>.

PURPOSE: The information is used by Headquarters, U.S. Marine Corps (HQMC) Staff Agencies/Activities for the purpose of confirming security clearance eligibility for access to National Security Information. The form is also used by HQMC Security Manager for the documentation and tracking of the level access that is given to an individual.

RETENTION AND SAFEGUARDS: Records are destroyed two years after final entry. The collected information will be maintained in the files of the HQMC Security Office/database with restricted, limited access by authorized personnel who are properly screened, cleared, and trained.

ROUTINE USES: Access to information is limited to security personnel with a need to know in order to confirm security clearance status and various officials outside the Department of Defense (DoD) specifically identified as a Routine Use in Privacy Act System of Records Notice DMDC 12 DoD for the stated specific purpose of that Routine Use, to include the White House; U.S. Citizenship and Immigration Services; Law Enforcement; federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information; to a federal agency in connection with the hiring or retention of an employee; Congress; Office of Personnel Management; or federal agency for counterintelligence purposes.

DISCLOSURE: Voluntary; however, failure to provide this information may result in your denial of access to National Security Information.

CLASSIFIED INFORMATION ACCESS AUTHORIZATION (5521)

SECNAV M-5510.30 AND HQMC IPSP SOP

NAVMC HQ 512 (REV. 05-17) (EF) (Previous editions will not be used)

FOUO - Privacy sensitive when filled in.

INSTRUCTIONS

This form is used to initiate and document an individual's authorization to handle classified information at Headquarters Marine Corps. ACCESS IS NOT AUTHORIZED UNTIL PART C IS APPROVED.

NAME (Last, First, Initial)

RANK/GRADE

SSN

UNITED STATES CITIZENSHIP

YES

NO

☐☐

ACTIVE

☐

RESERVE

☐

AGENCY, PHONE NO. AND ROOM NO.

PART A - (To be completed by Staff Agency Security Manager)

It is requested that the individual identified above be authorized access to classified information as follows:

TOP SECRET SECRET

SENSITIVE COMPARTMENTED INFORMATION (SCI)

☐

CLASSIFIED INFORMATION

☐☐

COSMIC

☐

ATOMAL

☐☐

NATO

☐☐ ACCESS TO CLASSIFIED INFO NOT REQUIRED

Signature: _____

(Agency Security Manager)

Date: _____

ATTESTATION

"I accept the responsibilities associated with being granted access to Classified National Security Information. I am aware of my obligation to protect Classified National Security Information through proper safeguarding and limiting access to individuals with the proper security clearance and/or access and official need to know. I further understand that, in being granted access to classified information and/or SCI/SAP, a special confidence and trust has been placed in me by the United States Government."

Signature: _____

Date: _____

(Individual Requiring Access)

PART B - (To be completed by the Special Security Officer)

This authorization is automatically withdrawn when the individual is detached or transferred. This individual's access status is:

Level and Date _____

Basis _____

Signature _____

Date _____

HQMC SPECIAL SECURITY OFFICERS (SSO)

PART C - (To be completed by Director of Administration and Resource Management)

Access is authorized as shown above. This authorization is automatically withdrawn when the individual is detached or transferred to another staff agency. The individual's clearance status is:

Level and Date _____

Basis _____

Signature _____

Date: _____

(HQMC Security Manager)

PART D - (To be completed by the individual when detached or reassigned)**SECURITY DEBRIEFING ACKNOWLEDGEMENT**

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me, that I have returned all classified information in my custody, that I will not communicate or transmit classified information to any unauthorized person or organization, that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

Signature _____

Date: _____

FOR OFFICIAL USE ONLY

Adobe live cycle designer 11

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.
2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.
4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, *952 and 1924, title 18, United States Code; *the provisions of section 783(b), title 50, United States Code; and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.
6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.
8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.
9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.
10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

(Continue on reverse.)

11. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 13526 (75 Fed. Reg. 707), or any successor thereto section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b) (8) of title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community, and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3)) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403g(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, *952 and 1924 of title 18, United States Code, and *section 4 (b) of the Subversive Activities Control Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001, section 2001.80(d)(2)) so that I may read them at this time, if I so choose.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)
ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)		

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS (Type or print) HEADQUARTERS MARINE CORPS ATTN: AR DIVISION 3000 MARINE CORPS PENTAGON WASHINGTON, DC 20350		NAME AND ADDRESS (Type or print)	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Public Law 104-134 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.



Headquarters Marine Corps



SECURITY ORIENTATION

Security Manager: Shameica S. Barnes

Assistant Security Manager: Luis Navarro

Phone number: (703) 614-3609

Use arrow keys or click with your mouse to take this training.

PURPOSE

The protection of Government assets, people, property, and information both Classified and Unclassified, is the responsibility of all personnel, regardless of how it was obtained.

Anyone with access to these resources has an obligation to protect it.

PURPOSE

You are responsible for becoming familiar with your individual security responsibilities as it pertains to your duties while assigned to Headquarters Marine Corps (HQMC).

This security orientation training describes the basic security information and common procedures that you should be aware of while assigned to HQMC.

TOPICS

- Check-in and Check-out
- Security Clearance Eligibility & Access
- Continuous Evaluation Program
- Information Security
- Personal Electronic Devices (PEDS)
- Compromise and Other Security Violations
- Information/Personnel Protection
- Information Assurance
- Foreign Travel Procedures
- Physical Security
- Security Training
- Staff Agency/Activity Security Contact Information

CHECK-IN



CHECK-IN

All personnel assigned to HQMC must check-in through their respective Staff Agency/Activity Security Coordinator.

Personnel that do not have eligibility to access classified information are not authorized to work where classified information is processed and stored.

Staff Agency/Activity Security Coordinators will ensure that all required security forms and briefs are completed and submitted to the HQMC Security Office.

When the Staff Agency/Activity determines that a contractor is onsite or offsite, the contractor must comply with HQMC security regulations. Contractor check-in procedures, are outlined in the HQMC Information and Personnel Security Program (IPSP) SOP Enclosure (6).

CHECK-OUT



CHECK-OUT

All departing personnel must check-out with their Staff Agency/Activity Security Coordinators.

All departing personnel must read and sign the HQMC Command Debriefing Form and the NATO Briefing Certificate (if applicable).

The Security Termination Statement will be read and signed by all Military and Civilian personnel that are separating, retiring or resigning.

All Military and Civilian personnel will surrender their Courier Card (if applicable) Common Access Card (CAC) for Civilian employees (if retiring, resigning, or leaving DoD) will be turned in to HR.

Contractor personnel will also surrender their Courier Letter (if applicable), and their Common Access Card (CAC).

All departing personnel will return KSV-21 Card (ECC Card) or any COMSEC Equipment to the Staff Agency/Activity LECO (if applicable).

SECURITY CLEARANCE ELIGIBILITY & ACCESS



SECURITY CLEARANCE ELIGIBILITY & ACCESS

No individual will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made. All military, civilian, and contractor personnel are subject to an appropriate investigation as required.

Investigation

- Step 1: The PSI: NACI, Tier 3, Tier 3R, SSBI, PPR, or SBPR.

Eligibility

- Step 2: Favorable eligibility determination granted by DoDCAF.
- **“Eligibility” replaced the old term “clearance”.**

Clearance Access

- Step 3: Granted by HQMC Security Manager, based on valid SF 312, “need-to-know”, and once all required Security check-in briefings have been complete.

SECURITY CLEARANCE ELIGIBILITY & ACCESS

Your position sensitivity and/or duties will determine your investigation, clearance eligibility, and access requirements.

All military personnel must meet the basic investigative requirement of Tier 3 regardless of MOS or citizenship.

All officers must maintain a minimum of secret clearance eligibility based on a NACLC/Tier 3 closed within 10 years.

Clearance eligibility must be met by those in a MOS or billet with an eligibility requirement.

Investigations may not be submitted within 12 months of separation or retirement.

Clearance eligibility does not “expire” unless there is a break in service over 2 years or a security incident resulting in revocation.

SECURITY CLEARANCE ELIGIBILITY & ACCESS

- A clearance upgrade will be requested only when an individual is assigned to a billet that requires a higher level of access.
- Top Secret (TS) investigations will only be submitted to OPM for billets coded appropriately in the Total Force Structure Management System (TFSMS) or Military Occupational Specialty Manual (MOS) designated. Contact the AR Division Manpower Analyst at (703) 614-1837 for assistance.
- Employees requiring access to NATO information must possess the equivalent final U.S. security clearance.
- Periodic Reinvestigations (PR):
 - Top Secret/Top Secret (SCI) every 5 years
 - Secret every 10 years
- 30 days before expiration, HQMC Security Office will send a notification email to the individual when their reinvestigation is due.

CONTINUOUS EVALUATION PROGRAM (CEP)



CONTINUOUS EVALUATION PROGRAM

What it is

- It ensures those granted eligibility remain eligible through continuous assessment & evaluation
- We must report ANY information that may affect clearance eligibility

What it is not

- Automatic grounds to terminate employment.
- Automatically revoking eligibility

Who it is for

- It applies to ALL military, civilian, and contractor personnel

Who is responsible for reporting

- EVERYONE

What is reported

- Information pertaining to the 13 adjudicative guidelines, as identified on slide 16

CONTINUOUS EVALUATION PROGRAM

This program relies on **ALL** HQMC personnel to report questionable or unfavorable information which may be relevant to a security clearance determination.

Individuals

- Report to Supervisor, Security Coordinator, or HQMC Security Manager & seek assistance.

Co-workers

- Advise Supervisor, Security Coordinator, or HQMC Security Manager.

Supervisors/Leadership

- Recognize problems early; react appropriately to ensure a balance is maintained regarding individual's needs and national security issues. Report any problems to Staff Agency/Activity Security Coordinator or HQMC Security Manager.

YOU MUST REPORT:

(Self-report and Indicators Exhibited by Others)

Divided Loyalty or
Non Allegiance to
the U.S.

Emotional, Mental,
and Personality
Disorders

Sexual
Behavior

Misuse of IT
Systems

Financial
Considerations

Alcohol
Consumption

Drug
Involvement

Foreign
Preference

Criminal Conduct

Personal Conduct

Foreign Influence

Foreign Outside
Activities

Security Violations

NOTE 1: Command personnel are encouraged to review their credit reports as a value to forestall potential financial problems.

NOTE 2: Combat veterans or victims of sexual assault suffering from Post Traumatic Stress Disorder (PTSD), who seek mental health care will not, in and of itself adversely impact that individual's ability to obtain or maintain their eligibility.

PTSD IS NOT A DISQUALIFYING FACTOR.

CONTINUOUS EVALUATION PROGRAM

Threats to classified and unclassified government assets can include:

- Insider (military, civilian, contractors, and authorized visitors).
- Criminal and terrorist activities.
- Foreign intelligence services and foreign governments.

What happens after reporting to the HQMC Security Manager?

- HQMC Security Manager submits the report to the adjudicative agency, Department of Defense Consolidated Adjudicative Facility (DoDCAF).
- Staff Agency/Activity Director/ Deputy Commandant will make a recommendation to the Director, Administration and Resource Management Division (DirAR), on the basis of all facts, to authorize, withdraw, or suspend an individual's access to classified information during the process.
- DoDCAF makes the determination whether to maintain clearance eligibility.

CONTINUOUS EVALUATION PROGRAM

Keys to an effective CEP

- Security education.
- Positive reinforcement to include management support, confidentiality, and employee assistant programs.
- Command involvement & support.
- Proper reporting.

INFORMATION SECURITY



INFORMATION SECURITY

Classified information or material will only be viewed or processed when adequate protection conditions have been met to prevent any type of compromise.

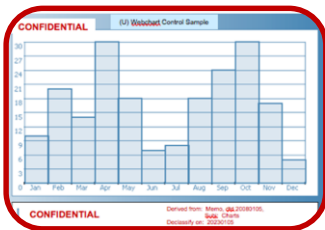
Classified Information must:

Be under the direct control by an authorized person or stored in a locked security container, vault, secure room, or secure area.	Be processed on approved equipment.	Be destroyed by one of the following authorized means: <ul style="list-style-type: none">-Cross-cut shredding.-Mutilation.-Chemical decomposition.	Be discussed on secure telephones or sent via, secure communications, and/or only discussed in authorized areas.
---	-------------------------------------	--	--

INFORMATION SECURITY

TYPES OF CLASSIFIED INFORMATION

Classified information can include any of these and must be properly marked:



Charts



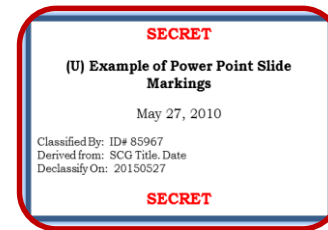
Maps, Photographs



Publications/Manuals



Documents, Reports, Messages



Briefing/Presentation slides



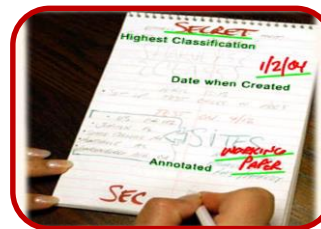
Machinery, Faxes, Scanners, Tablets



CD, DVD, External Hard Drives



Blogs, Web pages, Emails



Working papers



Reproductions

A descriptive guide outlining the proper procedures for marking classified information can be found at: <http://www.archives.gov/isoo/training/marketing-booklet.pdf>

INFORMATION SECURITY

TYPES OF CLASSIFICATION

Original:

- An initial determination, in the interest of national security, to protect information against unauthorized disclosure.
- Authority designated by SECNAV authorizing officials to originally classify information at a given level.
- Original Classification Authority (OCA) granted by virtue of position held. Authority not transferrable.
- Training required before exercising authority.
- OCAs must have jurisdiction over information they are classifying for the first time and must use 1 or more of the reasons for classification as described in Sec. 1.4 of EO 13526.
- OCA decisions codified in Security Classification Guides.

Derivative:

- Classification markings applied to material derived from classified source material by incorporating, paraphrasing, restating, or generating in a new form.
- Marking the newly developed material consistent with the classification markings that apply to the source information.
- Receive training Annually.
- Observe and respect OCA determinations.
- Observe and respect original markings.
- Carry forward declassification instructions (using the most stringent).
- Use only authorized sources.
- Use caution when paraphrasing.
- Derivative Classifiers are identified on documents they have derivatively classified.
- List all sources.
- All authorized military, civilians, and contractor personnel can be derivative classifiers.

INFORMATION SECURITY

AUTHORIZED SOURCES

Security Classification Guide (SCG)

- Is the primary source guide for derivative classification and is prepared by an OCA. An SCG contains a collection of precise, comprehensive guidance about a specific program, system, operation, or weapons system identifying what elements of information are classified. For each element of information, the SCG includes the classification level, the reason(s) for that classification, and information about when that classification will be downgraded or declassified.

Properly Marked Source Document

- Is an existing properly marked memo, message, letter, email, etc., from which information is extracted, paraphrased, restated, and/or generated in a new form or inclusion in another document. If there is an apparent marking conflict between a source document and an SCG regarding a specific item of information, derivative classifiers must follow the instructions in the SCG.

DD 254

- Provides classification guidance to contractors performing on classified contracts. The form identifies the level of information the contractor will need to access, the required level of security clearance for access, and the performance requirements.

INFORMATION SECURITY

MARKING

What is marking?

- The physical act of indicating the highest classification level for classified information is clearly identified, to ensure the proper protection and safeguards are adhered to.

Why is classified information marked?

- Alert holders of the presence of classified information.
- Ensure proper handling controls and special safeguards are adhered to.
- Identifies the office of origin and document originator applying the classification markings.
- Prevent unauthorized disclosure.
- Inform the holders of the level of protection required and duration of classification.

Who is responsible for marking?

- It is the responsibility of the Original Classifier and Derivative Classifier (Action Officers) to properly mark classified documents.

What are the marking requirements?

- Examples of the required markings are outlined on slides 25 and 26.

INFORMATION SECURITY

MARKING REQUIREMENTS

- All classified information shall be clearly identified by electronic labeling, designation, or marking. Must bear the following markings:
 - Banner markings must be applied on the top and bottom of all pages to include cover pages.
 - Portion Markings.
 - The Agency and office of origin.
 - Date of origin.
 - “Classified by” for original AND derivatively classified documents, “Name and Position”.
 - Reason (original classification only).
 - “Derived from” line for derivatively classified documents, “Sources must be listed”.
 - Declassification instructions, YYYYMMDD format.
 - Downgrading instructions, if applicable.
 - Dissemination control notices (front page).

Example of Derivative Classification:

The diagram illustrates a memorandum from the Department of Defense, Office of the Under Secretary of Defense, Intelligence. It is a memorandum for an unspecified recipient, dated, and subject to the delegation of SECRET Original Classification Authority (OCA). The memorandum contains three paragraphs of text, each with a classification marking: (U) for the first paragraph, (S) for the second, and (S/NF) for the third. A 'Portion Markings' box points to the (U) and (S) markings. A 'Banner Line (overall classification marking)' box points to the (S/NF) marking. A 'Classification Authority Block' box points to the 'Classified By' line. A 'Signature Block' box points to the 'Classified By' line. A 'Classification' box points to the (U) marking. A 'Separator' box points to the (S) marking. A 'Dissemination Control' box points to the (S/NF) marking. The memorandum is marked with SECRET//NOFORN at the top and bottom.

SECRET//NOFORN

OFFICE OF THE UNDER SECRETARY OF DEFENSE

INTELLIGENCE

date

MEMORANDUM FOR XXXXXXXXX XXXXXXXXXX

SUBJECT: (U) Delegation of SECRET Original Classification Authority (OCA)

(U) You are hereby delegated authority to classify information up to SECRET for information under your area of responsibility accordance with Executive Order 13526, "Classified National Security Information" (the Order).

(S) As an OCA you are required to receive training in original classification as provided by the Order and implementing directives prior to you exercising this authority. Your Security Manager will facilitate this training.

(S/NF) The Order also provides that OCAs shall prepare classification guides to facilitate the proper uniform derivative classification of information. Request that you provide a copy of your guide(s) to this office by December 31, 2010.

Signature Block

Classified By: John Doe, Director
Derived From: SecDef Memo, dtd 20101024, Subj: _____
Declassify On: 202011024

SECRET//NOFORN

Classification Authority Block

Portion Markings

Banner Line (overall classification marking)

Classification

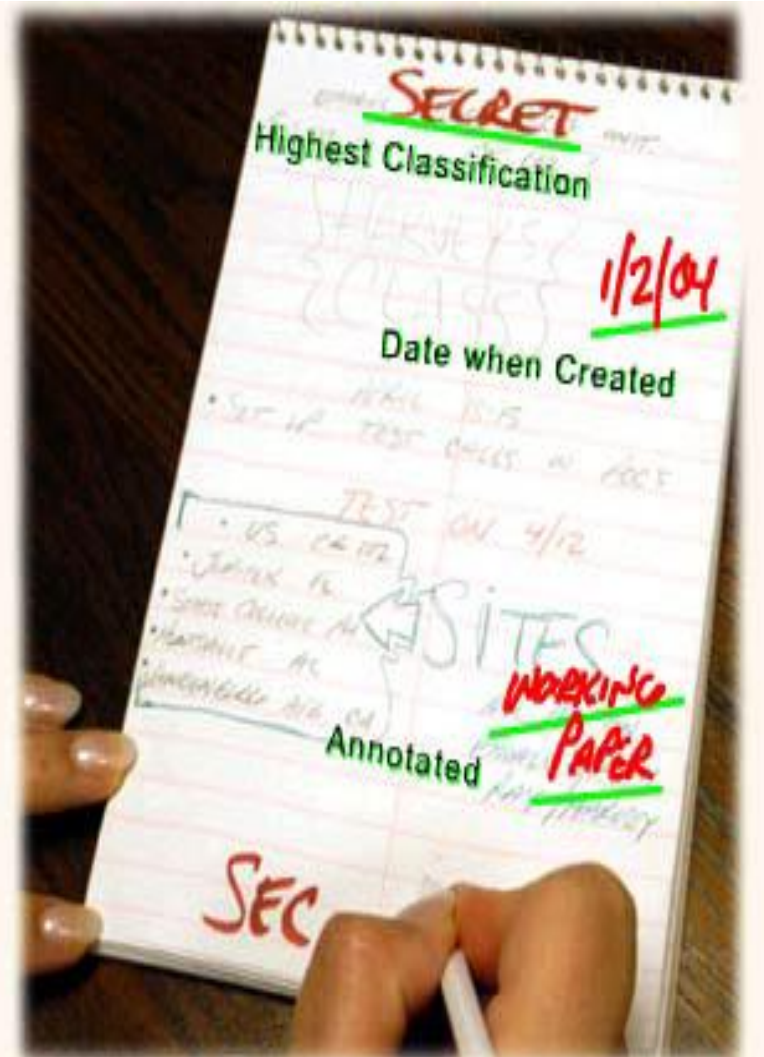
Separator

Dissemination Control

INFORMATION SECURITY

WORKING PAPERS

- Any notes taken from a training course, brief, presentation, conference, including research notes, rough drafts, and similar items that contain classified information.
- These notes shall be:
 - Marked with Highest Classification.
 - Protected in accordance with the measures required for the assigned classification.
 - Dated when created.
 - Annotated “Working Paper”.
 - Marked as Final Document:
 - 180 Days.
 - Transferred.
 - Properly destroyed when no longer needed.
 - Properly transported.
 - Emails are not working papers.
 - All TS “working papers” must be marked and treated as final document.



INFORMATION SECURITY

HANDLING OF CLASSIFIED INFORMATION

Safeguarding during working hours:

- Classified document cover sheets (SF 703, SF 704, or SF 705) will be utilized to prevent unauthorized disclosure and enforce need-to-know.
- Protect all classified items regardless of form to security classification level.
- No discussions of classified topics in public or areas that permit interception.
- Do not open or read classified material where it can be seen by unauthorized persons.

Hand carrying may be authorized only when:

- The classified information is not available at destination.
- The information cannot be transmitted by secure means.
- Carried aboard U.S. carrier with courier card and authorized written approval from the HQMC Security Manager.
- Advanced arrangements have been made to store the information at an authorized facility.



INFORMATION SECURITY

Courier Authorization:

- Appropriately cleared and briefed personnel may be authorized to escort or carry classified material.
- HQMC Security Manager provides written authorization (i.e., DD form 2501-Courier Card, Courier Letter).
- Valid for no more than 2 years.
- Individual should have recurring need.
- Authorization terminated upon transfer, termination, or when escort authority no longer required.

Courier Responsibilities:

- Possess a courier card or courier letter.
- Ensure the recipient(s) have authorized access, need to know, and can properly store the material.
- Ensure material is packaged as described in enclosure 5 of the HQMC IPSP SOP.
- Courier is liable and responsible for the material.
- Never discuss or disclose classified information in public place.
- Never deviate from itinerary.
- Never leave information unattended.
- During overnight stops, ensure material is stored at military facilities, embassies, or cleared contractor facilities.

INFORMATION SECURITY

Reproduction:

- Reproduction of classified material (e.g., paper copies, electronic files, and other materials) shall only be conducted as necessary on classified printers to accomplish the Staff Agency/Activity mission or to comply with applicable statutes or directives.

Removable media:

- The "WRITE" privileges (downloading) to all forms of removable media is prohibited without an approved waiver. Removable media is defined as CD, DVD, Tape, Removable Hard-Disk-Drive, Camera etc. Staff Agencies /Activities requiring SIPRnet "Write-To" removable media capability must submit a waiver request via the HQMC Security Office.

Annual clean out:

- All Staff Agencies/Activities who possess classified material must complete a minimum of one annual review to reduce the inventory of classified documents to “what is absolutely essential”, and report compliance to HQMC Security Manager no later than 1 December of the current year.

INFORMATION SECURITY

Classified Information SHALL NOT be declassified as a result of a spillage or unauthorized disclosure through unofficial open sources (e.g., news media, periodicals, and public web sites). When asked to verify, personnel should:

- Not confirm or deny the existence of potentially classified information in the public domain, and report the incident to your Staff Agency/Activity Security Coordinator or HQMC Security Manager.
- Not contribute to further dissemination of the potentially classified information by accessing websites or social media sites on unclassified IT systems where the information may reside.
- Ensure classified information is only disclosed to personnel with Authorized Clearance, Access, Need to Know, and only via authorized channels and systems.

INFORMATION SECURITY

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

National Policies

- EO 13556
- 32 CFR Part 2002

DoD Policies

- DoDI 5200.48, Controlled Unclassified Information

Definition

- CUI is unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, Government wide policies.

Responsibilities and Penalties for Mishandling

- All personnel of the Department of Defense (DoD) are personally and individually responsible for properly protecting CUI under their custody and control.
- Under 32 CFR Part 2002, DoD military, civilian, contractor personnel may be subject to criminal or administrative sanctions if they knowingly, willfully, or negligently disclose CUI to unauthorized persons.

INFORMATION SECURITY

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Protection

- FOUO and other CUI may NOT be posted to publicly-accessible Internet sites and may NOT be posted to sites whose access is controlled only by domain (e.g., limited to .mil and/or .gov) as such restricted access can easily be circumvented. At a minimum, posting CUI to a website requires certificate-based (e.g., common access card) or password and ID access as well as encrypted transmission using hypertext transfer protocol secure (https) or similar technology.
- During working hours, reasonable steps shall be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving CUI unattended where unauthorized personnel are present). After working hours, CUI may be stored in unlocked containers, desks, or cabinets if Government or Government-contract building security is provided. If such building security is not provided or is deemed inadequate, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, etc.

Public Release

- DoD Information for Public Release requires that a security and policy review be performed on all official DoD information intended for public release that pertains to military matters, national security issues, subjects of significant concern to the DoD and information intended for placement on publicly accessible websites or computer servers. Documents proposed for public release shall first be reviewed at the Staff Agency/Activity levels as required by SECNAVINST 5720.44B “Public Affairs Policy and Regulation” and may or may not be found suitable for public release without higher level consideration.

Threats from Foreign Entities

- There are many threats and techniques that foreign intelligence activities may use to gain access to (CUI).
- Examples: Airport screening or hotel room incursions, Fraudulent purchase requests or market surveys, and attempts to lure personnel into situations that could lead to bribery, blackmail, or extortion.

PERSONAL ELECTRONIC DEVICES (PEDS)



PERSONAL ELECTRONIC DEVICES (PEDS)

MEMORANDUM DTD 22 MAY 2018 FROM THE DEPUTY SECRETARY OF DEFENSE: Mobile Device Restrictions in the Pentagon

- This memorandum establishes restrictions for mobile devices anywhere within the Pentagon that is designated or accredited for the processing, handling, or discussion of classified information.
- Applies to all Department of Defense (DoD) and Office of the Secretary of Defense (OSD) Components ("Components"), as well as military personnel, civilian employees, contractors, and visitors in the Pentagon.

PERSONAL ELECTRONIC DEVICES (PEDS)

Policy:

- Personal and Government mobile devices that transmit, store, or record data are prohibited inside secure spaces within the Pentagon. Mobile devices may be used in common areas and spaces within the Pentagon that are not designated or accredited for the processing, handling, or discussion of classified information.
- Mobile devices must be stored in daily-use storage containers that are located outside the secure space. Devices must be powered off prior to being stored, and must remain powered off until retrieved.
- Signs displaying the prohibition and control procedures are posted outside all secure spaces.

PERSONAL ELECTRONIC DEVICES (PEDS)

Exceptions:

- Medical devices that have been approved based on individualized assessments consistent with the requirements of the Rehabilitation Act of 1973, as amended.
- Mobile devices having minimal storage and transmission capabilities such as key fobs used for medical alert, motor vehicles, or home security systems. This does not apply to fitness trackers that do not contain camera, microphone, cellular, or Wi-Fi technology.

PERSONAL ELECTRONIC DEVICES (PEDS)

Security Violations and Enforcement:

- Failure to abide by the rules promulgated in this memorandum and other applicable laws and regulations regarding security violations involving classified information may subject military members, civilian employees, and contractors to appropriate disciplinary and/or administrative actions, fines, or other appropriate actions, and may result in a review of the individual's security clearance eligibility. Also, military members may be subject to punishment under chapter 47 of the United States Code (also known as "the Uniform Code of Military Justice" or "UCMJ"). The Secretaries of the Military Departments will maintain regulations that make punishable, under Article 92 of the UCMJ, any violation of the restrictions imposed by this memorandum by persons subject to the UCMJ.
- In accordance with applicable rules and regulations regarding physical access to the Pentagon, persons who violate this policy may be denied access thereto.

PERSONAL ELECTRONIC DEVICES (PEDS)

Definitions:

- **Secure Space:** An area that has been designated or accredited for the processing, handling, or discussion of classified information.
- **Mobile Device:** Also referred to as a portable electronic device, a mobile device is a portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices include but are not limited to laptops, tablets, cellular phones, smartwatches, and other devices with these characteristics, but exclude those devices described in 2.c, 2.d, and 2.e.

COMPROMISE AND OTHER SECURITY VIOLATIONS



COMPROMISE AND OTHER SECURITY VIOLATIONS

A security violation is the possible mishandling, loss, or compromise of classified information. Common violations are:

- Electronic spillage (i.e., emailing classified over the NIPRnet, copying classified information on an unclassified copier).
- Unsecure Open Storage Secret (OSS) rooms and/or security containers.
- Sharing classified information at a meeting with un-cleared attendees.

All security incidents involving classified information require a Security Inquiry and/or an Investigation be conducted.

- The Security Inquiry or Investigation will be conducted to determine the facts surrounding the possible mishandling, loss, or compromise of classified information/material.

Report all violations IMMEDIATELY to your Staff Agency/Activity Security Coordinator.

INFORMATION/ PERSONNEL PROTECTION



INFORMATION/ PERSONNEL PROTECTION

Operations Security (OPSEC)

- OPSEC is a systematic process used to mitigate vulnerabilities and protect sensitive, critical, or classified information.
- For more guidance contact Staff Agency/Activity OPSEC Manager/Coordinator.
- Review the USMC Social Media Guide at:
<http://www.marines.mil/usmc/Pages/SocialMedia.aspx>

Antiterrorism Awareness

- Antiterrorism Awareness Program is in place to reduce the vulnerability to terrorist acts and prevent or mitigate hostile actions against personnel, resources, facilities, and critical information. For more information contact HQBN (S3 Office) at 703 614-1471.

Public Affairs (OUSMCC)

- Public release of government information must first be approved by the Office of United States Marine Corps Communications Department at:
 - Community Relations (703) 614-1034.
 - Media (703) 614-4309.

INFORMATION PROTECTION

Controlled Unclassified Information (CUI)

- CUI must be safeguarded to prevent unauthorized public access.
- Protect IT systems processing CUI from unauthorized access.
- For more guidance consult DoDI 5200.48, and SECNAVINST 5510.34.

Disclosure of CUI to Contractors

- Only by a validated need-to-know, contractors may receive CUI unless otherwise restricted.
- Do not disclose privately-owned or proprietary information without the owners consent.

For Official Use Only (FOUO)

- Is not a classification; it is a statutory marking prohibiting the automatic release of information to the public.
- The USMC uses FOUO when referring to CUI.
- For more information please view:
<http://www.hqmc.usmc.mil/USMC%20PRIVACY%20ACT/Index.htm>

INFORMATION ASSURANCE (IA)



INFORMATION ASSURANCE (IA)

- Information assurance protects and defends information and information systems by ensuring their availability, integrity, authenticity, and confidentiality.
- You must complete IA training in the current fiscal year.
- IA training is inclusive of threat identification, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.
- Uniformed personnel will complete MarineNet training curriculum "USMC Cyber Awareness Training", MarineNet code (cyberm0000).
- Civilians will complete all annual cyber awareness training in TWMS. The courses are titled "DOD Cyber Awareness Challenge V1" and "Privacy and Personally Identifiable Information (PII) Awareness Training".
- Contractor personnel will complete MarineNet training curriculum "Civilian Cyber Awareness Training", MarineNet code (cyberc).

FOREIGN TRAVEL PROCEDURES



FOREIGN TRAVEL PROCEDURES

- All personnel possessing a security clearance are required to complete a HQMC Foreign Travel Brief and submit an online Notification of Foreign Travel form before traveling outside of the United States. The brief and the Notification of Foreign Travel Portal can be found at: <https://ehqmcsupport.usmc.mil/sites/mcwar/default.aspx> /
 - To submit a Notification of Foreign Travel form, personnel must have an eHQMC SharePoint Portal account. To request for an account, visit the following site: <https://hqmcsupport.hqi.usmc.mil/sites/HQMCAR/default.aspx>
- Personnel should also visit the Foreign Clearance Guide for specific area of responsibility requirements and the U.S. Department of State website to review Travel Warnings, Travel Alerts, individual country specific information, and to Enroll in the Department of State's Smart Traveler Enrollment Program.
 - Foreign Clearance Guide: <https://www.fcg.pentagon.mil/>
 - Department of State: <https://travel.state.gov/content/passports/en/country.html>
 - Department of State's Smart Traveler Enrollment: <https://step.state.gov/step/>

PHYSICAL SECURITY



PHYSICAL SECURITY

- For “Lock Outs” or when personnel are unable to access an office space, contact Staff Agency/Activity Security Coordinator.
- For “Lock Failures” personnel may only use the emergency lockout contact information posted on the exterior of each HQMC, office space.
- Combination changes for security containers, vaults or rooms (designated for Open Storage) will be changed when first placed in use, when an individual knowing the combination no longer requires access or when the combination has been subjected to compromise.
- To request assistance in changing a combination you may contact Physical Security Section at (703) 614-2305 or (703) 693-2696.

SECURITY TRAINING



SECURITY TRAINING

Derivative Classifier Training

- Personnel who perform derivative classification must complete Derivative Classification Training annually. The training is available at: <http://www.cdse.edu/catalog/information-security.html>

Counterintelligence Awareness

- All HQMC personnel will receive a Counterintelligence Awareness and Reporting brief annually. This briefing will be delivered in person by an agent of the Naval Criminal Investigative Service. For class dates and availability contact your Staff Agency/Activity Security Coordinator

Antiterrorism Awareness Training

- All HQMC personnel are required to complete Level I Antiterrorism Awareness Training annually. Level I Antiterrorism Awareness Training is available at MarineNet code (JATLV10000) or at: <https://atlevel1.dtic.mil/at/>

Security Refresher Training

- All HQMC personnel are required to complete Security Refresher Training annually, which reinforces the policies and procedures covered in their initial and specialized training. The Refresher Brief is available at: <http://www.hqmc.marines.mil/ar/Branches/SecurityProgramsandInformationManagement.aspx>

Additional Training

- Contact your Staff Agency/Activity Security Coordinator for continuous training opportunities for you and your personnel such as short training sessions and online resources

STAFF AGENCY/ACTIVITY SECURITY CONTACT INFORMATION



STAFF AGENCY/ACTIVITY SECURITY COORDINATOR CONTACT INFORMATION

Assistant Commandant of the Marine Corps (ACMC)

- (703) 614-1201

Administration and Resource Management Division (AR)

- (703) 614-1837

Headquarters Marine Corps Aviation Department (AVN)

- (703) 614-2356

Command, Control, Communications and Computers (C4)

- (703)693-3464 or (703) 693-3463

Counsel for the Commandant (CL)

- (703) 614-2150

Commandant of the Marine Corps (CMC)

- (703) 614-1743 or (703) 614-2500

Deputy Commandant for Information (DCI)

- (703)639-8691

Director of Marine Corps Staff (DMCS)

- (703) 697-1668

Force Preservation Directorate (G10)

- (703) 692-5374

Headquarters and Service Battalion (H&S BN)

- (703) 614-2014

Health Services (HS)

- (703) 604-4602

Installations and Logistics (I&L)

- (703) 614-6706 or (703) 695-8655

Inspector General of the Marine Corps (IG)

- (703) 604-4626

Intelligence Department (Intel)

- (703) 614-2522

Staff Judge Advocate to the Commandant (JA)

- (703) 693-8673 or (703) 693-8401

Manpower and Reserve Affairs (M&RA)

- (703) 784-9012 (QUAN) or (703) 695-1929 (PNT)

Marine Corps Recruiting Command (MCRC)

- (703) 784-9430

Office of Legislative Affairs (OLA)

- (703) 614-1686 or (703) 692-0199

Office of Marine Forces Reserve (OMFR)

- (703) 604-4563

Office of Marine Corps Communications (OMCC)

- (703) 614-8010 or (703) 614-2445

Plans, Policies and Operations (PP&O)

- (703) 614-8497 or (703) 614-8487

Programs and Resources (P&R)

- (703) 614-1080 or (703) 614-3596

Chaplain of the Marine Corps (REL)

- (703) 614-3673

Safety Division (SD)

- (703) 604-4463

Special Projects Directorate (SPD)

- (703) 614-1515

Special Security Office SSO

- (703) 614-3350

Congratulations!!

**You have completed the Headquarters Marine Corps
Security Orientation Brief.**

Please proceed to the next page for your completion certificate.

Certificate of Completion



I, _____, acknowledge that I have
completed the HQMC Security Orientation Brief
on

DATE

(Click in date box and then out to insert date)

MEMBER'S SIGNATURE

**SECURITY COORDINATOR
SIGNATURE**