# SECURITY ORIENTATION

---

## Administration and Resource Management Division, Security Programs and Information Management Branch

**HQMC Security Manager: Kevin J. White**
**HQMC Assistant Security Manager: Michael J. Watson**
**Phone number: (703) 614-3609**

# 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
- Your Reporting Responsibilities
- Information Security
- Security Violations
- Information Protection
- Information Assurance
- Foreign Travel Procedures
- Antiterrorism/Force Protection
- 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<br>• We must report **ANY** information that may affect clearance eligibility |
| What it is not | • Automatic grounds to terminate employment.<br>• 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 allegiance to the U.S.
- Foreign influence
- Foreign preference
- Criminal Sexual behavior
- Personal conduct
- Financial considerations
- Alcohol consumption
- Drug involvement
- Emotional, mental, personality disorders
- Criminal conduct
- Security violations
- Outside activities
- Misuse of IT systems

NOTE: 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

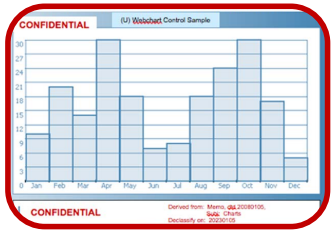
Classified information or material will only be viewed or processed when adequate protection conditions have been met to prevent any type of compromise.

| 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:<br>-Cross-cut shredding.<br>-Mutilation.<br>-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:

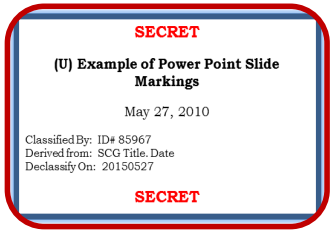



Charts

Maps, Photographs

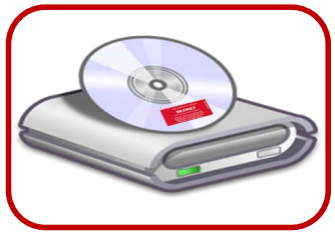
Publications/Manuals

Documents, Reports, Messages



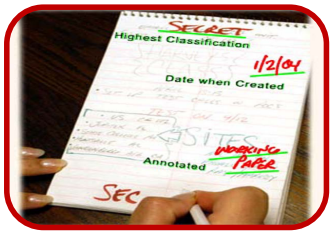

Briefing/Presentation slides

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/marking-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 every 2 years.
- 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?

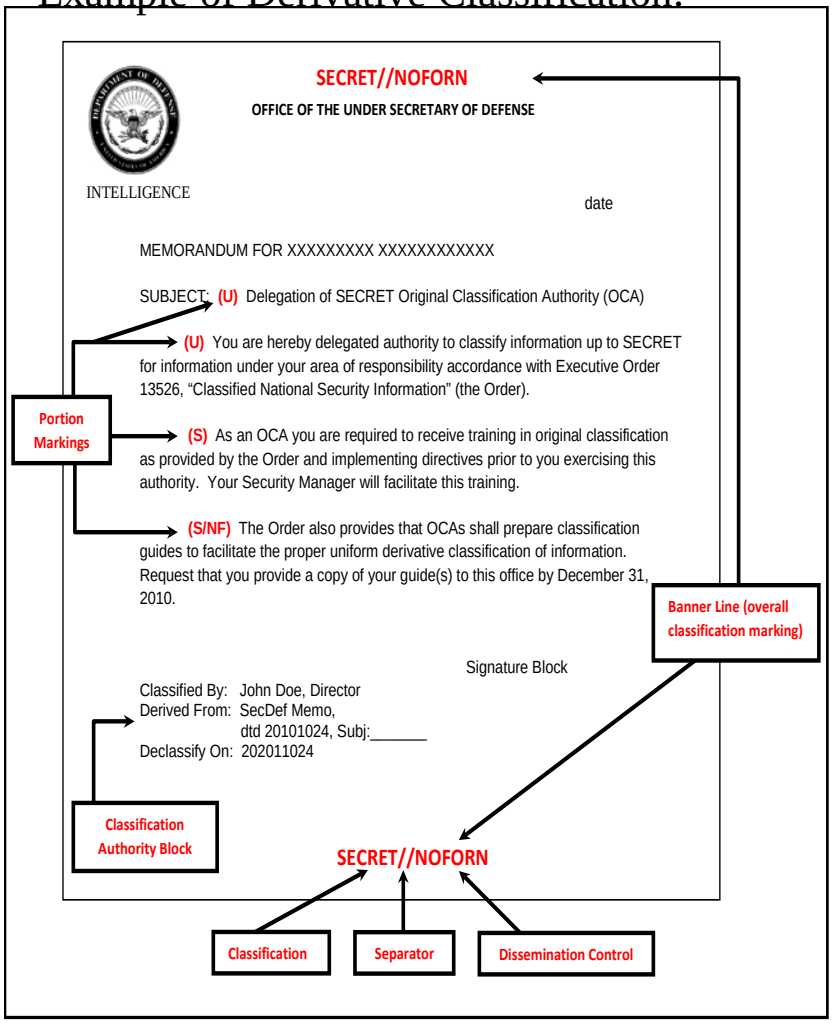
- Examples of the required markings are outlined on slides 25 and 26.

# 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).

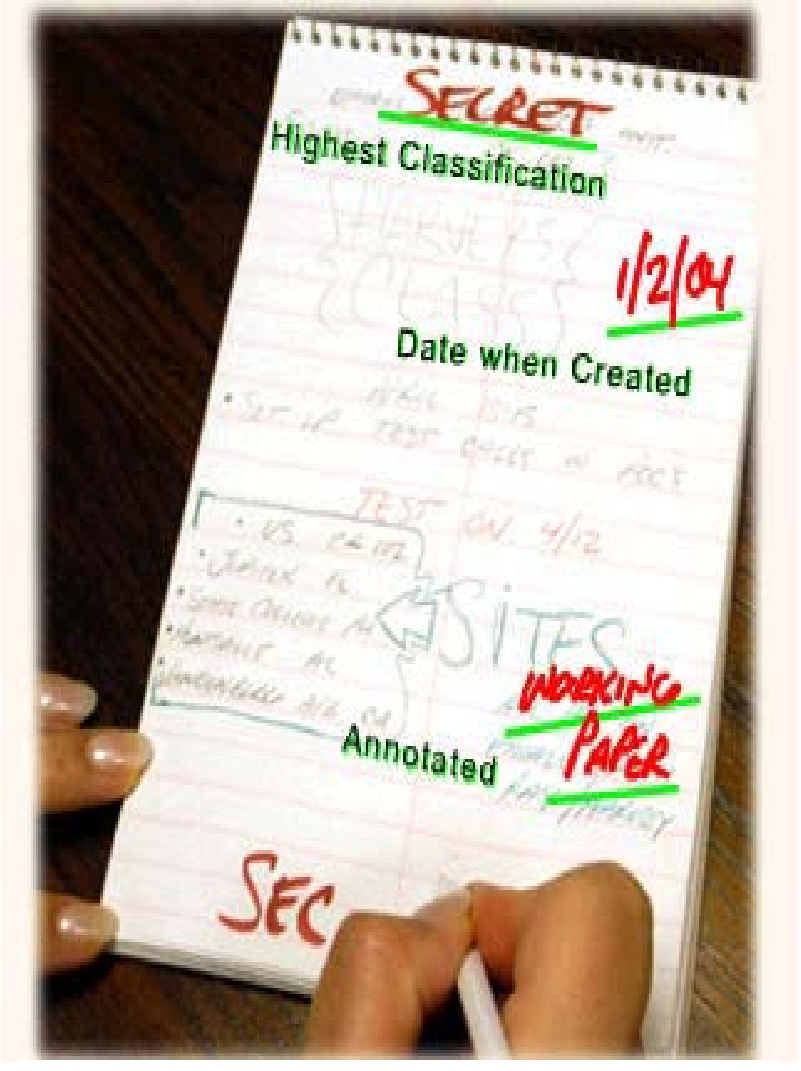
Example of Derivative Classification:



# 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 wavier. 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.

# 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 <u>IMMEDIATELY</u> 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 DoD M-5200.01, Vol 4 and SECNAVINST 5510.34.

## Disclosure of CUI to Contractors

- Only by a validated need-to-know, contractors may receive CUI unless otherwise restricted and a DD 2345.
- 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 eligibility are required to report foreign travel and foreign contacts to their Staff Agency/Activity Security Coordinator.
- Reporting will be accomplished by utilizing the "Notification of Foreign Travel Form" and “Foreign Contact Interview Form.” Security Coordinators will submit completed forms via the Security Mailbox at smb.hqmc.security@usmc.mil.
- All personnel must receive a foreign travel briefing. Personnel can schedule a briefing by contacting Headquarters and Service Battalion, (S-3 Office), at (703) 614-1471. General Officers and Senior Executive Service, will receive foreign travel briefing based on the area traveling to via desk side, email, or in person. For VIP scheduling contact HQSVC BN, S-3 Office at (703) 614-1471.
- Staff Agency/Activity Security Coordinators are to ensure personnel conducting foreign travel to USCENTCOM, USSOUTHCOM and USPACOM AOR, complete the Isolated Personnel Report (ISOPREP). Questions regarding completion and submission of the ISOPREP can be addressed to PO-SOD at (703) 571-1015.
- Visit https://www.fcg.pentagon.mil/ for information on what you need prior to travel.
- Visit http://travel.state.gov/ for passport and other travel guidance.

# 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 every 2 years. 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 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

Director of Marine Corps Staff (DMCS)
- (703) 697-1668

Marine Corps Expeditionary Energy Office (E2O)
- (571) 256-8781

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 the United States Marine Corps Communications (OUSMCC) - (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

HQMC Contracting Officer Representative
- (703) 614-3609

HQMC NATO Control Point
- (703) 614-3609

# Certificate of Completion

**THIS ACKNOWLEDGES THAT**

**(LAST NAME, FIRST NAME MI)**

**HAS SUCCESSFULLY COMPLETED THE HQMC SECURITY ORIENTATION BRIEF**

**SECURITY COORDINATOR SIGNATURE**

**DATE**