Information and Personnel Security Program (IPSP) Annual Refresher

---

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

HQMC Security Manager: Kevin J. White
HQMC Assistant Security Manager: Virginia Z. Bustillo
Phone Number: (703) 614-3609

PURPOSE

This security brief is a refresher of the basic security information and common procedures that you should be aware of while assigned to Headquarters Marine Corps (HQMC).

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.

TOPICS

- HQMC Security Policies and Procedures Update
- Counterintelligence
- Continuous Evaluation Program
- Your reporting responsibilities
- Information Security
- HQMC Security concerns
- Non-Disclosure Agreement (NDA) SF 312
- Staff Agency/Activity POCs

HQMC SECURITY POLICIES AND PROCEDURES UPDATE

HQMC SECURITY POLICIES AND PROCEDURES UPDATE

HQMC IPSP Security Operating Procedures (SOP) August 06, 2013

- This SOP represents the minimum requirements for HQMC IPSP program management and is published under the cognizance of the HQMC Security Manager.
- Staff Agency/Activity heads may impose more stringent security requirements within their Staff Agency/Activity if desired, but not more lenient.
- Security Note 02-15 Policy for Handling and Safeguarding NATO Material, supersedes enclosure (5) section (d), of the HQMC IPSP SOP.
- All military, civilian and government contractor personnel assigned to HQMC will comply with the provisions of the HQMC IPSP SOP.

HQMC SECURITY POLICIES AND PROCEDURES UPDATE

Security Notes

- HQMC Security Manager periodically disseminates Security Notes to all Staff Agencies/Activities concerning new or modified security related information, changes in procedures, problem areas, or to direct attention to specific matters.
- 01-14: 2013 Security Coordinator of the Year Recipient.
- 02-14: Personnel Security Eligibility Determination.
- 03-14: Sponsorship for DoD Building Pass and Visitor No Escort Required Building Pass.
- 01-15: 2014 Security Coordinator of the Year Recipient.
- 02-15: Policy for Handling and Safeguarding NATO Material.

COUNTERINTELLIGENCE

COUNTERINTELLIGENCE

What is counterintelligence?

- Is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, assassinations conducted for or on behalf of foreign powers, organizations, persons, or international terrorist activities.

What can be a threat?

- Foreign governments, competitors, or insiders (i.e., coworker).

How is information collected?

- Direct and indirect requests for information (e.g., e-mails, phone calls, conversations). A simple request can net a piece of information helpful in uncovering a larger set of facts.
- Solicitation or Marketing of services – foreign owned companies pursue business relationships to gain access to sensitive or classified information, technologies, or projects.
- Public Venues – conferences, conventions, symposiums and trade shows offer opportunities for adversaries to gain access to information and experts in dual-use and sensitive technologies.
- Official Foreign Visitors and Exploration of Joint Research – foreign government organizations, including intelligence and security services, consistently target and collect information through official contacts and visits.
- Foreign Targeting of U.S. Travelers Overseas – collection methods include everything from soliciting information during seemingly innocuous conversations and eavesdropping on private telephone conversations, to downloading information from digital storage devices.

To counter these threats, it is important to <u>REPORT</u> these occurrences. Any vulnerability, no matter how seemingly inconsequential, should be reported to Staff Agency/Activity Security Coordinator as soon as possible.

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's not	• Automatic grounds to terminate employment • Automatically revoking eligibility
Who's it for	• It applies to **ALL** contractor, military, and civilian personnel
Who's responsible for reporting	• **EVERYONE**
What's reported	• Information pertaining to the 13 adjudicative guidelines, as identified on slide 12

CONTINUOUS EVALUATION PROGRAM

The 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 balance maintained regarding individual's needs and national security issues; report to 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

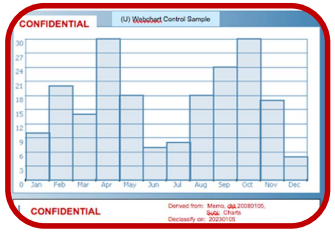
NOTE: Combat veterans or victims of sexual assault suffering from Post Traumatic Stress Disorder (PTSD), who seek mental health care will not, in and of itself adversely impact that individual's ability to obtain or maintain their eligibility. **PTSD IS NOT A DISQUALIFYING FACTOR.**

INFORMATION SECURITY

INFORMATION SECURITY

TYPES OF CLASSIFIED INFORMATION

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

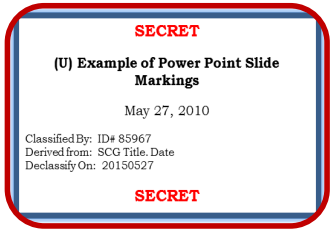


Charts

Maps, Photographs

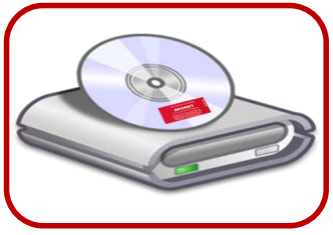
Publications/Manuals

Documents, Reports, Messages



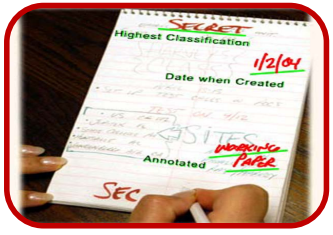
Briefing/Presentation slides

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

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?

- Banner markings must be marked on the top and bottom of the front page or title page and outside back cover (if any). Internal pages may be marked with the banner markings of the document or the highest classification of the information contained on that page.
- 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; “(List Sources)”.
- Declassification instructions, YYYYMMDD format.
- Downgrading instructions, if applicable.
- Portion Markings.
- Dissemination Control notices (front page).

INFORMATION SECURITY

TYPES OF CLASSIFICIATION

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:

- The incorporating, paraphrasing, restating or generating in a new form information that is already classified.
- 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)

- Are the primary source guide for derivative classification and are prepared by an OCA. An SCG contains a collection of precise, comprehensive guidance about specific program, system, operation, or weapons system identifying what elements of information are classified. For each element of information, the SCG includes its 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

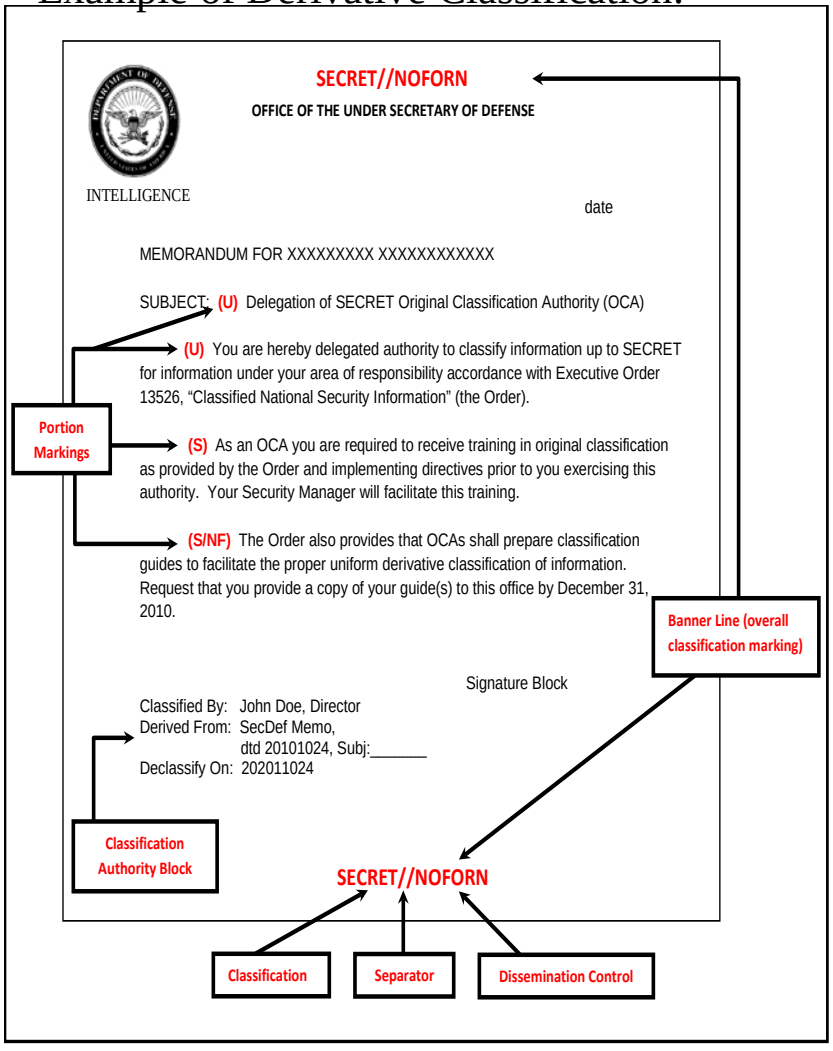
- Provides classification guidance to contractors performing on classified contracts. The form identifies the level of information they will need to access, the required level of security clearance for access, and the performance requirements.

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).

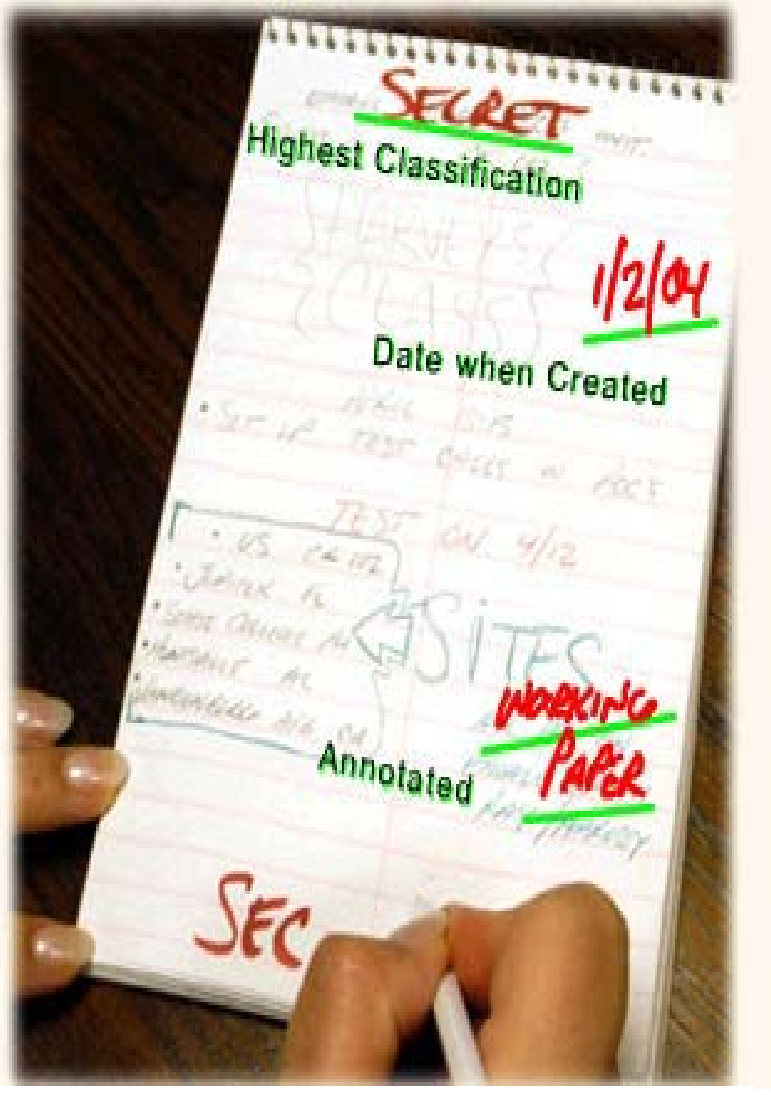
Example of Derivative Classification:



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

STANDARD FORMS (SF)

Purpose

- These forms serve the purpose of providing identification, control, and safeguarding of classified and sensitive information.
- For instructions and use of all these standard forms refer to the HQMC IPSP SOP. Note: Not all inclusive.

SF 700

- Provides the names, addresses and telephone numbers of employees who are to be contacted if the security container to which the form pertains is found open and unattended.

SF 701

- Provides a systematic means to make a thorough end-of-day security inspection for a particular work area and to allow for employee accountability in the event irregularities are discovered.

SF 702

- Provides a record of the names and times persons have opened, closed and checked a particular container that holds classified information.

SF 710

- In a mixed environment in which classified and unclassified information are being processed or stored, SF 710 is used to identify media containing unclassified information. Its function is to aid in distinguishing among those media that contain either classified or unclassified information in a mixed environment.

SF 700

SF 701

SF 702

SF 710

INFORMATION SECURITY

ADDITIONAL GUIDANCE

Safeguard reminders:

- Classified information or material will be used only where there are facilities or conditions adequate to prevent unauthorized persons from gaining access to the information.
- Persons in possession of classified material are responsible for safeguarding the material at all times.
- Individuals will not remove classified material from designated offices or work areas except in the performance of their official duties and under the conditions required by the HQMC IPSP SOP.
- When it is mission critical for individuals to remove classified information and materials for work at home, specific security measures and approvals are required see HCMC IPSP SOP for guidance.
- Sanitize all office spaces where classified material is stored, processed, or discussed when uncleared personnel are performing repairs, routine maintenance, or cleaning.

Training and support:

- ARS provides Staff Agencies/Activities continuous training opportunities for agency personnel, please contact the ARS Security Help Desk at (703) 614-3609 for avalability.

HQMC SECURITY CONCERNS

HQMC SECURITY CONCERNS

IT Spillages:

- Classified IT data spills occur when classified data is introduced either onto an unclassified information system, or to an information system with a lower level of classification, or to a system not accredited to process data of that restrictive category (i.e. Inserting a Secret CD into a unclassified computer, e-mailing classified information over the NIPRnet or making copies of a Secret document on an unclassified copier).

Classified material improperly marked:

- Mismarked information can lead to serious damage of national security which can be exploited by our adversaries.
- Remember the purposes of marking:
  - Alerts the holder to the presence of classified information.
  - Eliminates any doubt about the classification level.

Prevention:

- **Personnel must commit to a disciplined practice of information security and continue to refresh themselves so they don't become a point of vulnerability.**
- **Anyone with access to classified information is <u>individually responsible</u> for safeguarding that information!**

HQMC SECURITY CONCERNS

DOD credentials left unattended:

- The Common Access Card (CAC) technology allows for rapid authentication and enhanced security for all physical and logical access. CAC offers a variety of functions, the credentials embedded in the CAC can give access to a variety of systems.
- Don't leave unattended CAC in computer.
- Don't write pin down anywhere.

Combinations:

- Writing combinations on a "sticky note" makes it very easy for unauthorized personnel to obtain access to classified material.
- Combinations are classified = classified material being safeguarded.
- When to change combinations:
  - Upon initial use of container.
  - When a person with knowledge of combination, no longer requires access.
  - Combination may have been compromised.

Reminders:

- **Know the tools that are available (i.e., Standard Forms, Containers, etc).**
- **Know the procedures that are in place to deter or delay inadvertent disclosure and spoil attempts to compromise classified material.**

NON-DISCLOSURE AGREEMENT (NDA) SF 312

NON-DISCLOSURE AGREEMENT (NDA) SF 312

What is an NDA SF 312?

- An official authorized contract between an individual and the United States (U.S.) Government signed by the individual as a condition of access to classified national security information. The NDA specifies the security requirements for access and details the penalties for non-compliance.

What is its purpose?

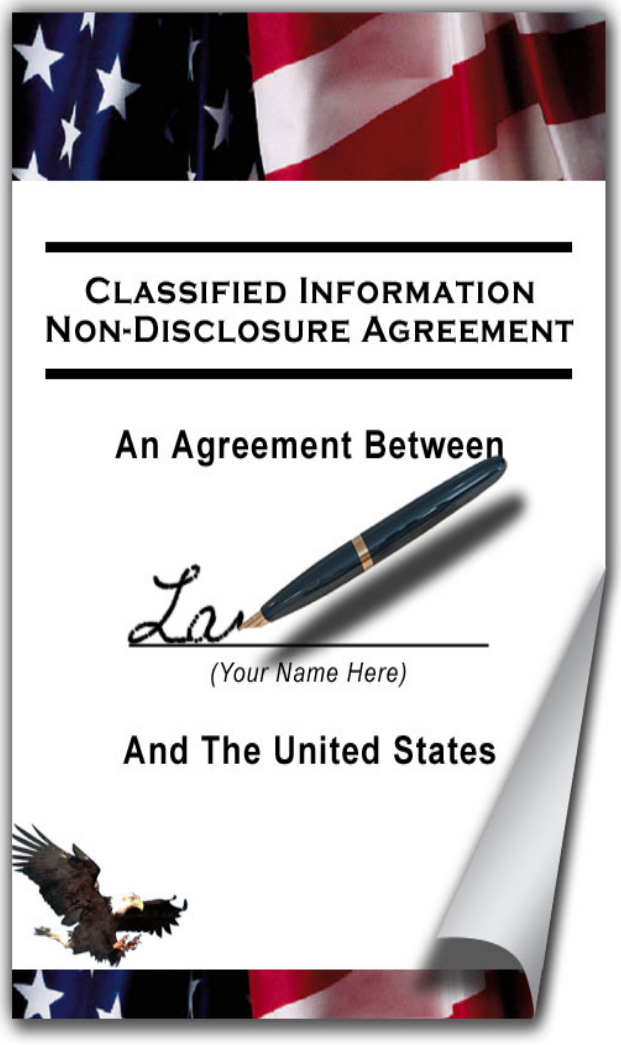
- The SF 312 is to inform employees of (a) the trust that is placed in them by granting them access to classified information; (b) their responsibilities to protect that information from unauthorized disclosure; and (c) the consequences that may result from their failure to meet those responsibilities.

Who signs the SF 312?

- Before being granted access to classified information, all personnel must sign SF 312, “Classified Information Nondisclosure Agreement”. Electronic signatures will not be used to execute the SF 312.

What are the penalties?

- The penalties for violating this agreement are severe and may include the loss of accesses, termination of position, fines, and imprisonment.



STAFF AGENCY/ACTIVITY POCS

STAFF AGENCY/ACTIVITY SECURITY POC'S

See below for your 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
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 IPSP ANNUAL REFRESHER

SECURITY COORDINATOR SIGNATURE

DATE