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: Orlando Roman

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 and property, both Classified and Controlled Unclassified Information (CUI), is the responsibility of all personnel, regardless of how it was obtained or what form it takes.

TOPICS

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

UPDATES OF HQMC SECURITY POLICIES AND PROCEDURES

UPDATES OF HQMC SECURITY POLICIES AND PROCEDURES

Revised the HQMC IPSP Security Operating Procedures (SOP)

- 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 requirements within their Staff Agency/Activity; if desired, but not more lenient.
- All military, civilian and government contractor personnel assigned to HQMC will comply with the provisions of the HQMC IPSP SOP.

UPDATES OF HQMC SECURITY POLICIES AND PROCEDURES

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.
- 01-13: Physical Security Lockout Procedures.
- 02-13: Personnel, Physical, Information and Communications, Security System (PPICSS) Deployment and Implementation.
- 03-13: HQMC Office Space Emergency After Hours Procedures.
- 04-13: HQMC Information, Personnel and Physical Security Assessment Program.
- 05-13: Cancellation of Obsolete Security Notes.
- 06-13: Residential Storage of National Security Information (NSI).
- 07-13: HQMC Security Education, Training, and Awareness Program.

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 information may be obtained:

- 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 seek business relationships to enable them 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 eliciting information during seemingly innocuous conversations, eavesdropping on private telephone conversations, to downloading information digital storage devices.

To counter these threats, it is important to REPORT these occurrences. Any vulnerability, no mater 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:

- Allegiance to the US
- 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

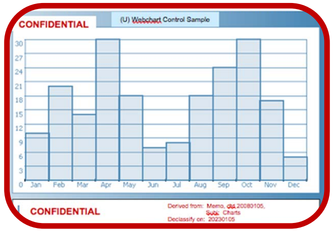
NOTE: Combat veterans or victims of sexual assault suffering from Post Traumatic Stress Disorder (PTSD), who seek mental health care will not, in and of itself adversely impact that individual’s ability to obtain or maintain their eligibility. **PTSD IS NOT A DISQUALIFYING FACTOR.**

INFORMATION SECURITY

INFORMATION SECURITY

TYPES OF CLASSIFIED INFORMATION

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


CONFIDENTIAL

(U) Webchart Control Sample

CONFIDENTIAL

Derived from: Memo, dtd 20080105,
Subj: Charts
Declassify on: 20230105

Charts

SECRET

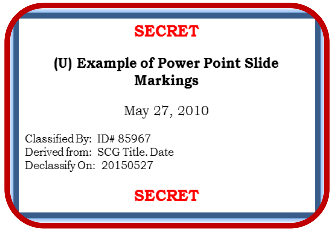
Classified by: John Smith, ABC Agency
Derived from: World Map Collection dtd, 20071210
Declassify on: 20171210

SECRET

Maps, Photographs

Publications/Manuals

Documents, Reports, Messages


SECRET

(U) Example of Power Point Slide Markings

May 27, 2010

Classified By: ID# 85967
Derived from: SCG Title. Date
Declassify On: 20150527

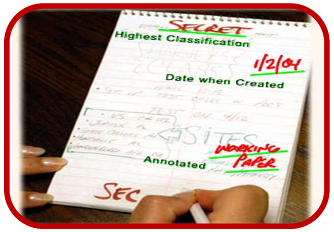
SECRET

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 classification level and material to ensure 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.

INFORMATION SECURITY

TYPES OF CLASSIFCIATION

Original:

- An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.
- Authority designated by SECNAV authorizing officials to originally classify information at a given level.
- 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.
- Are identified on documents they have derivatively classified.
- List all sources.

INFORMATION SECURITY

AUTHORIZED SOURCES

Security Classification Guides (Prepared by an OCA)

- Identifies exact classification/downgrading/ declassification and special handling caveats.

Properly Marked Source Documents

- Memo, message, letter, email, etc.

DD 254

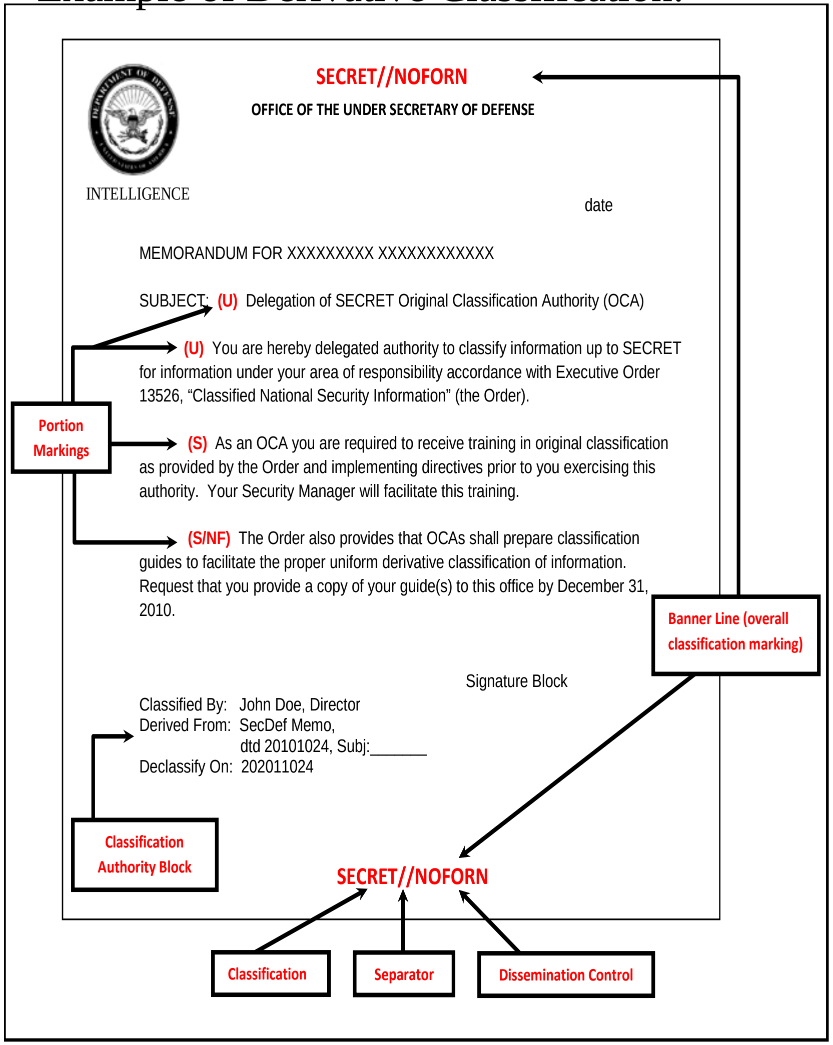
- Conveys applicable classification guidance for contractors on a classified contract.

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:



SECRET//NOFORN

OFFICE OF THE UNDER SECRETARY OF DEFENSE

INTELLIGENCE

date

MEMORANDUM FOR XXXXXXXXX XXXXXXXXXXXX

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

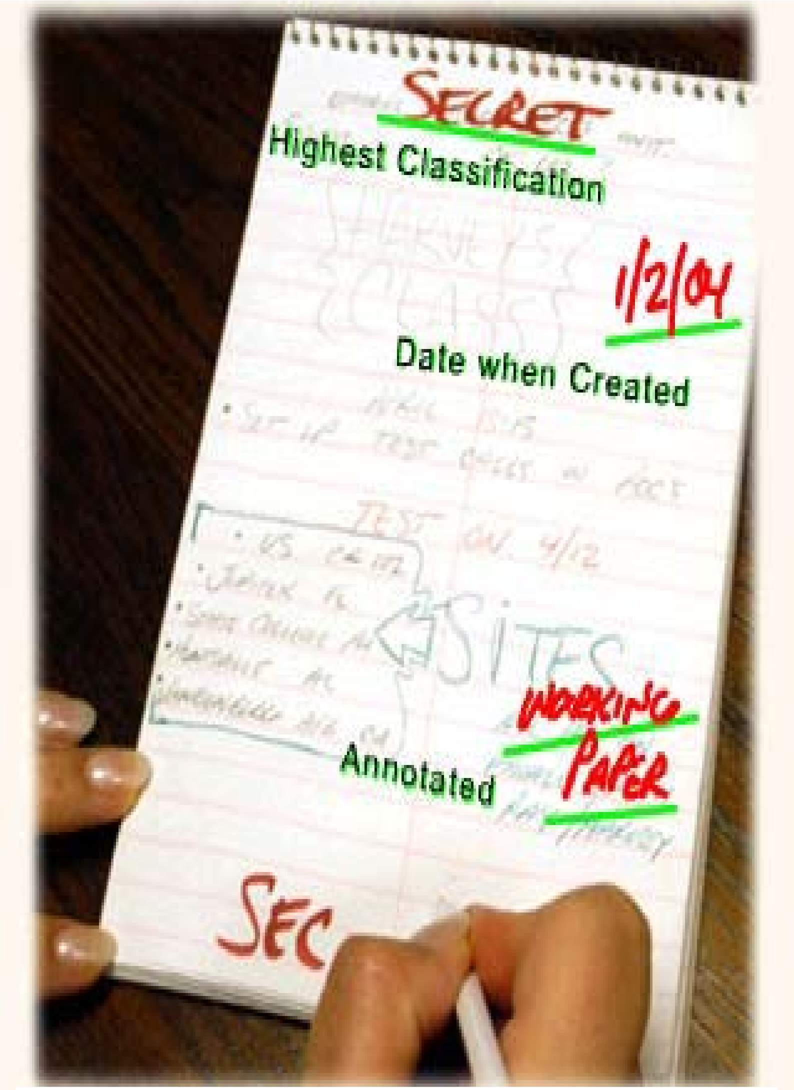
Portion Markings
Banner Line (overall classification marking)
Classification Authority Block
Classification
Separator
Dissemination Control

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

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.



UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

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.

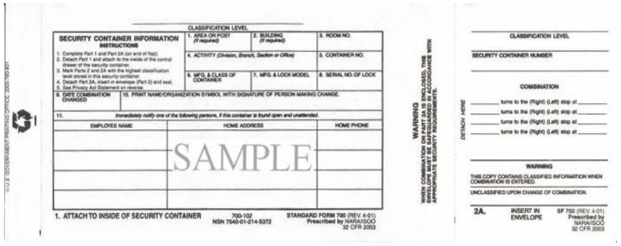
SF 702

- 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



CLASSIFICATION LEVEL

SECURITY CONTAINER INFORMATION
INSTRUCTIONS
1. Complete Part 1 and Part 2A (on end of flap).
2. Detach Part 1 and attach to the inside of the control drawer of the security container.
3. Mark Parts 2 and 2A with the highest classification level stored in this security container.
4. Detach Part 2A, insert in envelope (Part 2) and seal.
5. See Privacy Act Statement on reverse.

1. AREA OR POST (If required)
2. BUILDING (If required)
3. ROOM NO.
4. ACTIVITY (Division, Branch, Section or Office)
5. CONTAINER NO.
6. MFG. & CLASS OF CONTAINER
7. MFG. & LOCK MODEL
8. SERIAL NO. OF LOCK
9. DATE COMBINATION CHANGED
10. PRINT NAME/ORGANIZATION SYMBOL WITH SIGNATURE OF PERSON MAKING CHANGE.
11. *Immediately notify one of the following persons, if this container is found open and unattended.*

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE
	SAMPLE	

1. ATTACH TO INSIDE OF SECURITY CONTAINER
700-102
NSN 7540-01-214-5372
STANDARD FORM 700 (REV. 4-01)
Prescribed by NARA/ISOO
32 CFR 2003

U.S. GOVERNMENT PRINTING OFFICE: 2003-760-601

WARNING
WHEN COMBINATION ON PART 2A IS ENCLOSED, THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS.

DETACH HERE

CLASSIFICATION LEVEL

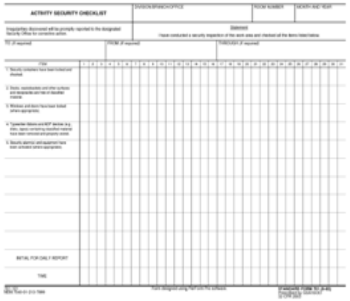
SECURITY CONTAINER NUMBER

COMBINATION
____ turns to the (Right) (Left) stop at ____
____ turns to the (Right) (Left) stop at ____
____ turns to the (Right) (Left) stop at ____
____ turns to the (Right) (Left) stop at ____

WARNING
THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN COMBINATION IS ENTERED.
UNCLASSIFIED UPON CHANGE OF COMBINATION.

2A. INSERT IN ENVELOPE
SF 700 (REV. 4-01)
Prescribed by NARA/ISOO
32 CFR 2003

SF 701



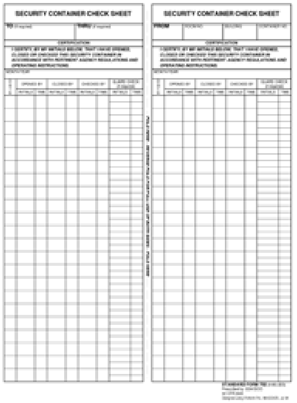
ACTIVITY SECURITY CHECKLIST
DIVISION/BRANCH/OFFICE
ROOM NUMBER
MONTH AND YEAR

Statement

INITIAL FOR DAILY REPORT

TIME

SF 702



SECURITY CONTAINER CHECK SHEET

CERTIFICATION

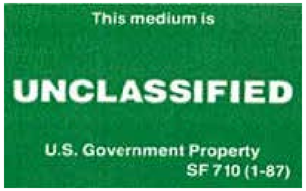
OPENED BY
CLOSED BY
CHECKED BY

SECURITY CONTAINER CHECK SHEET

CERTIFICATION

OPENED BY
CLOSED BY
CHECKED BY

SF 710



This medium is

UNCLASSIFIED

U.S. Government Property
SF 710 (1-87)

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 (e.g., IT equipment and associated storage media) for work at home, specific security measures and approvals are required see Security Note 06-13 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 e.g. derivative classification, safeguarding, PME's and online resources.

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, and/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 SF 312?

- The SF 312 is a contractual agreement between the U.S. Government and a cleared employee, in which the employee agrees never to disclose classified information to an unauthorized person.

What is its purpose?

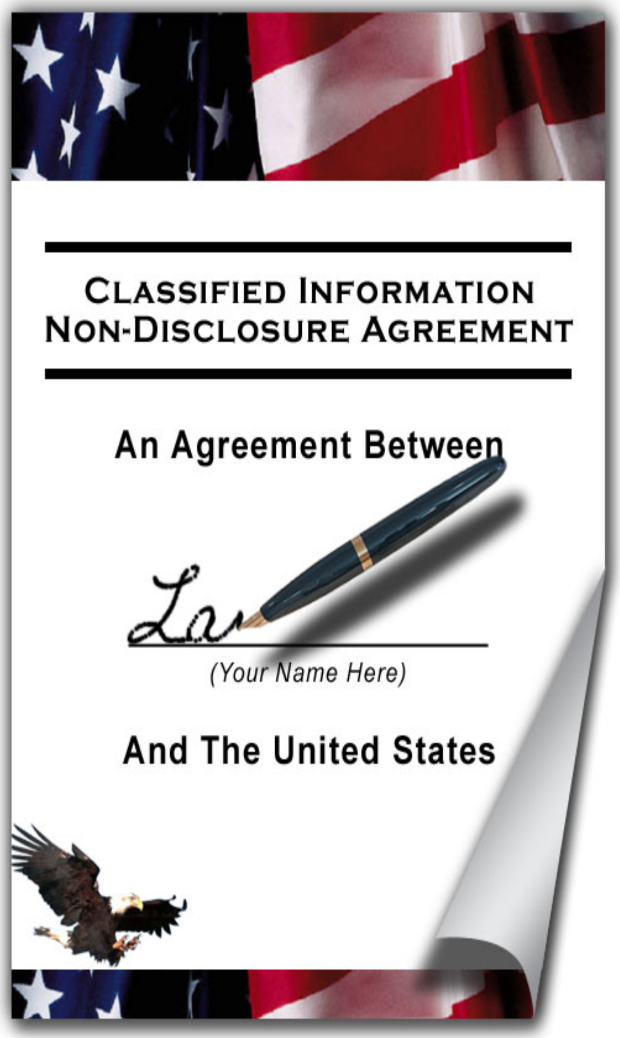
- The SF 312 is to inform employees of (a) the trust that is placed in them by providing them access to classified information; (b) their responsibilities to protect that information from unauthorized disclosure; and (c) the consequences that may result from their failure to meet those responsibilities.

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.



CLASSIFIED INFORMATION NON-DISCLOSURE AGREEMENT

An Agreement Between

(Your Name Here)

And The United States

STAFF AGENCY/ACTIVITY POCS

STAFF AGENCY/ACTIVITY SECURITY POC'S

To contact your staff agency/activity security POC by email please select your agency below:

- Assistant Commandant of the Marine Corps (ACMC)
- Administration and Resource Management (AR)
- Marine Aviation (AVN)
- Command, Control, Communications and Computers (C4)
- Counsel for the Commandant (CL)
- Commandant of the Marine Corps (CMC)
- Director of Marine Corps Staff (DMCS)
- Marine Corps Expeditionary Energy Office (E02)
- Headquarters Battalion (HQBN)
- Health Services (HS)
- Installations and Logistics (I&L)
- Inspector General of the Marine Corps (IG)
- Intelligence Department (Intel)

- Staff Judge Advocate to the Commandant (JA)
- Manpower and Reserve Affairs (M&RA)
- Marine Corps Recruiting Command (MCRC)
- Office of Legislative Affairs (OLA)
- Office of Marine Forces Reserve (OMFR)
- Division of Public Affairs (PA)
- Plans, Policies and Operations (PP&O)
- Programs and Resources (P&R)
- Chaplin of the Marine Corps (REL)
- Safety Division (SD)
- Special Projects Directorate (SPD)
- HQMC Contracting Officer Representative
- HQMC NATO Control Point

Certificate of Completion

THIS ACKNOWLEDGES THAT

(LAST NAME, FIRST NAME MI)

HAS SUCCESSFULLY COMPLETED THE
HQMC IPSP ANNUAL REFRESHER

SECURITY COORDINATOR
SIGNATURE

DATE