



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
5500
ARS

JUL 07 2009

DIRECTOR, MARINE CORPS STAFF MEMORANDUM 02-09

From: Director, Marine Corps Staff
To: All HQMC Departments, Staff Agencies, and Offices
Commanding General, Marine Corps Recruiting Command
Subj: HEADQUARTERS U.S. MARINE CORPS (HQMC) INFORMATION AND
PERSONNEL SECURITY PROGRAM (IPSP) STANDING OPERATING
PROCEDURES (SOP)

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) MCO P5510.14
(d) MCO 5510.17
(e) MCO 5510.20A
(f) SECNAVINST 5720.42F
(g) OPNAVINST 2221.5C
(h) DoD 5220.22-M (NISPOM)
(i) MARADMIN 624/08

Encl: (1) Responsibilities
(2) Program Management
(3) Personnel Security
(4) Information Security
(5) Industrial Security

1. Purpose. To publish policies and procedures for handling, processing and safeguarding classified materials at HQMC. The policies and procedures in this SOP represent the minimum requirements for the handling and storage of classified information. Staff Agency/Activity heads may choose to impose more stringent requirements within their staff agency/activity.

2. Background. Proper control and accountability of classified material enhances HQMC's ability to access needed documents and decreases the possibility of compromise of classified material. This SOP is published under the cognizance of the HQMC Security Manager and will be maintained by all HQMC Staff Agencies and Activities.

3. Applicability. Applicable to HQMC Staff Agencies/Activities and Marine Corps Recruiting Command (MCRC).

Subj: HEADQUARTERS U.S. MARINE CORPS (HQMC) INFORMATION AND
PERSONNEL SECURITY PROGRAM (IPSP) STANDING OPERATING
PROCEDURES (SOP)

4. Action. All military and civilian personnel and government contractors working in HQMC spaces, will comply with the provision of this document. This SOP cannot address every conceivable situation that might arise in day-to-day operations. When confronted by situations, the basic principles of personnel and information security, coupled with sound judgment, guidance from appointed security personnel and common sense should be exercised when dealing with classified information.

5. This document is to be used in conjunction with references (a) through (i). Though not all encompassing, this brief overview covers key points you should be aware of as Security Coordinators. Staff Agencies/Activities will comply with guidance provided by the HQMC Security Manager. Questions regarding IPSP should be directed to HQMC Security (ARS), at 703-614-2320 or by e-mail at smb.hqmc.security@usmc.mil.



R. S. KRAMLICH

HQMC IPSP SOP

Responsibilities

1. Per reference (a), the Head, Security Programs and Information Management Branch (ARS) is responsible for the formulation, implementation and enforcement of information and personnel security programs, their effectiveness, and compliance with all directives issued by higher authority.

2. Per reference (a), the HQMC Security Manager/Assistant Security Manager are the principal advisors for information security, personnel security, industrial security, security education and training within this headquarters and MCRC. The Security Manager/Assistant Security Manager are responsible for:

a. The management, formulation, implementation and enforcement of security policies and procedures for the protection of Classified Military Information (CMI), Controlled Unclassified Information (CUI), sensitive information, For Official Use Only (FOUO) originated by and or under the cognizance of HQMC and MCRC, in connection with the duties outlined in reference (a).

b. Developing basic policy and procedures for the classification, dissemination, transmission, control, accounting, storage, and protection of collaterally classified material at HQMC/MCRC.

c. Coordinating with the heads of HQMC Staff Agencies/Activities to ensure that all personnel who handle classified information have the proper security clearance, and that requests for personnel security investigations are properly prepared and submitted.

d. Providing advice to heads of Staff Agencies/Activities on Information and Personnel Security Program (IPSP) matters affecting HQMC.

e. Conducting both announced and unannounced security visits on staff agencies/activities to evaluate the effectiveness of the security program and ensure the staff agency/activity is in compliance with this SOP and higher directives.

f. Establishing a HQMC security education program.

HQMC IPSP SOP

3. HQMC Top Secret Control Officer (TSCO) (ARS)

a. The HQMC TSCO is responsible for the receipt, custody, accounting, reproduction, and disposition of Top Secret material received or originated by this Headquarters, with the exception of Sensitive Compartmented Information (SCI) material which is controlled by the Special Security Office (SSO). All other Top Secret material will be controlled per the current edition of references (a) through (b) and this SOP.

b. Per reference (b), the duties of the HQMC Top Secret Control Officer (TSCO) will be assigned in writing by the DirAR Division. Designees must be an officer/enlisted E-7 or above or a civilian employee, YA-2 or YC-2 or above. The TSCO must be a U. S. citizen and possess final Top Secret security clearance.

4. Heads of Staff Agencies/Activities. Heads of Staff Agencies/Activities are directly responsible for the control and safekeeping of classified information and shall:

a. Publish written instructions specifying how the requirements of this SOP, and other security directives affecting the Staff Agency/Activity, will be implemented.

b. Appoint an individual in writing to serve as the Security Coordinator for their Staff Agency/Activity. Refer to figure 1-1 for a sample letter. Assistant Security Coordinators may be appointed if required to assist the Security Coordinator in the performance of his/her duties. Refer to figure 1-2 for a sample letter. However, ultimate responsibility for the Staff Agency/Activity security program resides with the Security Coordinator. The Security Coordinator may be assigned as a full-time, part-time or collateral duty, but the person designated must be an officer/enlisted E-6 or above or a civilian employee, YA-2 or YC-2 or above, with sufficient authority and staff to manage the program. The Security Coordinator should be afforded direct access to the HQMC Security Manager. The Security Coordinator/Assistant Security Coordinator must be a U.S. citizen and at a minimum have been the subject of a favorably adjudicated National Agency with Local Agency and Credit Checks (NACLC) Investigation.

c. Establish procedures to report questionable or unfavorable information to the HQMC Security Manager on staff

Encl (1)

HQMC IPSP SOP

agency/activity personnel who have been granted access to classified information, or who have eligibility to classified information or assigned to sensitive duties.

5. Security Coordinator/Assistant Security Coordinator. The Security Coordinator/Assistant Security Coordinator are the principal information and personnel security program advisors to the Staff Agency/Activity head. The Staff Agency/Activity Security Coordinator may also be designated as the staff agency's Top Secret Control Officer and NATO Control Officer. Security Coordinators will assist in implementing the security programs by:

a. Ensuring all personnel under their cognizance comply with the references and this SOP.

b. Serving as a liaison between HQMC Security Office (ARS) and personnel under their cognizance.

c. Ensuring that personnel have the appropriate clearance eligibility, the need to know, and have received all required security briefs before allowing access to classified information.

d. Ensuring personnel assigned to their Staff Agency/Activity complete all required security training.

e. Submitting visit requests (to outside agencies) via Joint Personnel Adjudication System (JPAS) for personnel under their cognizance.

f. Requesting courier cards (DD 2501) for personnel under their cognizance that handle classified material, as required by billet sensitivity.

g. Reviewing classified material prepared in their organization for correct classification and marking.

h. Promoting security awareness within their Staff Agency/Activity in support of the command security awareness program, and ensuring that all personnel understand the procedures for protecting classified information per reference (b).

Encl (1)

HQMC IPSP SOP

i. Ensuring that all assigned personnel have a personnel security clearance/access according to the billet requirements.

j. Establishing visitor control procedures to accommodate visits to their Staff Agency/Activity involving access to, or disclosure of, classified information. At a minimum, these procedures will include verification of identity, validation of personnel security clearance eligibility and access using JPAS, and a need-to-know determination.

k. Ensuring the DirAR Division (ARS) is notified of all instances involving loss, compromise, or subjection to compromise of classified information or material.

l. Reporting Information Technology (IT) System spillages (i.e., inappropriate levels of classified information are introduced to a unclassified or classified non-SCI IT System) and compromise of Classified Military Information (CMI) to DirAR Division (ARS/ARI) and/or CMC (SSO) when compromised information is indentified as SCI. Refer to enclosure (4) for guidance on reporting procedures.

m. Reporting any incident or situation that could affect Staff Agency/Activity personnel continued eligibility to access classified information to DirAR Division (ARS).

n. Enforcing classified material control by means of receipt, distribution, inventory, reproduction and disposition.

o. Ensuring all Controlled Unclassified Information (CUI), Sensitive but Unclassified (SBU) and For Official Use Only (FOUO) information is safeguarded and destroyed in accordance with reference (f).

p. Briefing new personnel on local security practices and providing the employee with a copy of the Staff Agency/Activity security procedures and this SOP.

q. Utilizing figure 2-2, conduct Staff Agency/Activity Security Self Assessments to ensure the security program is compliant with all policies and regulations.

6. Agency Top Secret Control Officer (TSCO). If required, Staff Agencies/Activities must appoint a TSCO in writing, who is

Encl (1)

HQMC IPSP SOP

responsible for the receipt, control, reproduction, destruction, transmission and inventory of all Top Secret material for the Staff Agency/Activity. The TSCO will be subordinate to the Security Coordinator. The person designated as the TSCO must be an officer, non-commissioned officer E-6 or above or a civilian employee, YA-2/YC-2 or above. Refer to figure 1-3 for sample appointment letters. The Agency TSCO must be a U.S. citizen who has been the subject of an SSBI within the past five years, have been granted access to Top Secret information and be completely familiar with the requirements for protection of Top Secret information and the duties described in paragraph 2-3 of reference (b).

7. Staff Agency/Activity Contracting Officer Representative (COR). Per reference (b), the Staff Agency/Activity COR shall be designated, in writing, per Subpart 201.602-2 of the Defense Federal Acquisition Regulations Supplement. The designation shall be for the purpose of preparing and signing the "Contract Security Classification Specification" (DD Form 254), and revisions thereto, and other security related contract correspondence. The COR is responsible to the security manager for coordinating with program managers and procurement officials.

8. COR Industrial Security Specialist. Per reference (b), the COR industrial security specialist shall ensure that the industrial security functions specified below are accomplished when classified information is provided to industry for performance on a classified contract:

a. Review statement of work to ensure that access to or receipt and generation of classified information is required for contract performance.

b. Validate security classification guidance; complete and sign the DD 254:

(1) Coordinate review of the DD 254 and classification guidance.

(2) Issue a revised DD 254 and other guidance as necessary.

(3) Resolve any problems related to providing classified information to the contractor.

Encl (1)

HQMC IPSP SOP

c. Coordinate, any additional security requirements beyond those required by this policy manual, the DD 254, or in the contract document itself.

d. Initiate all requests for Facility Clearance (FCL) action with the Defense Security Services (DSS).

e. Verify the FCL and storage capability prior to release of classified information.

Encl (1)

HQMC IPSP SOP

(LETTER HEAD)

5510
Date

From: Deputy Commandant/Director, Staff Agency/Activity
To: Individual Appointed

Subj: APPOINTMENT AS STAFF AGENCY/ACTIVITY SECURITY COORDINATOR

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) HQMC IPSP SOP

1. In accordance with reference (a), you are hereby appointed as the Staff Agency/Activity Security Coordinator. You will be notified of any change in this appointment, when necessary.
2. You are directed to familiarize yourself with the provisions of references (a) through (c).
3. By return endorsement you will indicate that you have assumed the duties as the Security Coordinator.

Signature of Deputy Commandant/Director

FIRST ENDORSEMENT

From: Individual Appointed
To: Deputy Commandant/Director, Staff Agency/Activity
Subj: APPOINTMENT AS STAFF AGENCY/ACTIVITY SECURITY COORDINATOR

1. I have assumed the duties as the Security Coordinator and will familiarize myself with the references.

Signature of Appointee

Figure 1-1--Format of Security Coordinator Appointment Letter

Encl (1)

HQMC IPSP SOP

(LETTER HEAD)

5510
Date

From: Deputy Commandant/Director, Staff Agency/Activity
To: Individual Appointed
Subj: DESIGNATION AS STAFF AGENCY/ACTIVITY ASSISTANT SECURITY
COORDINATOR
Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) HQMC IPSP SOP

1. In accordance with reference (a), you are hereby appointed as the Staff Agency/Activity Assistant Security Coordinator. You will be notified of any change in this appointment, when necessary.
2. You are directed to familiarize yourself with the provisions of references (a) through (c).
3. By return endorsement you will indicate that you have assumed the duties as the Assistant Security Coordinator.

Signature of Deputy Commandant/Director

FIRST ENDORSEMENT

From: Individual Appointed
To: Deputy Commandant/Director, Staff Agency/Activity
Subj: APPOINTMENT AS STAFF AGENCY/ACTIVITY SECURITY COORDINATOR

1. I have assumed the duties as the Assistant Security Coordinator and will familiarize myself with the references.

Signature of Appointee

Figure 1-2--Format of Assistant Security Coordinator Appointment
Letter

Encl (1)

HQMC IPSP SOP

(LETTER HEAD)

5510
Date

From: Deputy Commandant/Director, Staff Agency/Activity
To: Individual Appointed

Subj: APPOINTMENT AS TOP SECRET CONTROL OFFICER

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) HQMC IPSP SOP

1. In accordance with reference (a), you are hereby appointed as the Staff Agency/Activity Top Secret Control Officer. You will be notified of any change in this appointment, when necessary.
2. You are directed to familiarize yourself with the provisions of references (a) through (c).
3. By return endorsement you will indicate that you have assumed the duties as the Top Secret Control Officer.

Signature of Deputy Commandant/Director

FIRST ENDORSEMENT

From: Individual Appointed
To: Deputy Commandant/Director, Staff Agency/Activity

Subj: APPOINTMENT AS TOP SECRET CONTROL OFFICER

1. I have assumed the duties as the Top Secret Control Officer and will familiarize myself with the references.

Signature of Appointee

Figure 1-3--Format of Top Secret Control Officer Appointment
Letter

Encl (1)

HQMC IPSP SOP

Program Management

1. Guidance or Interpretation. Individual requests for guidance or interpretation of this SOP are encouraged. Address all requests to the DirAR Division (ARS) via the Staff Agency/Activity security coordinator.
2. Records Disposition. The following instructions are provided:
 - a. Appointment Letters. Record copies of appointment letters for Staff Agency/Activity Security Coordinators, Top Secret Control Officers (TSCO), NATO Point Officers and the appointed assistants will be retained for a period of two years after the individual assignment has been terminated.
 - b. Reports of Security Violations. Correspondence reporting security violations, hazards, and problems or weaknesses in Staff Agency/Activity security programs will be retained for a period of 5 years.
 - c. Destruction Records. A record of destruction is required for Top Secret information. OPNAV 5511/12, "Classified Material Destruction Report", may used for this purpose. Destruction records for Top Secret information must be retained for 5 years and a copy provided to ARS. Records of destruction are not required for Secret and Confidential information.
 - d. Preliminary Inquires. Reports of completed preliminary inquires such as missing or unaccounted documents, unauthorized disclosures, spillage, unsecured spaces, etc, will be retained for 5 years.
 - e. Emergency Action Plans. Record copies of emergency action plans for HQMC staff agencies/activities which handle classified material, to include SCI destruction plans, will be retained for 2 years following revision or cancellation.
 - f. Security Education Documents. Rosters of HQMC personnel who have accomplished required security training, record copies of all security training curriculums used to brief/debrief HQMC personnel, and related supporting documents will be retained for 2 years.

Encl (2)

HQMC IPSP SOP

3. Staff Agency and Activity Standard Operating Procedure.

Each staff agency/activity which handles classified information is required to prepare, and keep current, a written SOP specifying how the requirements of this SOP will be implemented within their Staff Agency/Activity. Internal security procedures will include, at a minimum, the following actions:

- a. Accounting and controlling of Top Secret material.
- b. Physical security measures for protecting classified material.
- c. Controlling the reproduction, destruction, and screening of incoming material.
- d. Requesting and recording clearance and access.
- e. Security education.
- f. Review of classified material for proper classification and marking, downgrading, declassification, and destruction.
- g. Reporting the loss or compromise of all classified material.
- h. Control of visitors.
- i. Implementing systematic means of accounting for personnel attached to the Staff Agency/Activity.

4. Unannounced Security Visits (USV). The USV is a valuable tool in mitigating the risk associated with storage and handling of classified material. As a security awareness tool, USV's are intended to reduce the number of security violations within HQMC Staff Agencies/Activities. Figure 2-1 is a USV Checklist for your use. DirAR Division (ARS) personnel will conduct the USVs. These USV's will be conducted during normal working hours (0800-1630 Monday through Friday). During these visits the Security Section will not be searching in desks or other areas considered personal in nature (i.e. wall lockers, gym bags, purses, etc).

5. Security Assessment Program. The HQMC Information and Personnel Security Assessment Program is designed to ensure compliance with regulatory requirements and increase security awareness at the Staff Agency/Activity level. The security

Encl (2)

HQMC IPSP SOP

assessment will review procedures, inventory documents, and ensure that all security issues are addressed. Figure 2-2 will be used as a guide to ensure all procedural requirements are met.

6. Security Coordinator Meetings. The DirAR Division (ARS) will periodically hold security coordinator meetings (normally once per quarter) to highlight significant changes in security regulations and call attention to problem areas within the HQMC security program. Staff Agency/Activity Security Coordinator's or their assistants must attend the Security Coordinator meetings. Suggested agenda items should be submitted to the DirAR Division (ARS) in advance of the meeting.

7. Security Notes. The DirAR Division (ARS) will periodically disseminate 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. Security Notes carry the same weight as formal directives.

8. Security Education. The HQMC security education program was instituted in order to familiarize personnel with protecting classified information from exposure to unauthorized persons, or persons without a valid need to know, and reporting requirements listed in this SOP and reference (b). The security education program should be continuous, tailored to the needs of the Staff Agency/Activity, and in accordance with the requirements of higher security directives. The following are the minimum requirements of the security education program within HQMC:

a. Initial Orientation Briefing. An initial orientation briefing will be given to all personnel upon arrival to HQMC. The DirAR Division (ARS) will fulfill this requirement during check-in. Access to classified material will not be granted until this briefing has been completed.

b. Staff Agency/Activity Orientation Briefings. The Security Coordinator will conduct an orientation briefing, covering unique staff agency/activity security policies and procedures to all newly assigned personnel as soon as is practical. This briefing is most effective when given informally and practical demonstration and application are used to clarify security program requirements. An effective staff agency/activity orientation will normally require the

Encl (2)

HQMC IPSP SOP

involvement of the security coordinator, the new arrival's coworkers, and other persons having expertise in the subjects to be explained. Completion of this orientation will be recorded by the security coordinator and that record maintained for the duration of the individual's assignment to HQMC.

c. On-the-Job Training. On-the-Job-Training is the phase of security education when security procedures for the assigned position are learned. Security Coordinators will assist supervisors in identifying appropriate security requirements. This training does not require reporting outside the staff agency but must be recorded within the agency personnel security file.

d. Annual Refresher Training. Annual Refresher Training must be completed once each year by all personnel (Military, Civilian and Contractor) assigned to HQMC. The Annual Security Training is located on ARS's Website at <http://hqinet001.hqmc.usmc.mil/ar/ARS/ARSB/HQMCTraining.htm>

e. Special Briefings. Special briefings are occasionally required for select HQMC personnel. These include the following:

(1) Foreign Travel Briefing. Prior to conducting foreign travel (personal or business), all military, civilian and DoD contractor personnel must receive a foreign travel briefing conducted by the DirAR Division (ARS). Personnel can schedule a briefing by contacting ARS at (703) 693-2696. In addition to personnel receiving foreign travel briefings, Security Coordinators are to ensure personnel conducting foreign travel to USCENTCOM, USSOUTHCOM and USPACOM AOR, complete the Isolated Personnel Report (ISOPREP). To determine if an ISOPREP is required, personnel should be directed to the DoD Foreign Clearance Guide, which can be found at <https://www.fcg.pentagon.mil/fcg.cfm> for further information. Questions regarding completion and submission of the ISOPREP can be addressed to PO-SOD at (703) 571-1015 or ARS at (703) 614-2320.

(2) NATO Briefings. All personnel who require access to NATO information must be briefed on NATO security procedures by the Staff Agency/Activity Security Coordinator before access is granted, in accordance with reference (b). (See MCO 5510.17 and SECNAV M-5510.36, for NATO Security Briefing requirements.) A

Encl (2)

HQMC IPSP SOP

copy of the briefing certificate must be retained for 2 years after the member has detached.

(3) Sensitive Compartmented Information (SCI). The Special Security Officer (SSO) is responsible for briefing those individuals requiring access to SCI. To schedule a briefing, contact the SSO at (703) 693-6007.

Encl (2)

HQMC IPSP SOP

USV CHECKLIST

1. ARE DOCUMENTS PROPERLY SAFEGUARDED? YES NO
2. ARE ANY COMPUTERS LEFT UNATTENDED (NIPRNET/SIPRNET)? YES NO
3. ARE ANY USER ID'S WITH PASSWORDS WRITTEN DOWN UNDER KEYBOARDS, MOUSE PADS, TOP OF DESK, UNDER DESKTOP CALENDARS ON WALLS AND BULLETIN BOARDS? YES NO
4. ARE ANY BURN BAGS LEFT UNATTENDED WITHIN AN UNSECURED SPACE? YES NO
5. ARE THERE ANY UNSECURED, UNATTENDED COURIER CARDS, BUILDING PASSES, ETC? YES NO
6. IS EQUIPMENT DESIGNATED FOR THE REPRODUCTION OF CLASSIFIED MATERIAL? IF SO, IS THE EQUIPMENT PROPERLY MARKED AND SAFE GUARDED? YES NO
7. ARE FACSIMILE (FAX) MACHINES ADEQUATELY MARKED TO ENSURE PERSONNEL ARE AWARE THAT IT IS/IS NOT AUTHORIZED FOR TRANSMISSION OF CLASSIFIED MATERIAL? YES NO
8. IS OFFICE AUTOMATION MARKED /LABELED PROPERLY? YES NO
9. ARE SF700, 701, 702 FORMS AFFIXED TO SECURITY CONTAINERS/SECURED DOORS AND PROPERLY FILLED OUT? YES NO
10. ARE ANY STU III KEYS OR FORTEZZA CARDS LEFT UNATTENDED OR UNSECURED? YES NO
11. IS THE EMERGNECY ACTION PLAN FOR THE PROTECTION AND DESTRUCTION OF CLASSIFIED INFORMATION POSTED? YES NO
12. ARE ACCESS ROSTERS POSTED, CURRENT, AND ACCURATE? YES NO
13. ARE ADEQUATE VISITOR CONTROL PROCEDURES IN PLACE? (ROSTERS, LOGBOOKS, ETC.) YES NO
14. ARE WINDOWS COVERED CORRECTLY TO PROTECT THE INADVERTENT DISCLOSURE OF CLASSIFIED INFORMATION? YES NO

Figure 2-1--Unannounced Security Visit Checklist

Encl (2)

INFORMATION AND PERSONNEL SECURITY ASSESSMENT CHECKLIST

Staff Agency _____ Security Coordinator _____

1. Does the staff/agency hold the current editions of SECNAV M-5510.36 and SECNAV M-5510.30?

Reference
NONE

2. Has the Deputy Commandant/Director issued a command standing operating procedure?

Reference
SECNAV M-5510.36, PAR 2-1
SECNAV M-5510.30, PAR 2-2

3. Has the Deputy Commandant/Director ensured that the security coordinator and other security personnel receive appropriate security education and training?

Reference
SECNAV M-5510.36, PAR 2-1
SECNAV M-5510.30, PAR 2-2

4. Has the Deputy Commandant/Director approved an emergency plan for the protection and destruction of classified information?

Reference
SECNAV M-5510.36, PAR 2-1
SECNAV M-5510.30, PAR 2-2

5. Has the Deputy Commandant/Director designated, in writing, an agency security coordinator?

Reference
SECNAV M-5510.36, PAR 2-2
SECNAV M-5510.30, PAR 2-2

6. Is the Staff Agency/Activity security coordinator named and identified to agency personnel on command organizational charts, telephone listings, rosters, or other media?

Reference
SECNAV M-5510.36, PAR 2-2
SECNAV M-5510.30, PAR 2-3

Figure 2-2—Security Assessment Checklist

HQMC IPSP SOP

7. If applicable, has the Deputy Commandant/Director designated in writing an agency Top Secret Control Officer?

Reference

SECNAV M-5510.36, PAR 2-3

8. Has the Staff Agency/Activity security coordinator implemented regulations concerning the disclosure of classified information to foreign nationals?

Reference

SECNAV M-5510.36, PAR 2-2

9. Has the Staff Agency/Activity security coordinator developed security measures and procedures regarding visitors who require access to classified information? Is JPAS utilized for visit requests?

Reference

SECNAV M-5510.36, PAR 2-2

MARADMIN 077/04

10. Has the Deputy Commandant/Director established procedures for end of the day and after hours security checks, utilizing the SF 701 (Activity Security Checklist) and the 702 (Security Container Check Sheet), to ensure that all areas which process classified information are properly secured?

Reference

SECNAV M-5510.36, PAR 7-10

11. Has the Deputy Commandant/Director maintained a record of a SF 700 (Security Container Information) for each security container, showing the location of each, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combinations and who are to be contacted in the event the security container, vault or secure room is found open, unattended or if personnel are locked out.

Reference

SECNAV M-5510.36, PAR 10-12

12. Has the staff agency/activity security coordinator ensured that all classified information is stored in a GSA-approved security container, vault, modular vault, or secure room?

Reference

SECNAV M-5510.36, PAR 10-3

Figure 2-2--Security Assessment Checklist-Continued

Encl (2)

HQMC IPSP SOP

13. Has the Deputy Commandant/Director established at least 1 day each year as a "clean-out" day, when specific attention and effort is focused on disposition of unneeded classified and controlled unclassified information as recommended by the reference?

Reference
SECNAV M-5510.36, PAR 10-17

14. Is the Staff Agency/Activity security coordinator a US Citizen and has the investigative/clearance eligibility requirements needed for the level of access to classified information required?

Reference
SECNAV M-5510.30, PAR 2-6

15. Has the Staff Agency/Activity security coordinator ensured that all personnel who have access to classified information and spaces or will be assigned to sensitive duties are appropriately cleared through coordination with ARS?

Reference
SECNAV M-5510.30, PAR 2-4

16. Has the Staff Agency/Activity security coordinator ensured that all personnel who had access to classified information, who have transferred, separated or retired have been debriefed on the NAVMC 512 and have been removed from the access control list?

Reference
SECNAV M-5510.30, PAR 2-4 & 4-12

17. Has the Deputy Commandant/Director ensured personnel are made aware of the continuous evaluation program?

Reference
SECNAV M-5510.30, CH 10

18. Has the Deputy Commandant/Director established or coordinated oversight over classified work carried out by cleared DoD contractor employees in spaces controlled by their staff agency?

Reference
SECNAV M-5510.36, CH 11

Figure 2-2—Security Assessment Checklist-Continued

Encl (2)

HQMC IPSP SOP

Personnel Security

1. Access. Knowledge or possession of classified information is authorized only for those whose duties require access. No employee will be allowed knowledge or possession of classified information unless the following conditions have been met:

a. Have a "need to know" at a particular level (top secret, secret, confidential) in order to perform officially appointed duties, as certified by the staff agency security coordinator on the NAVMC HQ 512, and verified by the DirAR Division (ARS).

b. Has been granted a security clearance (either temporary access or final) commensurate with the level of access required.

c. Has been administered the staff agency security orientation briefing and has read and signed the HQMC Security Orientating Briefing administered by the DirAR Division (ARS).

2. Heads of Staff Agencies/Activities are responsible for ensuring all the above conditions are met prior to authorizing access to classified information. No employee will have access to classified information solely because of rank or position.

3. Temporary Access. Formerly known as "Interim Access" to classified or sensitive information, temporary access may be granted to an individual whose background investigation is not complete or is pending eligibility adjudication. Granting temporary access is a risk management decision and as such requires a favorable review of all available local records (e.g., personnel, medical, legal, security, base/military police, etc.) and the questionnaire for national security positions with no significant derogatory information/issues. Significant derogatory information/issues are information that could, in itself, justify an unfavorable administrative action or an unfavorable security determination. The ultimate decision to grant temporary access will reside with the DirAR Division (ARS). Upon receipt of a Letter of Intent (LOI) from the Department of the Navy Central Adjudication Facility (DONCAF) to deny an individual's security clearance, temporary access will be immediately withdrawn for those individuals who were granted temporary access.

4. Employees requiring access to NATO COSMIC or NATO Secret, or access to the SIRPNET terminals, must possess the equivalent

Encl (3)

HQMC IPSP SOP

final or temporary U.S. security clearance based upon the appropriate personnel security investigation, and have received and acknowledged a briefing on NATO security requirements.

5. Personnel Security Investigations. No individual will be given access to classified information or be assigned to sensitive duties unless a favorably personnel security determination has been made regarding his/her loyalty, reliability and trustworthiness. A Personnel Security Investigation (PSI) is conducted to gather information pertinent to these determinations. PSI requirements and definitions are as follows:

a. National Agency Check with Written Inquires (NACI). The NACI is the basic Executive Order (EO) 10450 investigative standard for Federal Government Civil Service Employment suitability determinations. A NACI consists of a NAC plus Written Inquires from former employers and supervisors, to references, and to schools covering the previous five years. NACI's are insufficient for determining personnel security clearance eligibility levels for access to classified information or assignment to sensitive duties.

b. Access NACI (ANACI). The ANACI is an OPM product that combines the NACI (for suitability of civilian employees within the Federal Government) and NACLIC (for determine security clearance eligibility). The ANACI meets the investigative requirements for appointment to non-critical sensitive positions and for access to Confidential or Secret national security information, for civilian employees. The ANACI includes a NAC, a credit check, and written inquiries covering the last five years to law enforcement agencies, to former employers and supervisors, to references, and to schools. A previously conducted NACLIC not beyond 10 years with a favorable eligibility determination will be used for Confidential and Secret access. The ANACI will be submitted to cover the scope of investigation for federal civilian employment.

c. National Agency Check with Local Agency and Credit Checks (NACLIC). The NACLIC is the basic EO 12968 standard for determination of eligibility to access to Confidential and Secret classified national security information. The NACLIC also provides the basis for military suitability determinations for Navy and Marine Corps enlisted members and officers. The NACLIC

Encl (3)

HQMC IPSP SOP

includes a NAC, credit bureau checks covering all locations where the subject has resided, been employed, or attended school for six months or more or the past 7 years, and checks of law enforcement agencies having jurisdiction where the subject has resided, been employed, or attended school within the last five years.

d. Single Scope Background Investigation (SSBI). The SSBI is the EO 12968 investigative standard for determinations of eligibility to access Top Secret classified national security information and SCI access eligibility determinations. The SSBI is also the basis for determinations of eligibility to occupy critical-sensitive or special-sensitive national security positions. The SSBI includes the NAC, verification of the subject's date and place of birth, citizenship, education and employment, neighborhood interviews, developed character reference interviews, credit checks, local agency checks, public record checks (i.e., verification of divorce, bankruptcy, etc.), foreign travel, foreign connections and organizational affiliations, with other inquiries, as appropriate. A formal subject interview is conducted, as applicable, as well as the subject's current spouse or cohabitant. The scope of an SSBI covers the most recent 10 years of the subject's life or from the 18th birthday, whichever is the shorter period; however at least 2 years will be covered. No investigation is conducted prior to the subject's 16th birthday.

6. Investigative Requirements for Clearance Eligibility. Only U.S. citizens are eligible for a security clearance. Security Clearance eligibility for access to classified information will be based on a PSI prescribed for the level of classification.

a. Top Secret. The investigative basis for Top Secret clearance eligibility is a favorably completed SSBI, SSBI-Periodic Review (PR) or Phased Periodic Review (PPR). For those who have continuous assignment for access to Top Secret information, the SSBI must be updated every five years by a PR.

b. Secret/Confidential. The investigative measurement for Secret or Confidential clearance eligibility is a favorably completed NACLIC or ANACI. For Secret or Confidential clearance, the investigation is updated every 10 years and 15 years, respectively.

Encl (3)

HQMC IPSP SOP

7. Continuous Evaluation. In order to ensure that everyone who has access to classified information remains eligible for a clearance, continuous assessment and evaluation is required. In accordance with reference (a), individuals are required to self report to their security coordinator and seek assistance for any incident or situation that could affect their continued eligibility for access to classified information. Security Coordinators shall brief Staff Agency/Activity personnel initially and periodically thereafter, to ensure familiarity with pertinent security regulations and the standards of conduct required of individuals holding positions of trust. The ultimate responsibility for maintaining eligibility to access classified information rests with the individual.

8. Check-ins. All personnel assigned to HQBN, HQMC, M&RA and MCRC must check-in with the HQMC Security Section. M&RA/MCRC personnel will check-in with the DirAR Division (ARS) office located in the Marsh Center, 3280 Russell Road, Marine Corps Base, Quantico, VA. Personnel assigned to Staff Agencies/Activities that do not have eligibility to access classified information are not authorized to work in Restricted Areas at any time. Security Coordinators will ensure that all required forms for the following services are provided to the Security Section:

a. Military: Security Services Form, (refer to figure 3-1), DoD Badge Request (refer to figure 3-2), HQ NAVMC 512 (Classified Information Access Authorization) (refer to figure 3-3), SF 312 (Non-Disclosure Agreement) (refer to figure 3-4), DoD Badge Agreement (refer to figure 3-5), and HQMC Security Orientation/Awareness Briefing (refer to figure 3-6).

b. Civilian: Security Services Form (refer to figure 3-1), DoD Badge Request (refer to figure 3-2), HQ NAVMC 512 (refer to figure 3-3), (SF 312) (refer to figure 3-4), Position Description, DoD Badge Agreement (refer to figure 3-5), and HQMC Security Orientation/Awareness Briefing (refer to figure 3-6).

c. For DoD Contractor check-in procedures, refer to enclosure (5).

9. Check-out/Debriefings. All personnel assigned to HQBN, HQMC, M&RA and MCRC must check-out with the HQMC Security Section. M&RA/MCRC personnel will check-out with the DirAR

Encl (3)

HQMC IPSP SOP

Divison (ARS) office located in Marsh Center, 3280 Russell Road, Marine Corps Base, Quantico, VA. Individuals who had access to classified information must be debriefed by their respective Staff Agency/Activity Security Coordinator and the HQMC Security Manager by signing part D of the NAVMC 512, debriefing section on the NATO Briefing Certificate, and execute a Security Termination Statement (OPNAV 5511/14) if retiring, EASing or leaving Federal Service. Surrender all government issued property to the Security Office (i.e., DoD Badge, CAC (Contractors Only, Courier Cards). The NAVMC HQ 512 and OPNAV 5511/14 will be retained in the staff agency's correspondence files for 2 years after the member's departure. HQMC personnel will be debriefed when one of the following conditions occurs:

- a. Prior to termination of active military service or civilian employment, temporary separation for a period of 60 days or more, including sabbaticals and leave without pay.
- b. At the conclusion of the access period when a Limited Access Authorization has been granted.
- c. When a security clearance is revoked for cause.
- d. When access is administratively withdrawn.
- e. When a Marine or civilian transfers, executes PCS orders, or otherwise permanently departs HQMC, M&RA or MCRC and no longer requires access to classified material.
- f. A debriefing will also be given, and a Security Termination Statement signed, when a member of this headquarters inadvertently had substantial access to information which that person was not eligible to receive.

10. Secret Internet Protocol Router Network (SIPRNET) Access. To request SIPRNET Access, the following forms will be submitted to the Security Section: Security Services Form (refer to figure 3-1), DD Form 2875 (System Access Authorization Request (SAAR)), (refer to figure 3-7), and NATO Briefing Certificate (refer to figure 3-8).

11. Courier Card. To request a courier card, the following forms must be submitted to the Security Section: Security Services Form (refer to figure 3-1) and a memorandum from the

Encl (3)

HQMC IPSP SOP

Staff Agency/Activity Security Coordinator indicating what type of courier card (i.e., NCR, CONUS, OCONUS), level of access and a duration date (refer to figure 3-9).

12. Alarm Zone (Swipe/Personal Identification Code (PIC)/Personal Identification Number (PIN) Request. To request Swipe and PIC/PIN access to an office space, submit an Alarm Zone Request (refer to figure 3-10) to the Security Office organizational mail box at SMB.HQMC.Security@usmc.mil. Request will normally be processed within 72 hours of receipt. E-mail confirming completion will be forwarded to the Security Coordinator.

13. Joint Personnel Adjudication System (JPAS) Accounts. Per reference (a), Staff Agency/Activity Security Coordinators and Assistant Security Coordinators will have Joint Personnel Adjudication System (JPAS) User Accounts with Level 10 access. Additional accounts may be requested with prior approval from the HQMC Security Manager. To request a JPAS User account, contact the HQMC Security Manager.

14. Common Access Card (CAC) Issuance. In accordance with MARADMIN 624/08, all CAC eligible Marine Corps personnel must complete a registration process that consists of identity proofing and background check before being issued a DoD CAC. Initial issuance of a CAC requires, at a minimum, the completion and submission of National Agency Check with written Inquiries (NACI) to the Office of Personnel Management (OPM) or a DoD determined equivalent investigation. In order to be issued a CAC an individual must present two forms of identification listed in figure 3-11 (i.e., driver's license, SSN card, U.S. Military ID, etc.). When it has been determined that personnel do not meet the minimum requirements, the following will take place:

a. Military personnel will submit a Questionnaire for National Security Positions, (SF 86) along with fingerprints.

b. Civilian personnel will submit a Questionnaire for Non-Sensitive Position (SF 85), Declaration for Federal Employment (OF 306), Resume, fingerprints and Report of Separation DD 214 (if applicable).

Encl (3)

HQMC IPSP SOP

c. For DoD Contractor CAC issuance procedures, refer to enclosure (5).

15. Building Access. Building access is controlled by the Pentagon Force Protection Agency (PFPA). Personnel requiring access to either the Pentagon or Navy Annex must first report to their Staff Agency/Activity Security Coordinator to receive the appropriate forms. Personnel will then report to the DirAR Division (ARS) Security Office to pick-up the DD Form 2249 (DoD Badge Request). In order to be issued a DoD Badge, an individual must present the DD 2249, and one (1) form of identification to the Badge Office at either the Pentagon (room #1F1084) or Navy Annex (room #G501A). Personnel must fall into one of the below categories to obtain a DoD Badge:

a. Permanent personnel that fall under the HQMC Staff Agency/Activity and work in a approved DoD facility.

b. Individuals visiting DoD Facilities at least 3-5 times a week.

c. To be issued a National Capital Region Badge, justification must be stated on the DoD Badge Request Form indicating that the individual requires recurring, unescorted access to buildings other than the Pentagon or FOB#2, between the hours of 2000 and 0600, Monday through Friday, and/or on the weekend.

d. To be issued a Continuity of Operation (COOP) Badge (regular DoD Badge with the number 3), Security Coordinators must verify that personnel are listed on the COOP Roster by contacting Plans, Policy and Operations (PP&O), Current Operations (POC) at (703) 571-1067.

e. To be issued a NCR "A" Badge, Security Coordinators must submit a request to the HQMC Security Manager. Refer to figure 3-12.

16. Visitor Control. For security purposes, the term "visitor" is defined as any person not assigned to or employed by this Headquarters. Heads of Staff Agencies/Activities are responsible for the conditions under which visits are permitted. These conditions must ensure the safeguarding of classified information within the staff agency/activity. The following

Encl (3)

HQMC IPSP SOP

building access and visitor controls apply to HQMC Staff Agencies/Activities.

a. Visitors who require access to any DoD facility but do not meet the requirements to obtain a badge can be added to the Non-Escort Required Visitor Access Control Roster. To add a visitor, the following procedures will be followed:

- The sponsoring Staff Agency/Activity Security Coordinator will submit a memorandum to Pentagon Access Control Division (PACD), providing the name, SSN, DOB, Citizenship, type of investigation, reason for the visit and the duration. Fax all requests to (703) 697-9085.

b. Visits not involving discussion of classified information or entry into secure areas do not require formal approval. Visits involving discussion of classified information require a formal request to the Staff Agency/Activity involved. All Agencies outside of HQMC must submit their visit request via the JPAS. The HQMC Security Management Office (SMO) Code number for a visit request is 540080084. Security Coordinators are responsible for ensuring that all visiting personnel have the proper security clearance upon arrival.

c. Monitor the movement of all visitors and inform personnel to protect classified information. When escorts are used, ensure all visitors have access only to information they have been authorized to receive.

d. Prior to Foreign Visitors arrival and immediately upon discovery of their pending arrival, all personnel must notify the Staff Agency/Activity Security Coordinator who will in turn notify the HQMC Security Manager and Foreign Disclosure Officer (PP&O). For further guidance refer to enclosure (4), paragraph 5.

Encl (3)

SECURITY SERVICES FORM

DATE REQUESTED: _____

AGENCY/DEPARTMENT REPRESENTATIVE INFORMATION:

NAME: _____ PHONE # _____

OFFICE CODE/ROOM # _____
EXACT LOCATION OF SERVICE REQUESTED _____

TYPE OF SERVICE REQUESTED

COMMUNICATION SECURITY: ___ CRYPTO MATERIAL/KEYING ___ SECURE PRODUCT
REQ/REPAIR ___ INSTALLATION ___ OTHER _____

PHYSICAL SECURITY: ___ LOCKS ___ ALARMS ___ DOOR HARDWARE ___ CONDUIT ___ PDS
___ PSE ___ OFFICE CERTIFICATION ___ ANTI-TERRORISM BRIEF ___ OTHER _____

PARKING: ___ PARKING REP TRAINING ___ PARKING CLEARANCES ___ SPECIAL EVENT
PARKING ___ PERMIT PROCESSING ___ MOTORCYCLE/HANDICAPPED PERMITS
___ OTHER _____

PERSONNEL SECURITY: ___ BADGE REQ. ___ ACCESS REQ. ___ SIPR REQ. ___ SWIPE ACCESS
___ CAC CARD REQ. ___ COURIER CARD REQ. ___ VISITOR REQ. ___ SECURITY INVESTIGATION
___ MAIL/REC. ___ CLASSIFIED MATERIAL ___ JPAS SUPPORT ___ OTHER _____

BRIEF DISCRIPTION OF THE PROBLEM: _____

ASSIGNED TO: _____ DATE COMPLETED: _____

FOLLOW-UP SERVICE DESCRIPTION/NOTES (IF REQUIRED): _____

CUSTOMER SATISFACTION RATING

1 2 3 4 5 6 7 8 9 10

(1 represents the least satisfied with the level of service provided 10 representing completely satisfied)

CUSTOMER COMMENTS: _____

CUSTOMER SIGNATURE: _____ DATE: _____

Figure 3-1—Security Services Form

HQMC IPSP SOP

ARS SECURITY DoD BUILDING PASS REQUEST
NAVMC HQ 943 (10-06)

Print Form

PRIVACY ACT STATEMENT			
<p>AUTHORITY: 37 U.S.C. Chapter 7; 10 U.S.C. Chapter 55; EO 9397, November 1943. PRINCIPAL PURPOSE: To obtain information to determine eligibility for access to DoD buildings ROUTINE USE(S): Copies of this form, information from this form and related documentation may be furnished to the Pentagon Force Protection Agency's Access Control Division and/or the Pentagon Police Department for the purpose of conducting various background checks, to include a review of National Crime Information Center (NCIC) and other sources. In order to determine suitability for issuance of a Pentagon Reservation Building Access Badge in accordance with the provisions of Pentagon Force Protection Agency Administrative Instruction #30 and other applicable laws, rules and policies. DISCLOSURE: Voluntary; however, the SSN is used for positive identification and if the required information is not furnished, the application may be disapproved.</p>			
DATE		CHECK ONE: <input type="checkbox"/> INITIAL REQUEST <input type="checkbox"/> RENEWAL	
LAST NAME		FIRST NAME	MI
RANK/ GRADE	SSN	AGENCY	OFFICE CODE
PHONE NUMBER		BUILDING ACCESS: CHECK ONE	<input type="checkbox"/> FOB2 (FEDERAL OFFICE BUILDING #2)
			<input type="checkbox"/> PENT (PENTAGON)
			<input type="checkbox"/> NCR (NATIONAL CAPITAL REGION)
JUSTIFICATION FOR NCR			
CONTRACTOR CAC REQUIRED:	<input type="checkbox"/> YES <input type="checkbox"/> NO	EMAIL:	

SECURITY COORDINATOR
 ASSISTANT SECURITY
 COORDINATOR SIGNATURE

***FOR RENEWAL PURPOSES, SECURITY MANAGERS MUST ENSURE REQUESTERS' BILLET REQUIRES SAME TYPE OF DoD BADE.**

ADOBE DESIGNER 7.0, OCT 2006

Figure 3-2--DoD Building Pass Request

HQMC IPSP SOP

CLASSIFIED INFORMATION ACCESS AUTHORIZATION (5521)
 NAVMC HQ 512 (REV. 6-02) (EF)
 (Previous editions will not be used)

THIS FORM IS SUBJECT TO THE PRIVACY
 ACT OF 1974.

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		SOCIAL SECURITY NO.	
UNITED STATES CITIZENSHIP	YES <input checked="" type="checkbox"/> NO <input type="checkbox"/>	ACTIVE <input type="checkbox"/>	RESERVE <input type="checkbox"/>	OFFICE CODE AND PHONE 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)	<input type="checkbox"/>	
CLASSIFIED INFORMATION	<input type="checkbox"/>	<input type="checkbox"/>
NATO	<input type="checkbox"/>	<input type="checkbox"/>
COSMIC ATOMAL	<input type="checkbox"/>	<input type="checkbox"/>
ACCESS TO CLASSIFIED INFO NOT REQUIRED	<input type="checkbox"/>	
<input type="checkbox"/>		
<input type="checkbox"/>		

AT TEST STATION:

"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 SC/SAP, A SPECIAL CONFIDENCE AND TRUST HAS BEEN PLACED IN ME BY THE UNITED STATES GOVERNMENT."

SIGNATURE: _____ DATE: _____
 (Individual Requiring Access)

Signature _____ Date _____
 (Agency Security Manager)

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:

Signature _____ Date: _____
 Level and Date _____ Basis _____
 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 ACKNOWLEDGMENT

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 _____

Figure 3-3-Classified Information Access Authorization

HQMC IPSP SOP

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 12958, 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 1.2, 1.3, and 1.4(e) of Executive Order 12958, 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 the 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 the 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 Section 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.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.

Reset

STANDARD FORM 312 (Rev. 1-00)
Prescribed by NARA/ISOO
32 CFR 2003, E.O. 12958

Figure 3-4—Classified Information Nondisclosure Agreement

Encl (3)

HQMC IPSP SOP

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958; 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 (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 expose confidential Government agents), 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 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.

11. 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 Section 2003.20) so that I may read them at this time, if I so choose.

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

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 <i>(Type or print)</i>		NAME AND ADDRESS <i>(Type or print)</i>	

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 <i>(Type or print)</i>	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 Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

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

Reset STANDARD FORM 312 BACK (Rev. 1-00)

Figure 3-4-Classified Information Nondisclosure Agreement-Continued

HQMC IPSP SOP

AGREEMENT TO THE WEARING OF THE DOD BADGE

BASIC POLICY

1. DoD building passes are issued to qualified federal employees and DoD contractors for their use only, for the sole purpose of facilitating the conduct of official U.S. government business. The lending of a pass to another individual or alteration of a pass in violation of 18 U.S.C. 499 (reference j) may result in prosecution. A building pass shall be issued to a person assigned duty to an office located in the building, or who is performing contractual service for the building occupants. Specific types of passes are required for admittance during designated hours.
2. All employees in the Pentagon shall wear a DoD building pass that is prominently displayed on the outer clothing above the waist at all times. To obtain a permanent building pass for admittance to the Pentagon Reservation, the applicant must work in a building on the Pentagon Reservation.
3. All lost, stolen, or unserviceable badge incidents must be reported to the HQMC Security Officer located in room 1010.
4. Permanent Badge holders may escort individuals inside of buildings designated as part of the Pentagon Reservation (i.e., Annex/Pentagon, etc.). Individuals serving as escorts may not leave their visitors unattended at any time.
5. Badges will be returned to the Security Office room 1010 upon completion of tour within the Pentagon Reservation (i.e., PCS, EAS, retirement, completion of contractor services).

I, _____, HAVE READ AND UNDERSTAND THE PROVISIONS AND RESPONSIBILITIES OF THE ISSUANCE OF THE DOD BUILDING PASS. I FURTHER UNDERSTAND THAT I AM TO TURN IN MY BADGE TO THE SECURITY OFFICE IN ROOM NUMBER 1010 UPON TRANSFERRING FROM THE PENTAGON RESERVATION.

MEMBER SIGNATURE _____ DATE _____

WITNESS SIGNATURE _____ DATE _____

Figure 3-5-DoD Badge Agreement

HQMC IPSP SOP

HQMC SECURITY ORIENTATION/AWARENESS BRIEFING

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

1. **Clearance and Access.** Only individuals with the appropriate clearance eligibility, a need-to-know, and billet requirements will have access to classified information. In addition, individuals requiring access to classified information who have a clearance based off of an out-dated personnel security investigation will be required to submit a Personnel Security Questionnaire (PSQ) w/fingerprint card to the HQMC Security Office.
2. **Classified Information.** Classified information, as well as computers (including laptops) may not be removed from the DoD buildings (Pentagon/Annex/etc.) without a proper courier authorization and without proper packaging and protection. Requests for courier cards must be provided to the HQMC Security Office (room 1006) via the appropriate Security Manager (i.e., I&L, P&R, etc.) Property passes from the responsible officer are required in order for Government equipment to be taken outside of any building located on the Pentagon reservation (i.e., Annex/Pentagon). While inside a DoD building (Pentagon/Annex, etc.), no classified information may be carried outside office spaces unless it is also properly covered and safeguarded (i.e., use of colored coversheets).
3. **Disposal.** Controlled documents (classified information) may not be destroyed without proper authorization from your Security Manager and then only in an authorized manner.
4. **Classified storage.** All classified information must be stored in an approved GSA container (i.e., safe) or in an approved open storage office space.
5. **Telephones.** Classified discussion via telephone is authorized only by use of classified telephones (Secure Telephone (STE)). Caution should be exercised when discussing classified information via classified phone to ensure that individuals cannot overhear the discussion.
6. **Faxes.** Faxes containing classified information may only be transmitted from a secure fax machine to a secure fax machine. Unclassified fax machines are not to be used to as copiers for the purpose of copying classified information, or for the transmission of classified information.

Figure 3-6—HQMC Security Orientation/Awareness Briefing

Encl (3)

HQMC IPSP SOP

7. **Computers.** Classified information may only be processed on approved secure computers. All approved computers and diskettes must be clearly marked with the appropriate security labels, and personally owned computers may never be used to process classified information. Transmission of classified information via computer may only be accomplished via SIPRNET.

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

9. **Security Violations.** Security violations are to be reported to your Agency Security Manager. If unavailable, the security violation is to be reported to the HQMC Security Officer in room 1006 of the Annex.

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

11. **Foreign Visitors/Disclosure.** While public domain information authorized and approved by the Public Affairs Office can be freely shared with foreign governments and interest, Classified Military Information (CMI) and Controlled Unclassified Information (CUI) is only shared with foreign governments when there is a clearly defined benefit to the U.S. Government. Prior to Foreign Visitors arrival and immediately upon discovery of their pending arrival, all personnel must notify the Staff Agency/Activity Security Coordinator for further guidance.

12. **Checking Out.** All personnel departing HQMC due to PCS/PCA, Terminal Leave, retirement/EAS, Transfer, etc. are required to checkout with their Security Coordinator and with the HQMC Security Office in room 1006 at the Annex.

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

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

Figure 3-6—HQMC Security Orientation/Awareness Briefing—
Continued

Encl (3)

HQMC IPSP SOP

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

16. HQMC/ARS/Security Website address is:

<http://hqinet001.hqmc.usmc.mil/ar/ARS/index.htm>

Signature: _____

Witness: _____

Figure 3-6—HQMC Security Orientation/Awareness Briefing-
Continued

Encl (3)

HQMC IPSP SOP

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)			
PRIVACY ACT STATEMENT			
AUTHORITY: PRINCIPAL PURPOSE: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.			
ROUTINE USES: DISCLOSURE: None. Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.			
TYPE OF REQUEST <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID _____		DATE (YYYYMMDD)	
SYSTEM NAME (Platform or Applications)		LOCATION (Physical Location of System)	
PART I (To be completed by Requestor)			
1. NAME (Last, First, Middle Initial)		2. SOCIAL SECURITY NUMBER	
3. ORGANIZATION		4. OFFICE SYMBOL/DEPARTMENT	5. PHONE (DSN or Commercial)
6. OFFICIAL E-MAIL ADDRESS		7. JOB TITLE AND GRADE/RANK	
8. OFFICIAL MAILING ADDRESS		9. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER	10. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR
USER AGREEMENT			
By signing Block 11 of this form, I have agreed to the terms and conditions stated in Block 27 and attached addendum. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.			
1A TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access) <input type="checkbox"/> I have completed Annual Information Awareness Training. DATE (YYYYMMDD) _____			
11. USER SIGNATURE		12. DATE (YYYYMMDD)	
PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)			
13. JUSTIFICATION FOR ACCESS			
14. TYPE OF ACCESS REQUIRED: <input type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED			
15. USER REQUIRES ACCESS TO: <input type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED (Specify category) <input type="checkbox"/> OTHER _____			
16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input type="checkbox"/>		16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)	
17. SUPERVISOR'S NAME (Print Name)		18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT		20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR		21a. PHONE NUMBER	21b. DATE (YYYYMMDD)
22. SIGNATURE OF IAO OR APPOINTEE		23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER
			25. DATE (YYYYMMDD)
DD FORM 2875, APR 2005			PREVIOUS EDITION IS OBSOLETE.
			Reset

Figure 3-7—System Access Authorization Request

Encl (3)

HQMC IPSP SOP

26a. NAME (Last, First, Middle Initial)		26b. SOCIAL SECURITY NUMBER	
27. OPTIONAL INFORMATION (Additional Information) By signing block 11 I agree to the following rules of behavior: - I understand that I am providing both implied and expressed consent to allow authorized authorities, to include law enforcement personnel, access to my files and e-mails which reside or were created on Government IT resources. - I will not conduct any personal use that could intentionally cause congestion, delay, or disruption of service to any Marine Corps system or equipment. - I will not install or use any Instant Messaging client or peer-to-peer file sharing application, except that which has been installed and configured to perform an authorized and official function. - I will not use Marine Corps IT systems as a staging ground or platform to gain unauthorized access to other systems. - I will not create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings, regardless of the subject matter. - I will not use Government IT Resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation. - I will not use Government IT resources for personal or commercial gain without commander approval. These activities include solicitation of business services or sale of personal property. - I will not create, download, view, store, copy, or transmit materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited such as transmitting sexually explicit or sexually oriented materials. - I will not use Marine Corps IT systems to engage in any outside fund-raising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited partisan political activity. - I will not post Marine Corps Information to external newsgroups, bulletin boards or other public forums without proper authorization. This includes any use that could create the perception that the communication was made in ones official capacity as a Marine Corps member, unless appropriate approval has been obtained or uses at odds with the Marine Corps mission or positions. - I will not use Marine Corps IT resources for the unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data. - I will not modify or attempt to disable ant anti-virus program running on a Marine Corps IT system without proper authority. - I will not connect any personally owned computer or computing system to a DoD network without prior proper written approval. (Continued on addendum page)			
PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION			
28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION (YYYYMMDD)	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> LEVEL III	
29. VERIFIED BY (Print name)	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE (YYYYMMDD)
PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION			
TITLE:	SYSTEM	ACCOUNT CODE	
	DOMAIN		
	SERVER		
	APPLICATION		
	DIRECTORIES		
	FILES		
	DATASETS		
DATE PROCESSED (YYYYMMDD)	PROCESSED BY (Print name and sign)	DATE (YYYYMMDD)	
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign)	DATE (YYYYMMDD)	

DD FORM 2875 (BACK), APR 2005 Reset

Figure 3-7—System Access Authorization Request-Continued

HQMC IPSP SOP

DD 2875 ADDENDUM STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

- You consent to the following conditions:

- o The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- o At any time, the U.S. Government may inspect and seize data stored on this information system.

- o Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

- o This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

- o Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and

User Initials _____

Figure 3-7—System Access Authorization Request-Continued

Encl (3)

HQMC IPSP SOP

data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence

investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (Le., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

o All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

User Initials _____

Figure 3-7--System Access Authorization Request-Continued

Encl (3)

HQMC IPSP SOP

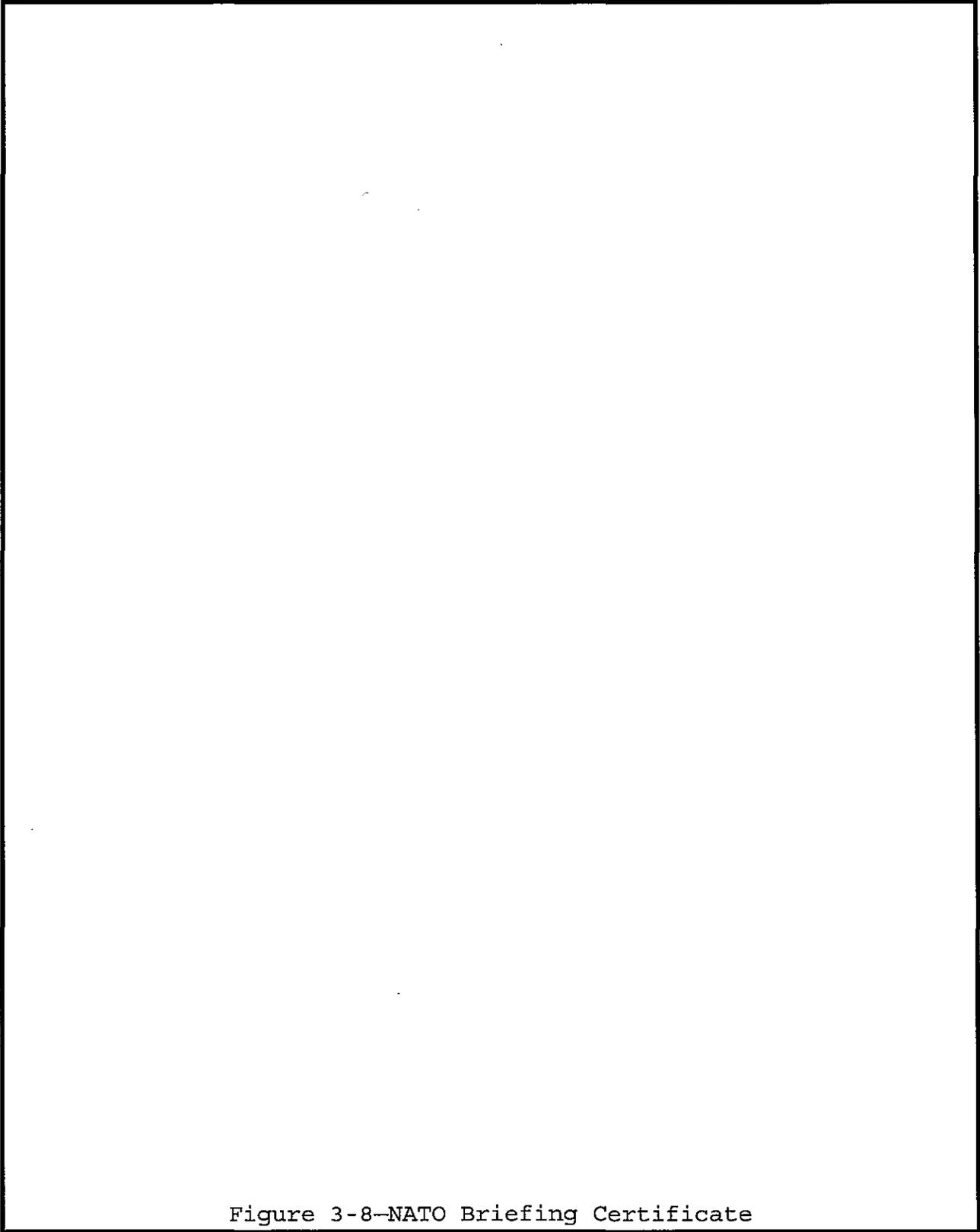


Figure 3-8-NATO Briefing Certificate

Encl (3)

HQMC IPSP SOP

(LETTER HEAD)

5500
XX
DATE

From: Security Coordinator, Staff Agency/Activity Name
To: Security Manager, Headquarters U.S. Marine Corps

SubJ: REQUEST FOR NATIONAL CAPITAL REGION (NCR) COURIER CARD

1. Request the following personnel be issued a NCR Courier Card. Due to additional duties in billet assignment, the individual listed below will be required to carry classified material within NCR.

<u>NAME</u>	<u>RANK</u>	<u>LAST 4 SSN</u>	<u>ACCESS</u>	<u>DURATION</u>
MARINE, I. M.	SGT	XXX XX 1234	TOP SECRET	3

2. If there are questions regarding this matter please contact (list point contact information).

SIGNATURE

Figure 3-9-Courier Card Request Memorandum

Encl (3)

LISTS OF ACCEPTABLE DOCUMENTS

LIST A	OR	LIST B	AND	LIST C
Documents that Establish Both Identity and Employment Eligibility		Documents that Establish Identity		Documents that Establish Employment Eligibility
1. U.S. Passport (unexpired or expired)		1. Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address		1. U.S. social security card issued by the Social Security Administration (other than a card stating it is not valid for employment)
2. Certificate of U.S. Citizenship (Form N-560 or N-561)		2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address		2. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350)
3. Certificate of Naturalization (Form N-550 or N-570)		3. School ID card with a photograph		3. Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal
4. Unexpired foreign passport, with I-551 stamp or attached Form I-94 indicating unexpired employment authorization		4. Voter's registration card		
5. Permanent Resident Card or Alien Registration Receipt Card with photograph (Form I-151 or I-551)		5. U.S. Military card or draft record		
6. Unexpired Temporary Resident Card (Form I-688)		6. Military dependent's ID card		4. Native American tribal document
7. Unexpired Employment Authorization Card (Form I-688A)		7. U.S. Coast Guard Merchant Mariner Card		5. U.S. Citizen ID Card (Form I-197)
8. Unexpired Reentry Permit (Form I-327)		8. Native American tribal document		6. ID Card for use of Resident Citizen in the United States (Form I-179)
9. Unexpired Refugee Travel Document (Form I-571)		9. Driver's license issued by a Canadian government authority		7. Unexpired employment authorization document issued by DHS (other than those listed under List A)
10. Unexpired Employment Authorization Document issued by DHS that contains a photograph (Form I-688B)		For persons under age 18 who are unable to present a document listed above:		
		10. School record or report card		
		11. Clinic, doctor or hospital record		
		12. Day-care or nursery school record		

Illustrations of many of these documents appear in Part 8 of the Handbook for Employers (M-274)

Figure 3-11-List of Acceptable Identifications

HQMC IPSP SOP

(LETTER HEAD)

5500

XX

DATE

From: Security Coordinator, Staff Agency/Activity Name

To: Security Manager, Headquarters U.S. Marine Corps

SubJ: REQUEST ISSUANCE OF NCR "A" (CONCEALED CARRY) BADGE

1. Request the individual listed below be granted a NCR-A badge. The following information is provided:

- a. NAME:
- b. SSN:
- c. DOB/POB:
- d. CLEARANCE LEVEL-DATE:

2. Justification: _____

3. If there are questions regarding this matter please contact (list point contact information).

SIGNATURE

Figure 3-12-Alarm Zone Request

HQMC IPSP

Information Security

1. Marking. Per reference (b), the proper marking of a classified document is the specific responsibility of the original or derivative classifier. Although markings on classified documents are intended primarily to alert holders that classified information is contained in a document, they also serve to warn holders of special access, control or safeguarding. The following marking requirements must be met:

a. All classified information shall be clearly marked with the date and office of origin, the appropriate classification level and all required "associated markings". "Associated markings" include those markings that indentify the source of classification (or for original decisions, the authority and reason for classification); downgrading and declassification instructions; warning notices, intelligence control markings and other miscellaneous markings. Refer to reference (b) for guidance on the placement of associate markings.

b. Marking is required on all information technology (IT) systems and electronic media, including removable components that contain classified information. IT systems include any equipment, interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data. Electronic media includes Universal Serial Bus drives, flash drives, pen drives, compact disks, scanners, videotapes, floppy disks, recordings, etc. IT systems that process classified data, in forms other than traditional documents, such as weapon, navigation, and communication systems also require appropriate marking.

2. Safeguarding. Staff Agencies/Activities shall ensure that classified information is processed only in secure facilities, on accredited IT systems, and under conditions which prevent unauthorized persons from gaining access.

a. Control Measures

(1) All Top Secret information, including copies originated or received by HQMC shall be continuously accounted for, individually serialized, and entered into HQMC Top Secret

Encl (4)

HQMC IPSP SOP

Inventory Database. HQMC TSCO shall obtain a record of receipt from each recipient for Top Secret information distributed internally and externally. Top Secret Information shall be physically sighted and accounted for at least semi-annually and more frequently as circumstances warrant (e.g., change of TSCO, or upon report of loss or compromise). Staff Agencies/Activities receiving new Top Secret documents will contact the HQMC TSCO and provide the following information: Bucket Tag Number, Short Title Subject, Document Date and Date of Receipt.

(2) Secret/Confidential information. Staff Agencies/Activities shall establish administrative procedures for the control of Secret/Confidential information appropriate to their staff agency, based on an assessment of the threat, and the location and mission of their Staff Agency/Activity. These procedures shall be used to protect Secret information from unauthorized disclosure by access control and compliance with the marking, storage, receipting, transmission, and destruction requirements of reference (b) and this SOP.

b. Working Papers

(1) Secret and Confidential working papers such as classified notes from a training course or conference, research notes, rough drafts, and similar items that contain Secret or Confidential information shall be:

(a) Dated when created;

(b) Conspicuously marked centered top and bottom of each page with the highest overall classification level of any information they contain along with the words "Working Paper" on the top left of the first paragraph in letters larger than the text;

(c) Protected per the assigned classification level; and

(d) Destroyed, by authorized means, when no longer needed.

(2) Staff Agencies/Activities shall establish procedures to control and mark all Secret and Confidential working papers in the manner prescribed for a finish document when retained more than 180 days from the date of creation or official release

Encl (4)

HQMC IPSP SOP

outside the organization. A document transmitted over a classified IT system is considered a finished document.

(3) The accounting, control, and marking requirements prescribed for a finished document will be followed when "working papers" contain Top Secret information.

c. Daily Control Measures

(1) 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. The exact nature of security requirements will depend on a thorough security evaluation of local conditions and circumstances. Security requirements must allow for the accomplishment of essential functions, while affording classified information the appropriate security. The requirements specified in this SOP represent the minimum acceptable standards.

(2) Persons in possession of classified material are responsible for safeguarding the material at all times. An office space that is not authorized for "open storage" requires classified material to be secured in a GSA approved security container whenever the material is not in use, in the custody of authorized personnel or during after hours to prevent inadvertent disclosure. Procedures must be followed to ensure classified information is not disclosed, discussed within the hearing of, or uncovered within the presence of unauthorized persons.

(3) Individuals will not remove classified material from designated offices or work areas except in the performance of their official duties and under conditions providing the protection required by this SOP. Approval will be given only when there is an overriding need, the physical safeguards including approved storage are provided, and a list of the material removed is kept at the HQMC Staff Agency/Activity. Approval to remove classified material will not include permission for overnight storage in any location other than a secure Government or cleared contractor facility.

(4) Staff agencies/activities storing classified information will ensure adequate security measures are in place to prevent unauthorized persons from gaining access to

Encl (4)

HQMC IPSP SOP

classified information. Security measures must also prevent persons outside the building or spaces from viewing or hearing classified information. To preclude exposure to those not having a valid need-to-know, Staff Agencies/Activities should establish compartmentalization within their offices or facilities, as appropriate. The following should be done to prevent such occurrences:

(a) Sanitize all office spaces where classified material is stored, processed, or discussed when uncleared personnel are performing repairs, routine maintenance, or cleaning. These persons will be escorted at all times and all individuals will be alerted to their presence.

(b) Ensure that adequate controls are established to prevent unauthorized individuals from being exposed or gaining access to areas where classified material is used or stored.

(c) Keep extraneous material (such as unclassified papers, ADP printouts, and publications), office equipment and personal items off the tops of security containers to prevent inadvertent intermingling of classified with unclassified material, deter any suspicious tampering and eliminate any hidden compromise of the container.

(d) Burn bags will not be placed adjacent to trash receptacles because the subconscious, and habitual, act of discarding waste material in the "trash can" could result in classified material being mistakenly discarded with regular trash.

(e) Classified Military Information (CMI) and Controlled Unclassified Information (CUI) processed by Marine Corps computer-based systems must be properly safeguarded against unauthorized accidental or intentional disclosure, modification, or destruction. Safeguards will be applied so that such information is accessed only by authorized persons, is used only for its intended purpose, retains its data integrity, and is properly marked as required.

(f) All Marines, civilian employees of the Marine Corps, and DoD contractor personnel supporting Marine Corps efforts are responsible for proper protection of CMI and CUI computer-based information which comes into their possession by

Encl (4)

HQMC IPSP SOP

any means. The following measures will be in place to prevent access by unauthorized persons:

1. Classified documents removed from storage must remain within the possession of authorized persons at all times. Classified Material Cover Sheets for Top Secret (SF 703), Secret (SF 704) and for Confidential (SF 705) will be used as a covering for the top page of a classified document, or on the exterior of a folder containing classified material when it is hand delivered from one person or office to another.

2. Discuss classified information only when unauthorized persons cannot overhear the discussion. Take particular care when there are visitors or workmen present. Escorts should alert fellow workers announcing their presence when visitors or workmen are in a classified processing area.

3. Protect preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information either by destruction after they have served their purposes, or by giving them proper classification and safeguarding per reference (b) and this SOP.

4. All offices, unless open storage, with classified material out of the safe or the safe unlocked, are required to have a cleared person with rightful access to the material present at all times. Locking the office door with classified material left unsecured, and then leaving the area, constitutes a security violation.

3. Security Checks. Security Checks will be conducted at the end of the working day, ensuring all classified material is properly secured. The Activity Security Checklist (SF 701) (refer to figure 4-1) will be used to ensure that the following actions have been taken:

a. All classified material is stored in the manner prescribed.

b. Burn bags are properly stored.

c. The contents of wastebaskets have been checked for classified material. (NOTE: Burn bags and wastebaskets should not be adjacent to each other.)

Encl (4)

HQMC IPSP SOP

d. Classified notes, plastic typewriter ribbons, rough drafts, and similar items are properly secured or destroyed.

e. Security containers have been locked by the responsible custodians. Classified container checkout sheets (SF 702) (refer to figure 4-2) will be used as a record of security container locking and double checks to ensure they are locked. (The dial of combination locks must be rotated at least four complete times in the same direction when securing safes.)

f. SF 701's and 702's may be destroyed 30 days after the last entry unless they are used to support an ongoing investigation.

4. Dissemination

a. Classified information originated in a non-DoD Department or agency shall not be disseminated outside the DoD without consent of the originator except where specifically permitted.

b. Top Secret information originated within DoD shall not be disseminated outside of DoD without the consent of the originator or higher authority, except as provided for in paragraph 8-1.4 of reference (b).

c. Unless specifically prohibited by the originator, Secret and Confidential information originated within the DoD may be disseminated to other DoD components and agencies within the executive branch of the U.S. Government, except as provided for in paragraph 8-1.4 of reference (b).

5. Foreign Disclosure

a. While public domain information authorized and approved by the Public Affairs Office can be freely shared with foreign governments and interest, CMI and CUI is only shared with foreign governments when there is a clearly defined benefit to the U.S. Government. Disclosure of such information can be made only by a Designated Disclosure Authority (DDA) or in accordance with a Delegation of Disclosure Authority Letter (DDL) issued in support of a specific international agreement.

b. Foreign Visitors must have either a Foreign Visit System (FVS) request submitted through their embassy or be on

Encl (4)

HQMC IPSP SOP

Invitation Travel Orders (ITO) and vetted accordingly before access can be given. Official visits include one-time recurring, and extended visits. Upon receipt of a foreign visit request, Security Coordinator's will ensure the HQMC Staff Agency/Activity can support the visit and that it will not conflict with other scheduled functions or operational activities. In addition, security coordinators will ensure a U.S. Contact Officer/Escort has been indentified within the receiving agency. Indentify the expected level of CMI or CUI to be disclosed or released in conjunction with the visit. Conduct verification of identification credentials to include physically viewing a photo ID of the visitor. The ID must contain an ID Number, Date of Birth, and Nationality. A foreign passport is the preferred form of official ID, but any other form of official ID which contains the above specified information is acceptable.

c. Foreign Disclosure and release actions are conducted in accordance with reference (e). For questions regarding foreign disclosure contact DC, PP&O, (PLU) at (703) 614-4221.

6. Transmission. Staff Agencies/Activities shall ensure that only appropriately cleared personnel or authorized carriers transmit, transport, escort, or hand carry classified information. The selected means of transportation should minimize the risk of a loss or compromise while permitting the use of the most cost-effective mode of conveyance.

a. All outgoing classified mailing will be done through the HQMC Security Section. The following guidelines will be followed and each item below must be provided when dropping off items to be mailed:

(1) Envelopes with loose address labels for the organization and the recipient.

(2) Point of contact for packages to be mailed.

(3) After each mail out, the point of contact will be notified by the HQMC Security Section and given the tracking number for each package.

(4) The guard mail system will not be used for the transmission of classified material. Messenger (guard mail) envelopes will not be used as the outer envelope when transmitting classified material by any means. Security

Encl (4)

HQMC IPSP SOP

Coordinators will ensure that all personnel are aware of this prohibition.

(5) All incoming mail must be sent to the below address:
COMMANDANT OF THE MARINE CORPS HQMC (CODE ARS) ROOM 1006, ATTN:
Security Manager, 2 NAVY ANNEX, WASHINGTON DC 20380-1775.

(6) If classified mail arrives to an address other than the above address, that mail must be delivered to the Security Manager for accountability.

b. Telephone. Classified information will not be discussed via telephone except as authorized on approved secure communication devices (i.e., Secure Telephone Equipment (STE)) and will not be transmitted via unapproved TELEFAX equipment located within HQMC.

c. Hand Carry

(1) All classified material hand carried within the NCR will only be done with written authorization. Routine and recurring courier assignments may be authorized by issuance of a Courier Card (DD Form 2501), which can be requested from the DirAR Division (ARS) and requires written submission of sufficient justification. Refer to figure 3-9.

(2) All classified material hand carried within this Headquarters to include bulk material, will be protected by placing an appropriate classified document cover sheet as the top page to prevent casual observation. Classified material will not be carried into common areas such as the PX, snack bar, restrooms, or the barbershop and individuals will utilize the most direct route to destination. When transporting classified material outside the building, the material must be doubled wrapped. The inner envelope must have the appropriate classification marking and the outer envelope will not reveal any information pertaining to the contents within. A briefcase may be used as the outer wrapping except when traveling via commercial airline.

(3) Individuals hand carrying classified material via commercial airline must receive prior approval from the DirAR Division (ARS).

Encl (4)

HQMC IPSP SOP

7. Storage

a. All classified material will be secured in a General Services Administration (GSA) approved security container or a certified vault or strong room. All security containers will have the "GSA Approved Security Container" metal tag affixed. If lost or destroyed, replacement labels may be obtained by providing the make, model number, and serial number to the DirAR Division (ARS).

b. Staff Agencies/Activities are responsible for safeguarding all classified information under their cognizance. This includes ensuring it is stored in the manner prescribed in this SOP when it is not being used or is not under the direct observation of cleared individuals.

c. Report any weakness or deficiency concerning equipment used to safeguard classified material to your Staff Agency/Activity Security Coordinator.

d. Do not store valuables, including money, jewelry, precious metals, etc., in the same containers used to store classified material. They may increase the risk of a container being opened or stolen, resulting in compromise of the information in the container. Additionally, placing items on top of the security container is also prohibited.

e. For identification purposes, and in the event of emergency destruction or evacuation, place a number or symbol indicating relative priority on the exterior of each security container (i.e., A or I equals Priority I, B or II equals Priority II, and C or III equals Priority III). The external container markings and instructions contained in the emergency action plan will not indicate the level of classified information stored in the container.

f. Security containers will not be requested or procured until a requirement has been validated and approved by the Staff Agency/Activity Security Coordinator. All requests for security equipment such as alarms, shredders, security containers, and locking devices will be processed through the DirAR Division (ARS) Physical Security Section. The security coordinator will ensure the following:

Encl (4)

HQMC IPSP SOP

(1) Combinations of security containers are given only to personnel who have the responsibility and possess the appropriate security clearance eligibility and access.

(2) Combinations are 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.

(3) Use Security Container Information (SF 700) (refer to figure 4-3) to maintain a record for each security container, showing the location of each, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combinations and who are to be contacted in the event the security container is found unattended.

(4) Part 1 of the completed SF 700 is placed on the interior location in the security container. Mark Parts 2 and 2A of the SF 700 to show the highest classification level and any special access notice applicable to the information stored therein. Store Parts 2 and 2A in a security container other than the one to which it applies.

(5) Provide the DirAR Division (ARS) Physical Security Section with the SF 700 for any master safe that is designated to hold other SF 700's.

(6) Access Rosters will be posted on the outside of all secure office spaces, listing personnel who have unescorted access and who to contact in the event of an emergency. Staff Agency/Activity personnel will be instructed to contact their Security Coordinator or the DirAR Division (ARS) Physical Security Section, if they forget the combination to the security container or secure office space.

(7) Utilize the Activity Security Checklist (SF 701) (refer to figure 4-1) to ensure that all areas which process classified information are properly secured. Additionally, utilization of the Security Container Check Sheet (SF 702) (refer to figure 4-2) is used to document that classified security containers, vaults and secure rooms have been opened and closed.

8. Destruction. Destroy classified information no longer required for operational purposes per reference (b). Destruction of classified information shall be executed by means

Encl (4)

HQMC IPSP SOP

that eliminate risk of recognition or reconstruction of the information.

a. Destruction Procedures. Security Coordinators shall establish procedures to ensure that all classified material intended for destruction is destroyed by authorized means and cleared personnel. Procedures shall include but are not limited to:

(1) Classified material pending destruction shall be controlled in a manner designed to minimize the possibility of unauthorized removal or access.

(2) Records of destruction are not required for Secret and Confidential information except for special types of classified information (see paragraph 7-8 and 10-17) of reference. For Top Secret the following procedures will be followed:

(a) Use OPNAV 5511/12, "Classified Material Destruction Report". Refer to figure 4-4.

(b) Record destruction of Top Secret by any means as long as the record includes complete identification of the information destroyed and date of destruction.

(c) Two witnesses shall sign the record when the information is placed in a burn bag or actually destroyed.

(d) Copy of the OPNAV 5511/12 must be provided to the DirAR Division (ARS).

b. Clean Out Day. Security Coordinators will establish at least one day each year as "clean-out" day when specific attention and effort are focused on disposition of unneeded classified material. Classified material that cannot be destroyed because of its historical value shall be reevaluated and, when appropriate, downgraded, declassified, or retired to a designated record center.

c. Burn Bag Disposal. Burn bag destruction at the Navy Annex is held every Friday unless notified otherwise and at the Pentagon Monday through Friday from 0800-0900 and again from 1100-1200. Burn Bags for the Navy Annex can be brought to the loading dock located on the 1st Floor Second Wing and for the

Encl (4)

HQMC IPSP SOP

Pentagon at the Remote Delivery Facility (RDF) located in the basement of Corridor 5. A burn bag receipt figure 4-5 will be utilized when dropping off bags. Each bag must adhere to the following guidelines.

(1) Weigh less than 10 pounds and not more than 3/4 full.

(2) The following items must be annotated on the outside of the bag: organization, phone number, highest classification of material inside the bag and if the media is something other than paper (i.e., cds, hard drives, floppy disks, etc.) mark the burn bag with "SPECIAL BURN" and notify the driver, so that the contents can be properly destroyed.

(3) Burn bags are not garbage bags and will not contain certain material such as plastic, styrofoam cups, candy wrappers, soda cans, bottles, etc. Burn bags will be periodically checked for such materials. Any burn bag containing unauthorized material will be returned to the staff agency.

9. Meetings. Classified information will not be discussed at conferences and meetings unless the release of such information serves a government purpose and adequate security measures are provided. Staff Agencies/Activities holding routine, in-house meetings, attended by members of this Headquarters or official visitors authorized under this SOP, have full security responsibility for those meetings. The following guidance will be followed for all classified meetings:

a. Per reference (b), paragraph 7-13, all meetings and conferences where classified information is discussed will only be conducted in approved U.S. Government controlled facilities.

b. The Staff Agency/Activity is responsible for compliance with security regulations when hosting meetings/conferences at conference facilities.

c. Verifying clearance, maintaining access rosters, and access control measures are the responsibility of the Staff Agency/Activity. Differences in clearance and access rosters will be resolved by the Staff Agency/Activity Security Coordinator prior to permitting access to the conference. All clearances of personnel not assigned to HQMC will be verified

Encl (4)

HQMC IPSP SOP

and certified by the Staff Agency/Activity Security Coordinator. Clearance data on TAD orders is not adequate for granting access to classified information.

d. Hotels or civilian conference rooms/convention centers are not authorized. When choosing a location for your brief, the space must be designated as a secure space to hold such a brief. If the space is not designated as a secure space, a guard must be posted at the points of ingress and egress to ensure that only authorized personnel are admitted into the briefing area, and that unauthorized people are not listening to conversations thru doors or windows. The Staff Agency/Activity Security Coordinator is ultimately responsible and must ensure these measures are enforced.

10. Compromise and Other Security Violations. There are two types of security violations: violations resulting in compromise or possible compromise of classified information, and violations in which security regulations are breached but no compromise occurs. Compromise occurs when classified information is disclosed to a person who is not authorized to have access to that information. The unauthorized disclosure may occur knowingly, willfully, or through negligence. A compromise is confirmed when conclusive evidence indicates that classified information has been disclosed to an unauthorized person. A possible compromise occurs when facts indicate that classified information may have been subjected to unauthorized disclosure, but compromise is not positively certain. The following will take place upon discovery of a known or possible compromise:

a. Any individual who becomes aware of a security violation and/or the compromise of classified information or material will immediately notify their Security Coordinator who will inform the HQMC Security Manager.

b. Heads of Staff Agencies/Activities will notify the DirAR Division (ARS) of all instances involving loss, compromise, or subjection to compromise of classified information or material. Upon report of a security violation or the possible compromise of classified information, the Staff Agency/Activity Security Coordinator will conduct an inquiry to discover the facts and recommend a preliminary inquiry of up to a JAG Manual Investigation, if required. This determination will be based on whether the classified material was compromised or subjected to

Encl (4)

HQMC IPSP SOP

compromise, if any significant security weaknesses exist, or if punitive administrative or judicial action is warranted.

c. Electronic Spillages. In the event of electronic spillage (introducing classified information to unclassified system), the Staff Agency/Activity Security Coordinator will facilitate the following:

(1) Immediately inform the HQMC Security Manager and Information Assurance Manager (ARI).

(2) Complete the NMCI Spillage Questionnaire. Refer to figure 4-6.

(3) Conduct an inquiry to discover the facts and recommend a preliminary inquiry up to a JAG Manual Investigation, if required.

Encl (4)

HQMC IPSP SOP

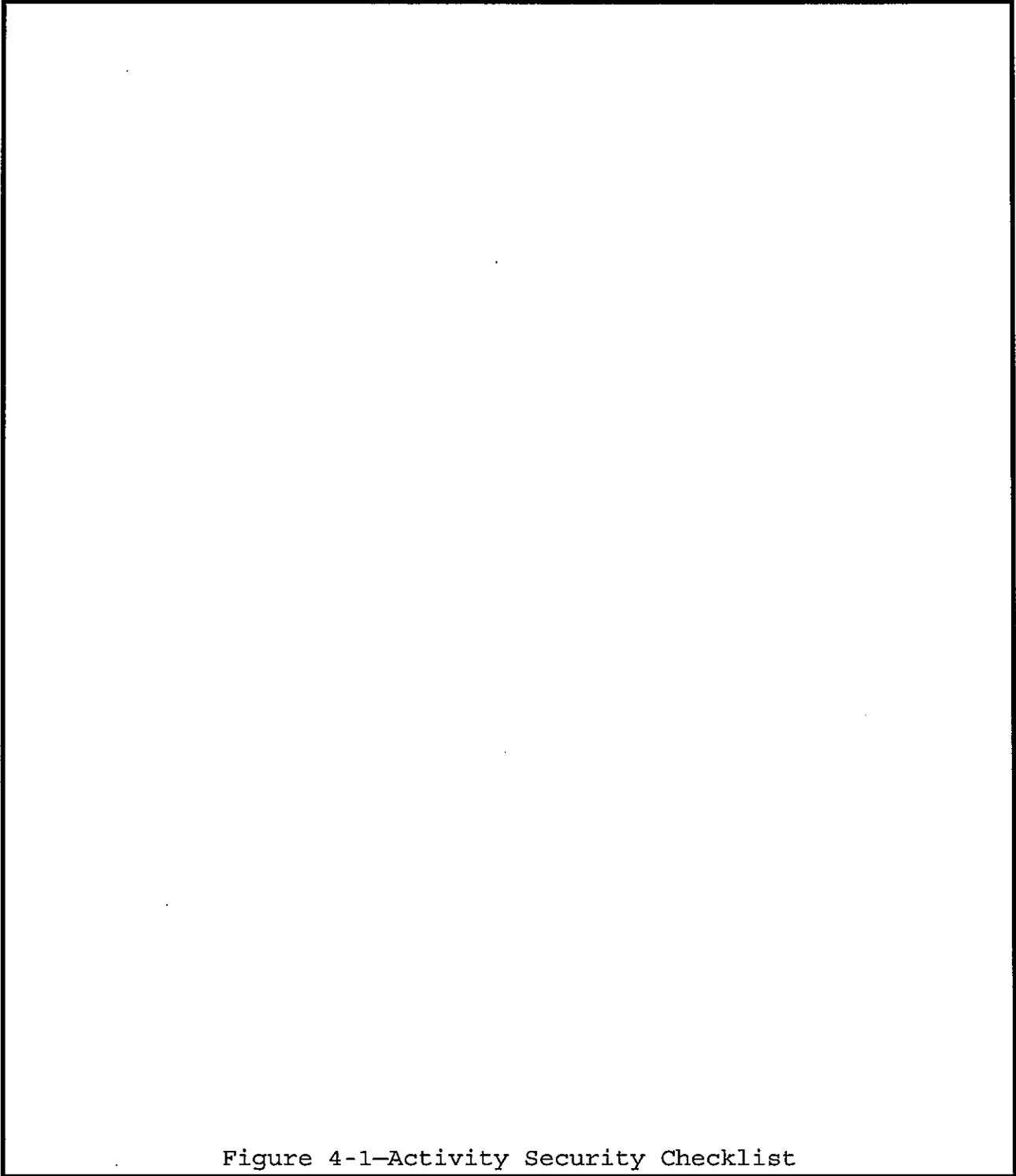


Figure 4-1-Activity Security Checklist

Encl (4)

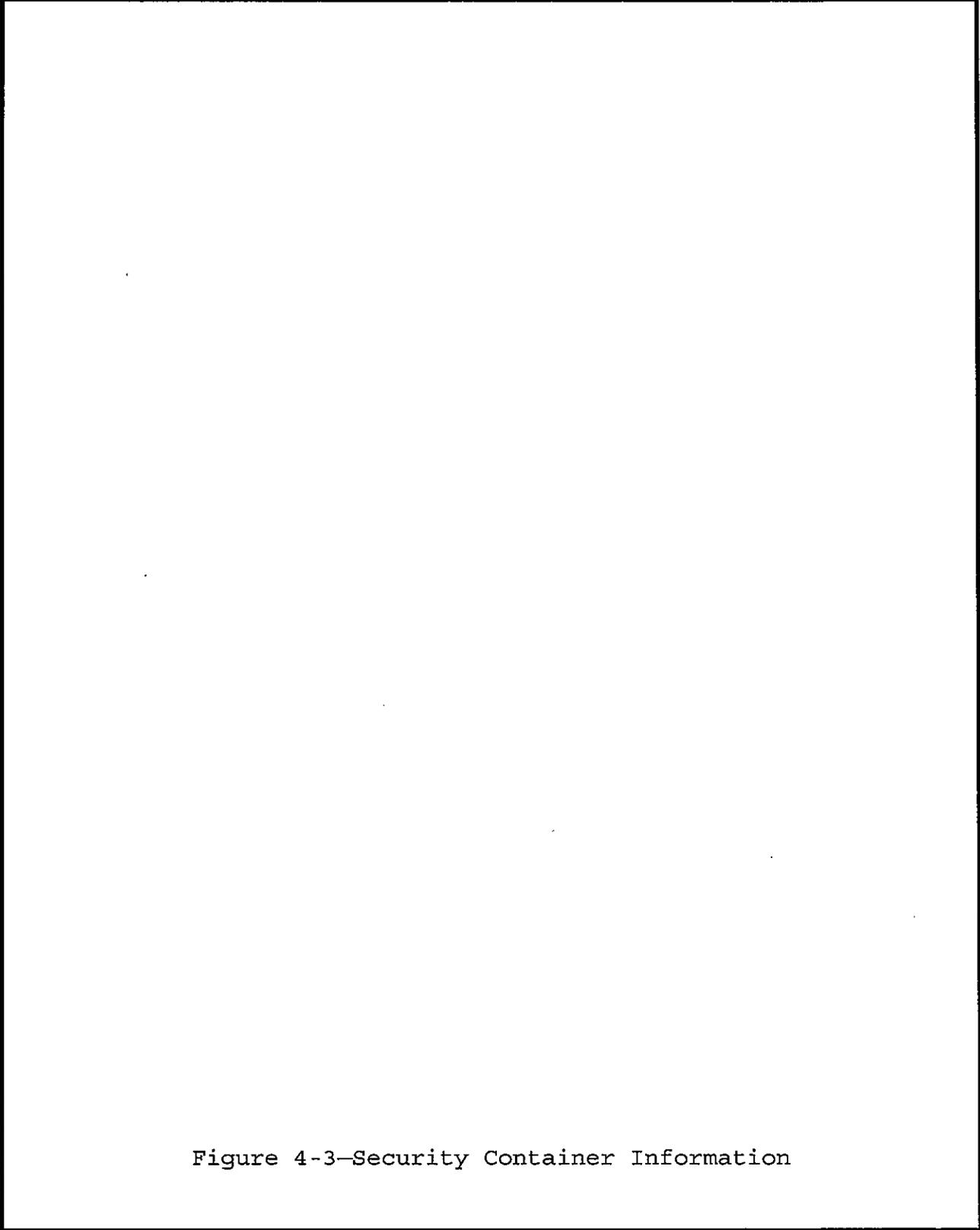


Figure 4-3—Security Container Information

Encl (4)

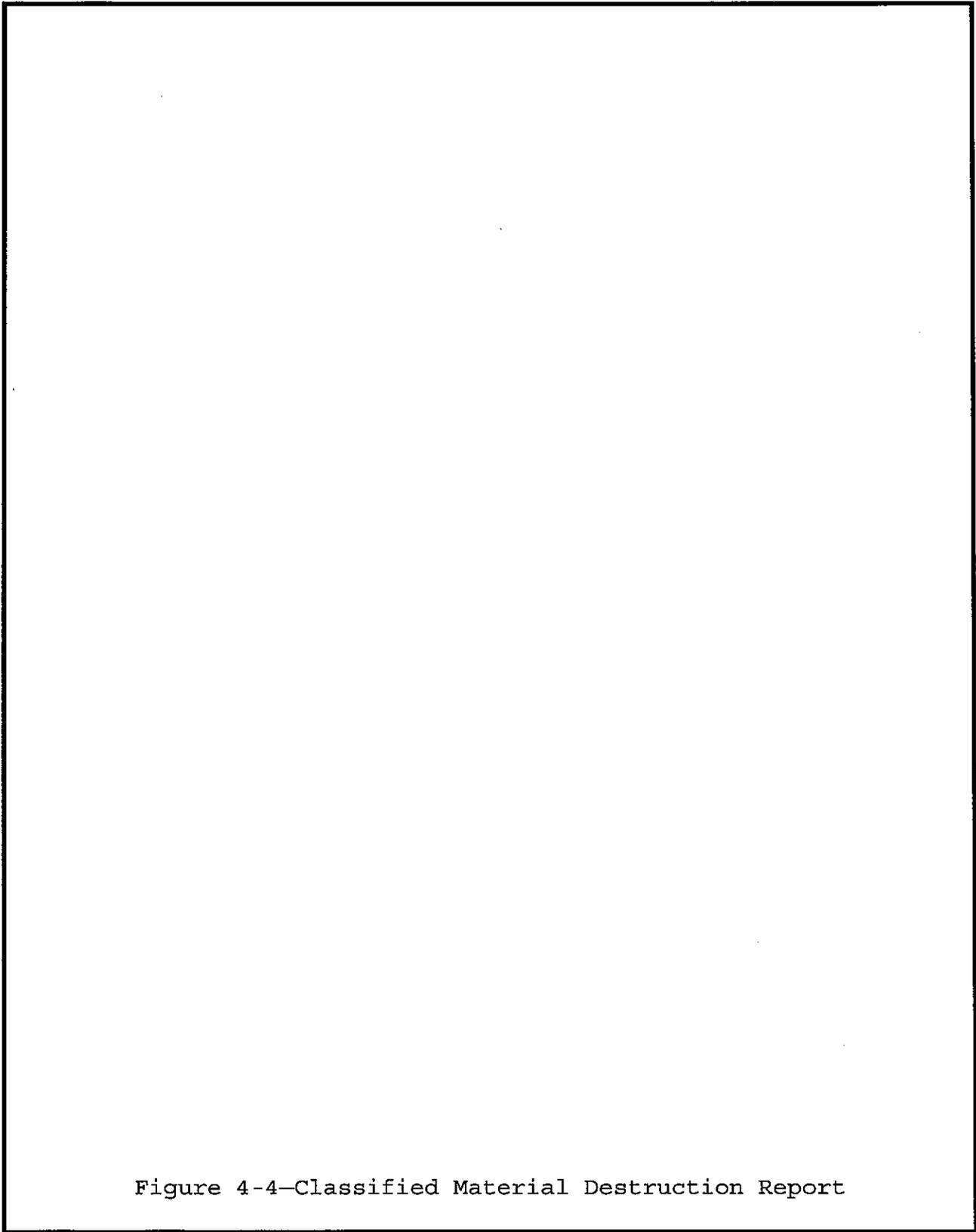


Figure 4-4—Classified Material Destruction Report

Encl (4)

HQMC IPSP SOP

FOR OFFICIAL USE ONLY	
CLASSIFIED MATERIAL DESTRUCTION RECORD	
1. DATE (YYYYMMDD)	2. MILITARY DEPARTMENT OR AGENCY NAME Headquarters, United States Marine Corps (HQMC)
3. OFFICE SYMBOL OR COMPONENT NAME Administration and Resource Security (ARS)	4. TELEPHONE NUMBER <i>(Include Area Code)</i> (703) 614-3609
5. NUMBER OF BAGS (NOTE: There is a ten (10) pound weight limit per bag.)	
a. NUMBER OF UNCLASSIFIED BAGS	
b. NUMBER OF CONFIDENTIAL BAGS	
c. NUMBER OF SECRET BAGS	
d. NUMBER OF TOP SECRET BAGS	
e. NUMBER OF SCI BAGS	
f. TOTAL NUMBER OF BAGS	
g. REMARKS	
6. NAME OF DELIVERY PERSON(S) <i>(Delivery person be cleared at the same level of, or higher than the material delivered.)</i>	
7. RECEIVED BY <i>(To be completed by incinerator plant personnel/driver)</i>	
DEPARTMENT OF DEFENSE CLASSIFIED WASTE FACILITY 425 OLD JEFFERSON DAVIS HIGHWAY ARLINGTON, VA 22202	
TELEPHONE: (703) 695-1828 or (703) 695-2265	

DD FORM 2843, SEP 2001

FOR OFFICIAL USE ONLY

Adobe Professional 7.0

Figure 4-5-Burn Bag Receipt

Encl (4)

HQMC IPSP SOP

NMCI Spillage Questionnaire

User: call the NMCI helpdesk - report a spillage - and the helpdesk will ask you to answer the following questions

1. Who is the Command IAM/IAM (Formally ISSM)?

Is this Unauthorized Disclosure on the Legacy/AOR'd systems, NMCI or both? If legacy, then User/IAM must contact the legacy help desk and provide information. If spillage occurred on NMCI or AOR Legacy, continue with the following steps:

2. When did the disclosure occur?

3. Did your command originate this disclosure? If yes (Go to 4)

a. Has the originator been contacted?

b. Who was the originator?

c. Who was the message sent to? (TO: line, CC line, BCC,)

4. What is the Classification of the data spilled?
(Confidential, Secret, Top Secret, U-NNPI, or C-NNPI)
(If data is Secret or below, open unclassified ticket. If message classification is above Secret, C-NNPI, Special Category (SPECAT) or above, then escalate the disclosure reporting to the High-Side Help Desk.)

5. What is the Classification of the system data went to?

6. Was the disclosure material clearly marked?

7. Are there any special markings?

8. How many users are affected? Who did this get sent too?
(Caller must provide either a list of valid user LOG ON names/Commands/ or valid NMCI distribution list. Check Global Address List (GAL) to verify distribution.)

9. Was a public folder involved?

Figure 4-6-NMCI Spillage Questionnaire

HQMC IPSP SOP

10. What is the EXACT Subject Line of disclosure? (Regardless of the type of disclosure, get the caller to cut and paste sender, receiver, and subject line for you to place in ticket)

11. Is this disclosure?

a. Physical Media disclosure or Contamination? (Go to 12)

b. E-mail? (Go to 13)

c. Message traffic? (Go to 14)

12. Physical Media disclosure or Contamination: (Hard drive, Floppy, Web page, Zip, etc)? (Media is contaminated when it contacts media of a higher classification)

a. What type of media was contaminated?

b. What are the names of the assets affected (workstation names, printer names, server names, etc)?

c. Has the IAM taken the affected workstations off the network?

13. E-mail disclosure. Was the disclosure contained within the E-mail or within an attachment? (One user sends classified E-mail or attachment to another user)

Attachment:

14. Message disclosure. What is the Date/Time/Group and originator of message:

15. Have you notified anyone else of this Disclosure? Did command IAM initiate SITREP?

Yes:

Who:

16. Have caller contact their Site Manager and Base Ops Manager with ticket number provided after this call.

Figure 4-6--NMCI Spillage Questionnaire-Continued

Encl (4)

HQMC IPSP SOP

Industrial Security

1. Responsibilities

a. Heads of Staff Agencies/Activities shall establish an industrial security program. Procedures outlined in their Industrial Security instruction shall include appropriate guidance, consistent with reference (b) and this SOP, to ensure that classified information released to industry is safeguarded.

b. Head of Staff Agencies/Activities may, at any time, deny contractor employees access to areas and information under their control for cause. However, suspension or revocation of contractor security clearances can only be affected through the Defense Industrial Security Clearance Office (DISCO). Actions taken to deny a contractor access to areas and information will be reported to the Contracting Officer Representative (COR). If SCI access is of concern, a report will also be forwarded to the Special Security Officer (SSO).

c. Contractors are required to have either a final or interim security clearance, in order to have access to classified information at HQMC. In addition, reference (g) requires that contractors granted access to classified COMSEC or NATO material must hold a FINAL security clearance for the level of classification involved.

d. Responsibility for initiating and submitting the request for a security investigation to Defense Security Service (DSS), lies with the contractor's parent company/facility. This includes requests for initial security investigations and periodic reinvestigations (PRs).

e. Contractors are responsible for designating their cleared employees as couriers, and escorts, per reference (h). Therefore, the issuance of courier cards/letters is the responsibility of the employee's parent company, not HQMC.

2. Access. DoD Contractors will perform work within HQMC in one of the following ways:

Encl (5)

HQMC IPSP SOP

a. When the Staff Agency/Activity determines that the contractor is a short or long-term visitor, the DoD Contractor must comply with HQMC security regulations and shall be included in the HQMC security education program.

b. When the contractor is a tenant within HQMC spaces, i.e., has sole occupancy of a facility or space that is controlled and occupied by the contractor, the host Staff Agency/Activity shall assume responsibility for security oversight over classified work carried out by the cleared DoD contractor employees in the facility. The Staff Agency/Activity is responsible for all security aspects of the contractor's operations in the facility/space.

3. Check-in. Security Coordinators will ensure DoD Contractors reporting to their staff agency/activity check-in with the HQMC Security Section. M&RA/MCRC contractors will check-in with the DirAR Division (ARS) office located in Marsh Center, 3280 Russell Road, Marine Corps Base, Quantico, VA. DoD contractors will have the following documents when reporting: Security Services Form (refer to figure 3-1), DoD Badge Request (refer to figure 3-2), HQ NAVMC 512 (refer to figure 3-3), SF 312 (refer to figure 3-4), DoD Badge Agreement (refer to figure 3-5), HQMC Security Orientation/Awareness Briefing (refer to figure 3-6), Visitor Request (must be submitted via the Joint Personnel Adjudication System (JPAS), (If contractor personnel are not in JPAS, a Visitor Authorization Letter (VAL) on company letterhead with the Name, Address, and Telephone Number and assigned Commercial and Government Entity (CAGE) Code, if applicable, must be submitted, with the following information: name, SSN, DOB, POB, citizenship of the employee intending to visit, access level required, contract number, and visit dates not to exceed one year), copy of the current contract Statement of Work (SOW) and Contract Security Classification Specification (DD Form 254) (refer to figure 5-1). If the contractor does not require access to classified information, the DD 254 is not required.

4. DoD Badge

a. When requesting a renewal of a DoD Badge, Security Coordinators will ensure DoD Contractors have the following documents: Security Services Form (refer to figure 3-1), DoD Badge Request (refer to figure 3-2), Visitor Request (must be

Encl (5)

HQMC IPSP SOP

submitted via the JPAS, and copy of the current contract Statement of Work (SOW).

b. DoD Contractors may not request escorting privileges unless they are required as part of their contractual duties to escort other contractor personnel and visitors, or due to limited government staff, or have an integrated office (at least half are contractors) and the need for escorting is required.

5. DD Form 254. Staff Agencies/Activities shall ensure that a DD 254 is incorporated into each classified contract. The DD 254, with its attachments, supplements, and incorporated references, is designed to provide a contractor with the security requirements and classification guidance needed for performance of a classified contract. An original DD 254 shall be issued with each request for proposal, other solicitations, contract award, or follow-on contract to ensure that the prospective contractor is aware of the security requirements and can plan accordingly. A revised DD 254 shall be issued as necessary during the lifetime of the contract when security requirements change. A final DD 254 shall be issued on final delivery or on termination of a classified contract. As required by reference (h), the DD Form 254 shall be periodically reviewed during the performance stages of the contract and a revised DD Form 254 issued if needed.

6. Common Access Card (CAC)

a. Per reference (i), Contractors who require access to the Marine Corps Enterprise Network (MCEN) account, or who must access multiple installations within the NCR on a regular basis, must meet the minimum investigation requirement of NACI prior to CAC issuance.

b. When it has been determined that a contractor does not meet the minimum investigative requirements, the Staff Agency/Activity Security Coordinator will ensure DoD Contractors submit a Public Trust Positions Security Questionnaire (Standard Form (SF) 85P) and Fingerprint Card (SF-258) (provided by the Facility Security Officer (FSO)) and Report of Separation (DD 214) (if applicable) to the HQMC Security Manager.

c. A CAC will be issued when the investigation questionnaire has been submitted to OPM for processing. In

Encl (5)

HQMC IPSP SOP

order to be issued a CAC, a contractor must present two forms of identification listed in figure 3-11. If issues exist which prevent favorable adjudication of the investigation, "No Determination Made" will be entered into JPAS, and the investigation will be forwarded to the HQMC Security Manager for final determination. Contractors not receiving a "favorable" determination will have their CAC revoked.

7. Check-out/Debriefings. All contractors assigned to HQBN, HQMC, M&RA and MCRC, must check-out with HQMC Security Section. M&RA/MCRC contractors will check-out with the DirAR Division (ARS) office located in Marsh Center, 3280 Russell Road, Marine Corps Base, Quantico, VA. Those individuals who had access to classified information must be debriefed by their respective Staff Agency/Activity Security Coordinator and the HQMC Security Manager, by signing part D of the NAVMC 512 and surrender all government issued property to the HQMC Security Office (i.e. DoD Badge, CAC). The NAVMC HQ 512 will be retained in the Staff Agency/Activity correspondence files for 2 years after the contractor departs.

8. Security Education. Refresher training must be completed annually by all contractor personnel assigned to HQBN, HQMC, M&RA and MCRC.

Encl (5)

HQMC IPSP SOP

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort)</i>		1. CLEARANCE AND SAFEGUARDING	
		a. FACILITY CLEARANCE REQUIRED:	
		b. LEVEL OF SAFEGUARDING REQUIRED:	
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>		3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>	
a. PRIME CONTRACT NUMBER		a. ORIGINAL <i>(Complete date in all cases)</i>	Date (YYMMDD)
b. SUBCONTRACT NUMBER		b. REVISED <i>(Supersedes all previous specs)</i>	Revision No. Date (YYMMDD)
c. SOLICITATION OR OTHER NUMBER	DUE DATE (YYMMDD)	c. FINAL <i>(Complete item 3 in all cases)</i>	Date (YYMMDD)
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input type="checkbox"/> NO, If yes, complete the following Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input type="checkbox"/> NO, If yes, complete the following: In response to the contractor's request dated _____, retention of the identified classified material is authorized for a period of: _____			
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>			
a. NAME, ADDRESS, AND ZIP	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>	
7. SUBCONTRACTOR			
a. NAME, ADDRESS, AND ZIP	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>	
8. ACTUAL PERFORMANCE			
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	YES NO	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR GOVERNMENT ACTIVITY	YES NO
b. RESTRICTED DATA		b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
d. FORMERLY RESTRICTED DATA		d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
e. INTELLIGENCE INFORMATION		e. PERFORM SERVICES ONLY	
(1) Sensitive Compartmented Information (SCI)		f. HAVE ACCESS TO US CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	
(2) Non-SCI		g. BE AUTHORIZED TO USE THE SERVICES OF THE DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	
f. SPECIAL ACCESS INFORMATION		h. REQUIRE A COMSEC ACCOUNT	
g. NATO INFORMATION		i. HAVE TEMPEST REQUIREMENTS	
h. FOREIGN GOVERNMENT INFORMATION		j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
i. LIMITED DISSEMINATION INFORMATION		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
j. FOR OFFICIAL USE ONLY INFORMATION		l. OTHER <i>(specify)</i>	
k. OTHER <i>(specify)</i>			

DD Form 254, DEC 89 (EF)

Previous editions are obsolete.

(GSA FPODS, Inc)

Figure 5-1 Contract Security Classification Specification

