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

IN REPLY REFER TO:
5500
ARS

AUG 0 6 2013

From: Staff Director, Headquarters Marine Corps
To: All HQMC Departments, Staff Agencies and Activities

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

Ref: (a) SECNAV M-5510.30
(b) DoD M-5200.01
(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 098/10
(j) SECNAV M-5510.36
(k) CMC WASHINGTON DC 101326Z Jun 11
(l) CNO Memo Ser N09N2/6U871156, dtd 2 Jun 06

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

1. Purpose. To publish policies and procedures directing the management of Headquarters, U.S. Marine Corps (HQMC) Information, Personnel, and Industrial Security Programs (IPSP). This Standing Operating Procedures (SOP) represents the minimum requirements for program management and is published under the cognizance of the HQMC Security Manager. Staff Agency/Activity heads may impose more stringent requirements within their staff agency/activity; if desired, but not more lenient.

2. Background. The protection of our personnel and classified information continues to be a growing challenge. Proper access, control, and accountability of classified information enhance HQMC's ability to decrease the possibility of compromise.

3. Applicability. Applicable to HQMC Staff Agencies/Activities. For the purposes of this SOP, HQMC Staff Agencies/Activities herein refers to Marine Corps Agencies/Activities aboard the Pentagon, Naval Support

Facility, the Manpower and Reserve Affairs Department and Marine Corps Recruiting Command (MCRC) aboard Marine Corps Base Quantico.

4. Authority

a. The Staff Director, HQMC is responsible for establishing and maintaining a IPSP in compliance with the provisions of Executive Order's, public laws, DoD regulations and other security directives regarding trustworthiness standards and the protection of classified information for HQMC Staff Agencies/Activities.

b. The Director, Administration and Resource Management Division (DirAR) is designated the senior IPSP and Physical Security official for HQMC Staff Agencies/Activities. The DirAR is responsible for ensuring that HQMC has an effective IPSP and for complying with all directives issued by higher authority.

5. Action. All military, civilian and government contractor personnel assigned to HQMC will comply with the provisions of this SOP. This SOP does not address every conceivable circumstance that may arise in day-to-day operations. Should such a situation occur not addressed in this SOP, the basic principles of security management, coupled with sound judgment, guidance from appointed security personnel and common sense should be exercised.

6. Though not all encompassing, this SOP provides implementing guidance geared toward the successful management of security programs within HQMC, Staff Agencies/Activities. Questions regarding this SOP should be directed to HQMC Security (ARS), at 703-614-3609 or by e-mail at smb.hqmc.security@usmc.mil.

A. A. WASHINGTON
By direction

HQMC IPSP SOP Table of Contents

Systems Support.....Encl (1)

Responsibilities.....Encl (2)

Program Management.....Encl (3)

Personnel Security.....Encl (4)

Information Security.....Encl (5)

Industrial Security.....Encl (6)

HQMC IPSP SOP

Systems Support

1. The Security Program and Information Management Branch (ARS) uses a variety of systems and databases to implement the HQMC IPSP.

a. Personnel, Physical, Information, Communications Security System (PPICSS). PPICSS is a web-enabled, single-source-solution, for security program management and services. PPICSS will be utilized to request security services which include, but not limited to check-ins, background investigations, access to classified information, DoD Badges, contractor CAC's, locks, office space accreditations, swipe access and cryptographic equipment. PPICSS will also be utilized by all HQMC personnel to access and complete required annual security training. A PPICSS user manual is available to appointed Security Coordinators by contacting the HQMC Security Manager. PPICSS helpdesk support will be available during normal business hours for Security Coordinators only. HQMC personnel will report PPICSS issues to their respective Security Coordinators. All forms contained within this SOP are accessible via PICCS.

b. Classified Document Control Catalog (CDCC). The CDCC is a section of PPICSS that will be utilized by HQMC Personnel with access to classified information to manage inventories, transference, itemization and destruction of classified material. Classified Hard Disk Drives (HDD) and media created by way of the “write-to-media” function will be managed using the CDCC.

c. Joint Personnel Adjudication System (JPAS). JPAS is the Department of Defense (DoD) personnel security clearance and access database. It facilitates personnel security program management for the DoD Central Adjudication Facility (CAF), for DoD security managers, and Sensitive Compartment Information (SCI) program managers. JPAS is the system of record for personnel security adjudication, clearance and verification history. JPAS interfaces with Defense Security Service (DSS) and the Office of Personnel Management (OPM) to populate personnel security investigation data. DoD commands are required to use JPAS to record all access determinations which includes temporary access, upgrades, downgrades, suspensions, continuous evaluation reports, and visit requests.

Enclosure (1)

d. Trusted Associate Sponsorship System (TASS). TASS is a web based system used by authorized personnel to sponsor contractor personnel for issuance of a Common Access Card (CAC) via Defense Enrollment Eligibility Defense Enrollment Eligibility Reporting System (DEERS). The CAC is used by military, civilians, eligible contractors and federal government affiliates to gain access to the Marine Corps Enterprise Network, and for physical access to DoD installations.

e. Electronic Questionnaires for Investigations Processing (e-QIP) system. The e-QIP system is an automated, web-based system that was designed to facilitate the processing of standard investigative forms used when conducting background investigations for Federal security, suitability, fitness and credentialing purposes. This e-QIP system allows the user to electronically enter, update and transmit their personal investigative data over a secure internet connection to a requesting agency.

Responsibilities

1. Per reference (a), the Head, Security Programs and Information Management Branch (ARS) is responsible for the formulation, implementation and enforcement of information, personnel and industrial 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, personnel, 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 information originated by 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 information at HQMC and 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, Personnel, and Industrial Security Program 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.

3. ARS Security Operations Chief (ARSOC). The ARSOC is responsible for the day-to-day operations of the security section under the cognizance of the security manager and assistant security manager. The ARSOC will:

a. Serve as the security manager in the absence of the security manager and assistant security manager for the day-to-day operations.

b. Distribute assignments to security specialists and ensure timely and accurate completion of all work assigned.

c. Serve as the liaison between the security specialists and the HQMC Security Coordinators for all matters pertaining to assignments and business processes.

d. Provide seamless, efficient and first-rate support to twenty staff agencies/activities populated by approximately 3800 military, civilian and contractor personnel, ensuring compliance with personnel and information security policy and regulation.

e. Serve as an assistant to the security manager and assistant security manager to support all aspects of security management, advising management on matters affecting information and personnel security, with responsibilities cutting across staff functional and operational areas internal to HQMC.

f. Coordinate and advise staff agencies security coordinators on matters related to the security of classified/sensitive unclassified information within their respective areas to ensure comprehensive plans are in place to run an effective and efficient IPSP.

g. Coordinate and advises external agencies regarding security services to support official visitors to include Very Important Persons (VIPs).

4. ARS Information Security Specialist (ARISS). The ARISS is responsible for the day-to-day Information Security Management operations for HQMC with a focus on implementing DoD Information Security policies throughout the Headquarters. The ARISS will:

a. Enforce policy and procedures related to information security in accordance with reference (b).

b. Manage the implementation and compliance with information security policy to include, security training/education and security awareness throughout the Headquarters.

c. Serve as the HQMC North Atlantic Treaty Organization (NATO) Control Officer.

d. Coordinate and advise Staff Agency/Activity Security Coordinators and Security Assistants on matters related to the security of classified information within their respective areas to ensure comprehensive protection and destruction plans are in place.

e. Ensure Staff Agencies/Activities are in compliance with Executive Orders, Department of Defense and Secretary of the Navy policy decisions regarding Information Security Policy.

f. Serve as the HQMC site administrator for the Classified Document Control Catalog (CDCC).

g. Coordinate with HQMC Cyber Security to ensure classified information is processed, stored, or transmitted on the Automated Information Systems (AIS) and is protected in accordance with reference (b).

5. ARS Electronic Key Management System (EKMS) Manager (AREKMS). The AREKMS is responsible for all actions associated with the receipt, handling, issue, safeguarding, accounting, and disposition of Communication Security (COMSEC) material assigned to an EKMS account and also serves as the primary advisor to DirAR (ARS) on EKMS account management matters. The AREKMS Manager will:

a. Acquire, monitor, and maintain HQMC authorized COMSEC holdings. Maintain complete accountability of records, including a complete running inventory of all COMSEC material chargeable to the HQMC COMSEC account.

b. Provide written guidance to COMSEC local holders/users concerning proper safeguarding, handling, and accounting procedures for COMSEC material and equipment.

c. Provide EKMS program support for the primary HQMC account and other sub-accounts located throughout the National Capital Region.

d. Supervise the EKMS Program for COMSEC material systems. Manage the reserve, Reserve-on-Board (ROB), contingency material, and hardware equipment.

e. Assume responsibility for the installation, monitoring, maintenance and training of personnel that use COMSEC material and equipment.

6. ARS Physical Security Specialist (ARPSS). The ARPSS is responsible for the management of the HQMC Physical Security Program. The ARPSS provides guidance and recommendations for evaluating, planning, and implementing the HQMC physical security program. The ARPSS will:

a. Provide technical expertise and leadership to the design, formulation, and development of physical security policies, standards, systems, and procedures for implementation throughout HQMC.

b. Evaluate new or different types of security systems and equipment for application within HQMC. Perform cost benefit analysis and recommend installation/implementation of systems and equipment.

c. Serve as technical expert on approved protection systems designated to provide maximum security to HQMC Staff Agencies/Activities with minimal impact to their mission.

d. Develop and maintain the HQMC Lock and Key Control Program. This program is designed to protect or secure restricted areas, classified material, sensitive material, supplies, and other critical assets.

e. Perform Physical Security Surveys and Restricted Area Certifications, for all office spaces throughout HQMC requiring restricted area designations to comply with applicable information assurance and physical security regulations.

7. ARS Security Specialist (ARSS). The ARSS is responsible for technical and help desk support in areas of Personnel,

Information and Industrial Security as determined by the Security Manager. The ARSS will:

a. Process requests for personnel security investigations and the taking of fingerprints.

b. Process Department of Defense (DoD) Badge request in order for personnel to obtain building pass.

c. Issue and account for courier cards and letters.

d. Process Common Access Card (CAC) requests in order for contractor personnel to obtain CAC.

e. Endorse requests for SIPR network accounts.

f. Process requests for swipe and pin access to controlled and restricted areas.

g. Process personnel check-in and check-outs.

8. HQMC Top Secret Control Officer (TSCO)

a. The HQMC TSCO is responsible for the receipt, custody, accounting, reproduction, and disposition of Top Secret information received or originated by this Headquarters, with the exception of Sensitive Compartmented Information (SCI) which is controlled by the Special Security Office (SSO).

b. Per reference (b), the duties of the HQMC Top Secret Control Officer (TSCO) will be assigned in writing by the Director, Administration and Resource Management Division (DirAR). Designees must be an officer/enlisted E-7 or above or a civilian employee, GS-9 or above. The TSCO must be a U.S. citizen and possess a final Top Secret security clearance.

9. 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 an Agency/Activity SOP specifying how the requirements of this SOP, and other security directives affecting the Staff Agency/Activity, will be implemented. Contents of the instruction must be written in such a way so that they are understood by all agency/activity personnel and

fully executable. The successful execution of the SOP may require consideration of manpower and fiscal constraints.

b. Develop an emergency plan for the protection, removal, or destruction of classified information in case of fire, natural disaster, civil disturbance, terrorist activities or enemy action. Plans that are developed will contain precautionary measures which can be taken prior to an emergency to include:

(1) Securing ALL classified material and NATO material at the end of each workday in a GSA approved security container. Leaving classified information or NATO material out overnight in an Open Storage Secret (OSS) further increases the risk of loss.

(2) Limiting the volume of classified material and NATO material, held to the minimum amount necessary for operations.

(3) Ensuring all documents, file folders, and binders are clearly and properly marked according to their contents.

c. 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. The person designated must be an officer/enlisted E-6 or above or a civilian employee, GS-9 or above, with sufficient authority and staff to manage the program. 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 or Access National Agency Check with Written Inquires (ANACI).

d. Establish procedures to report questionable or unfavorable information to the HQMC Security Manager on staff agency/activity personnel who have been granted access to classified information, or who have eligibility to classified information or assigned to sensitive duties.

10. 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. Security Coordinators will implement the security programs within their Agency/Activity by:

a. Having direct and ready access to the Executive Assistant or Deputy Commandant/Director ensuring all pertinent issues concerning security program management are addressed.

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

c. 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).

d. Utilizing the Security Assessment Checklist, available in Security Note 04-13, and conduct Staff Agency/Activity Security Self Assessments to ensure the security program is compliant with all policies and regulations.

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

f. Enforcing classified information control by means of receipt, distribution, inventory, reproduction and disposition.

g. Ensuring personnel who create, process, or handle classified information are fully trained on the requirements to properly mark classified information.

h. Ensuring the DirAR (ARS) is notified of all:

(1) Instances involving loss, compromise, or subjection to compromise of classified information.

(2) Information Technology (IT) System spillages (i.e., inappropriate levels of classified information are introduced to an unclassified or classified non-SCI IT System). Notify the Director, Intelligence Department (SSO) when information is identified as SCI. Refer to enclosure (5) for guidance on reporting procedures.

i. 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.

j. Ensuring that only appropriately cleared, authorized, and briefed personnel transmit, transport, escort, or hand carry classified information.

k. Ensuring that personnel have the appropriate clearance eligibility for their billet, the need to know, and have received all required security briefs before requesting access to classified information.

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

m. Notify the DirAR (ARS) regardless of circumstances:

(1) Any incident or situation that could affect Staff Agency/Activity personnel continued eligibility to access classified information.

(2) When personnel who have access to classified information have entered the following status: Unauthorized Absentees, Deserters, and Civilians Absent Without Leave (AWOL).

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

o. Submitting visit requests (to outside agencies) via JPAS for personnel under their cognizance.

p. Ensuring a current Staff Agency/Activity Accreditation Letter is on file for review by DirAR (ARS).

q. Ensuring access rosters that identify personnel authorized to enter a controlled access area in performance of their duties are posted according to the provision of this SOP.

r. Establish procedures for end of the day security checks, utilizing the Activity Security Checklist Standard Form, (SF 701), and the Security Container Check Sheet (SF 702), to ensure that all areas which process classified information are properly secured.

s. Ensuring all combinations have been changed and recorded on the Security Container Information (SF 700), according to the provision of this SOP.

t. Establish an industrial security program if the Staff Agency/Activity engages in the purchase of a system, technology or information that is classified or when cleared DoD contractors operate within areas under their direct control. Refer to enclosure (6) for guidance.

11. Agency Top Secret Control Officer (TSCO). Staff Agencies/Activities holding Top Secret material must appoint a TSCO in writing, who is responsible for the receipt, control, reproduction, destruction, transmission and inventory of Top Secret material. The Staff Agency/Activity Security Coordinator may also be designated as the Staff Agency/Activity Top Secret Control Officer. Personnel designated as the TSCO must be an officer, non-commissioned officer E-6 or above or a civilian employee, GS-9 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 reference (b).

12. HQMC Security Contracting Officer Representative (SCOR). Per reference (j), the HQMC SCOR shall ensure that the industrial security functions specified below are accomplished when classified information is provided to industry for performance on a classified contract. The SCOR will:

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.

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.

13. Trusted Associate Security Manager (TASM). The DirAR (ARS) has been identified as the HQMC TASM for the Trusted Associate Sponsorship System (TASS), Site ID 173429. The TASM will be responsible for:

a. Troubleshooting TASS questions and issues for the site.

b. Managing site Trusted Agents (TAs).

c. Training all site TA’s operating TASS.

d. Ensuring positive identification of all site TAs.

e. Ensuring all Contractor personnel requiring issuance of Common Access Card (CAC) have at a minimum been the subject of a favorable adjudicated National Agency Check with Written Inquires Investigation (NACI).

f. Ensure Contractor TASS Re-verifications are completed in accordance with TASS requirements.

g. Ensure CAC’s are revoked when contractor personnel are no longer assigned to HQMC or are not meeting the investigative requirement for issuance.

(LETTER HEAD)

5510
XXX
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) DoD M-5200.1
(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

Date

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

Enclosure (2)

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

(LETTER HEAD)

5510
XXX
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) DoD M-5200.1
(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

Date

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

Enclosure (2)

(LETTER HEAD)

5510
XXX
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) DoD M-5200.1
(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

Date

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

Enclosure (2)

Letter

Enclosure (2)

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 (ARS) via the Staff Agency/Activity Security Coordinator.

2. Records Disposition. The following instructions are provided:

a. Appointment Letters. Appointment letters for Staff Agency/Activity Security Coordinators, Top Secret Control Officers (TSCO), and the assistants will be retained for a period of two years after the individual assignment has been terminated.

b. Inquires and Investigations. Reports of completed Inquires and Investigations will be retained for 5 years. This includes but is not limited to correspondence pertaining to security violations, infractions, incidents, hazards, or deficiencies in the Staff Agency/Activity.

c. Destruction Records. A record of destruction is required for Top Secret information. OPNAV 5511/12, “Classified Material Destruction Report”, may be 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. Emergency Action Plans. 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.

3. Staff Agency and Activity Standard Operating Procedure. Staff Agencies/Activities are required to publish, and keep current, a written SOP in regards to internal security procedures. Internal security procedures will include, at a minimum, the following actions:

a. Requesting access to classified information.

b. Accounting for personnel attached to the Staff Agency/Activity and control of visitors.

c. Accounting and controlling of Top Secret material.

d. Establish procedures that facilitate the oversight of classified information by addressing:

(1) Accountability of classified material on hand and personnel with authorized access.

(2) Limited reproduction as necessary to accomplish Staff Agency/Activity mission or to comply with applicable statutes or directives.

(3) Classified information intended for destruction is destroyed by authorized means and appropriately cleared personnel.

(4) Safeguard measures and controls that are prescribed to protect classified information.

(5) Review of classified information for proper classification markings, downgrading, and declassification.

e. Reporting of all possible Security Violations and Infractions.

f. Security education.

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 3-1 is a USV Checklist for your use. DirAR (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 assessment will review procedures, inventory documents, and ensure that all security issues are addressed. An update of the

security assessment checklist will be published yearly via separate correspondence.

6. Security Manager In-Call. All newly appointed staff agency/activity Security Coordinators will meet with the HQMC Security Manager for an in-call to review policy, address responsibilities and to ensure Security Coordinators are provided with the necessary skill sets and knowledge to manage the agency/activity IPSP proficiently.

7. Security Coordinator Meetings. The DirAR (ARS) will periodically hold security coordinator meetings (quarterly) 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 (ARS) in advance of the meeting.

8. Security Coordinator of the Year Award Program. This award program will recognize Security Coordinators of a large Staff Agency/Activity (that has 50+ personnel) and a small Staff Agency/Activity (that has 49 or less personnel) who have demonstrated exceptional performance managing their security program. The award will be based on the following criteria:

a. No incidents involving Information Technology (IT) Spillages for the entire fiscal year.

b. No Communication Security Violations for the entire fiscal year.

c. No Physical Security Violations for the entire fiscal year.

d. No violations or infractions involving the conduct of a Inquiry or Investigation for the entire fiscal year.

e. Received a "Mission Capable" during the annual Security Assessment Visit.

f. Promoting Security Awareness within their respective Staff Agency/Activity.

g. Ensured all personnel assigned to their Staff Agency/Activity completed all required security training.

h. Received Zero violations during Unannounced Security Visits.

i. Staff Agency/Activity representation at all Security Coordinator Meetings.

j. Recipients of the award will receive a Staff Agency/Activity Award Plaque and the Security Coordinator will receive a Certificate of Commendation signed by the Staff Director, HQMC.

9. Security Notes. The DirAR (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.

10. 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 (a). 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 and Refresher Security Briefings.

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

(2) Refresher. Security Refresher Training must be completed each year by all personnel (Military, Civilian and Contractor) assigned to HQMC that reinforces the policies and procedures covered in their initial and specialized training.

(3) Counterintelligence Awareness. Personnel attached to HQMC will receive periodic briefings, annually, on all threats posed by foreign intelligence and terrorist organizations. These briefings will be scheduled annually and delivered in person by an agent of the Naval Criminal Investigative Service.

b. 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. Supervisors are ultimately responsible for procedural violations and infractions that result from improperly trained personnel. Expecting subordinates to learn proper security procedures by trial-and-error is not acceptable. This training does not require reporting outside the Staff Agency but must be recorded within the agency personnel security file.

c. Derivative Classifier Training. Personnel who perform derivative classification must complete Derivative Classification Training every 2 years. The training is available online at the Defense Security Service website, at http://www.cdse.edu/catalog/information-security.html.

d. 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. Personnel can schedule a briefing by contacting Headquarters Battalion, HQMC (S-3 Office), at (703) 614-1471. 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) 614-3609.

(2) NATO Briefing. 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 (a) and (d). A copy of the briefing certificate must be retained for 2 years after personnel have 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) 614-3350.

UNANNOUNCED SECURITY VISIT CHECKLIST

Agency: _____ Room #: _____

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. IS THERE AN EMERGENCY ACTION PLAN IN PLACE FOR THE PROTECTION AND DESTRUCTION OF CLASSIFIED MATERIAL? YES NO

11. ARE ACCESS ROSTERS POSTED, CURRENT, AND ACCURATE? YES NO

12. 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

Inspector Name: _____ Date: _____

Figure 3-1--Unannounced Security Visit Checklist

HQMC IPSP SOP

Personnel Security

1. Access. Knowledge or possession of classified information is authorized only for those whose duties require access. Employees will not 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/Activity Security Coordinator on the NAVMC HQ 512, and verified by the DirAR (ARS).

b. Personnel have executed Classified Information Non-Disclosure Agreement (NDA), Standard Form (SF) 312 as a condition of access to classified information.

c. A verbal pronouncement of the Attestation statement, accepting the responsibilities of being granted access to classified information.

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

e. Has been administered the HQMC Security Orientation Brief.

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

3. Temporary Access

a. 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.

b. Granting temporary access is a risk management decision and as such requires a favorable review of all available local records (e.g., personnel, legal, security, base/military police,

Enclosure (4)

etc.) and the questionnaire for national security positions with no significant derogatory information. Significant derogatory information is information that could, in itself, justify an unfavorable administrative action or an unfavorable security determination (e.g. DUI, criminal, financial).

c. The ultimate decision to grant temporary access will reside with the DirAR. Temporary access will not be granted in JPAS until the investigation is received and opened at the Office of Personnel Management (OPM).

d. Upon receipt of a Letter of Intent (LOI) from the Department of Defense Central Adjudication Facility (DODCAF) to deny an individual's security clearance, temporary access will be immediately withdrawn for those individuals who were granted temporary access.

4. Suspension of Access. When questionable or unfavorable information becomes available concerning an individual who has been granted access to classified information or assigned to sensitive duties the following will take place:

a. Staff Agency/Activity Director, Deputy Commandant will make a recommendation to the DirAR, on the basis of all facts, to suspend or limit an individual's access to classified information, or reassign the individual to non-sensitive duties pending a final eligibility determination by the DoD CAF.

b. The ultimate decision to suspend access will reside with the DirAR. Manpower or fiscal constraints are not sufficient reasons that will mitigate security concerns. Depending on the nature of the incident, suspension of access may occur without delay or Staff Agency/Activity recommendation.

c. Whenever a determination is made to suspend access to classified information, the individual concerned must be notified of the determination **in writing** within 10 days by DirAR By direction Authority authorized to include a brief statement of the reason(s) for the suspension action consistent with the interest of national security.

d. DirAR (ARS) will report the information to DODCAF via JPAS and suspend access to classified information.

e. Staff Agency/Activity Security Coordinator will:

(1) Remove the individual's name from all local access rosters and notify all co-workers of the suspension.

(2) Ensure that the combination to classified storage containers to which the individual had access are changed unless sufficient controls exist to prevent access to the lock.

(3) Submit a Pentagon Force Protection Agency (PFPA) Alarmed Space Access Request Form (refer to Figure 4-13) to DirAR (ARS) requesting to have the individual's swipe access to Open Storage Secret (OSS) areas terminated.

(4) Cancel or hold in abeyance any Permanent Change of Station (PCS) orders per MARADMIN 659/09.

f. If after suspension of access, DODCAF adjudicates the reported information favorably, that information will no longer be the basis for continued suspension of access.

5. North Atlantic Treaty Organization (NATO) Access. Employees requiring access to NATO COSMIC or NATO Secret information must possess the equivalent final or temporary U.S. security clearance based upon the appropriate personnel security investigation, and have received and acknowledged a briefing (refer to Figure 4-6) on NATO security requirements.

6. 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 NACLC (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, credit check, and written inquiries covering the last five years to law enforcement agencies, former employers, supervisors, references, and schools. A previously conducted NACLC 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 (NACLC). The NACLC is the basic EO 12968 standard for determination of eligibility to access to Confidential and Secret classified national security information. The NACLC also provides the basis for military suitability determinations for Navy and Marine Corps enlisted members and officers. The NACLC 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 inquiries of law enforcement 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.

7. 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

(1) 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.

(2) Per reference (k), the SSBI/SBPR/PPR investigations will only be submitted to OPM for billets coded appropriately in the Total Force Structure Management System (TFSMS) or Military Occupational Specialty (MOS) designated.

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

8. Notification E-mails

a. Per reference (a) a periodic reinvestigation (PR) must be submitted every 5 years to support access to Top Secret/SCI material, every 10 years for access to Secret material and every 15 years for access to Confidential material

b. As a courtesy, the DirAR (ARS) will send notification e-mails to individuals assigned to HQMC and Marine Corps Recruiting Command (MCRC) and the Staff Agency/Activity Security Coordinator 30 days before expiration. These emails allow the employee time to gather information and prepare all documents necessary for completion of the PR through the E-QIP system. Security Coordinators are notified of requirement to ensure submission does not extend beyond 30 days.

c. Per reference (l), reinvestigations will not take place earlier than 30 days prior to expiration of the current investigation. Additionally, e-QIP system requires that once initiated by HQMC Security Office, the Personnel Security Investigation (PSI) must be completed within 30 days of the initial notification. Failure to comply for reasons that cannot be supported with proper documentation may result in the following:

(1) Suspension of access to classified information.

(2) Suspension of swipe access to office space.

(3) Deactivation of DoD building badge.

d. The provisions of reference (a) mandate that the submission of the PR is sufficient to maintain access based on previously assigned eligibility. The investigation does not have to be completed for access to be assigned or maintained.

e. Staff Agency/Activity Security Coordinators will receive all notification emails for General Officers (GO) and members of the Senior Executive Service (SES) assigned to their agency/activity. DirAR (ARS) recommends that all Staff Agencies/Activities discuss their internal notification process with the Executive Assistant (EA) in order to ensure the GO/SES population maintains a current background investigation.

9. Continuous Evaluation Program (CEP). When questionable or unfavorable information becomes available concerning an individual who has been granted access to classified information, or who has eligibility to classified information or is assigned to sensitive duties, this information will be reported to the HQMC Security Manager by the Security Coordinator.

a. Individuals are ultimately responsible to report to their supervisor or their staff agency/activity security coodinator and seek assistance for any incident or situation that could affect their continued elgilibity for access to classified information.

b. Co-workers have an obligation to advise their supervisor or Staff Agency/Activity Security Coordinator when they become

aware of information with potenatial security clearance significance.

c. Supervisors and managers play a critical role in ensuring the success of the CEP. The goal is early detection of an individual's problems. Supervisors are in a unique position to recoginize problems early and must react appropriately to ensure balance is maintained regarding the individual's needs and national security requirements.

d. The following types of information will be reported:

(1) Involvement in activities or sympathetic association with a person which/who unlawfully practice, or advocate the overthrow or alteration of the United States Government by unconstitutional means.

(2) Foreign influence concerns/close personal association with foreign nationals or nations.

(3) Foreign citizenship (dual citizenship) or foreign monetary interest.

(4) Sexual behavior that is criminal or reflects a lack of judgment or discretion.

(5) Conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations, or unwillingness to cooperate with the security clearance process.

(6) Unexplained affluence or excessive indebtedness.

(7) Alcohol abuse.

(8) Illegal or improper drug use/involvement.

(9) Apparent mental, emotional or personality disorder(s).

(10) Criminal conduct.

(11) Noncompliance with security requirements.

(12) Engagement in outside activities which could cause a conflict of interest.

(13) Misuse of Information Technology Systems.

e. Keys to a successful CEP are security education and positive reinforcement of reporting requirements in the form of management supporting confidentiality, and employee assistance referrals.

10. Check-ins. All personnel assigned to HQMC, who receive security service support, must check-in with the HQMC Security Section via PPICCS. 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 completed within the PPICSS application and submitted to the Security Section:

a. Military. DoD Building Badge Pass Request (refer to Figure 4-1), HQ NAVMC 512 (Classified Information Access Authorization) (refer to Figure 4-2), SF 312 (Non-Disclosure Agreement) when requested by the Security Section (refer to Figure 4-3), DoD Badge Agreement (refer to Figure 4-4), and HQMC Security Orientation/Awareness Briefing (refer to Figure 4-5).

b. Civilian. DoD Building Badge Request (refer to Figure 4-1), HQ NAVMC 512 (refer to Figure 4-2), (SF 312) Non-Disclosure Agreement) when requested by the Security Section (refer to Figure 4-3), DoD Badge Agreement (refer to Figure 4-4), and HQMC Security Orientation/Awareness Briefing (refer to Figure 4-5).

c. For DoD Contractor check-in procedures, refer to enclosure (6).

11. Check-out/Debriefings

a. All personnel assigned to HQMC must complete a security check-out prior to departing. The DirAR (ARS) has granted Staff Agency/Activity Security Coordinators the authority to complete the final security checkout of personnel (military, civilian and contractor) assigned to their staff agency. To ensure this process works effectively, Security Coordinators will ensure the

following procedures are followed for each individual checking out:

(1) Military Personnel Checkout. Read and sign the HQMC Command Debriefing Form, the NATO Briefing Certificate (if applicable), the Security Termination Statement (if retiring or separating), surrender the Courier Card (if applicable), the DoD Badge, and return KSV-21 Card (ECC Card) or any COMSEC Equipment assigned to the individual (if applicable).

(2) Civilian Personnel Checkout. Read and sign the HQMC Command Debriefing Form, the NATO Briefing Certificate (if applicable), the Security Termination Statement (if retiring), surrender the Courier Card (if applicable), the DoD Badge, the Common Access Card (CAC) (if retiring or leaving DoD) and return KSV-21 Card (ECC Card) or any COMSEC Equipment assigned to the individual (if applicable).

(3) Contractor Personnel Checkout. Read and sign the HQMC Command Debriefing Form, the NATO Briefing Certificate (if applicable), surrender the Courier Card Letter (if applicable), the DoD Badge, the Common Access Card (CAC) and return KSV-21 Card (ECC Card) or any COMSEC Equipment assigned to the individual (if applicable).

b. Upon completion of the security checkout, the Security Coordinator will deliver the original copy of all Security Debriefing Forms listed above, including the updated CMS Acknowledgement Form, the DoD Badge, the CAC and Courier Card/Courier Letter (if applicable) to ARS, room 2A288A.

c. Security Coordinators will retain a copy of the Security Debriefings Forms for two years from date of checkout. Security debriefing forms are items subject to inspection during yearly Assessment and Unannounced Visit Programs.

d. Staff Agencies/Activities that fail to comply with the provisions of this SOP, will forfeit the privilege of conducting internal security checkouts. Employees must then report to the Security Office to checkout with an escort provided by the Staff Agency/Activity.

e. HQMC personnel will be debriefed when one of the following conditions occurs:

(1) 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.

(2) At the conclusion of the access period when a Limited Access Authorization has been granted.

(3) When a security clearance is revoked for cause.

(4) When access is administratively withdrawn.

(5) 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.

(6) A debriefing will also be given, and a Security Termination Statement signed, when a member of any HQMC Staff/Agency inadvertently had substantial access to information which that person was not eligible to receive.

12. Secret Internet Protocol Router Network (SIPRNET) Access. To request SIRPNET Access, the following forms will be submitted within PPICSS for processing: DD Form 2875 [System Access Authorization Request (SAAR) (refer to Figure 4-7)]; and NATO Briefing and Debriefing for access to SIPRNet Computer (refer to Figure 4-8); and the DD Form 2842 [DoD Public Key Infrastructure (PKI)] Certificate of Acceptance and Acknowledgement of Responsibilities) (refer to Figure 4-9)].

13. Courier Card. To request a courier card, the Staff Agency/Activity Security Coordinator will submit a request via PPICSS, indicating what type of courier card (i.e., NCR, CONUS, OCONUS), level of access and a duration date (not to exceed two years). All personnel that have been issued a courier must read and acknowledge their responsibilities when escorting or hand carrying classified information (refer to Figure 4-10).

14. Joint Personnel Adjudication System (JPAS) Accounts. Per reference (a), Staff Agency/Activity Security Coordinators and Assistant Security Coordinators will have 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.

15. Common Access Card (CAC) Issuance. In accordance with reference (i), all CAC eligible Marine Corps civilians and contractors 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 4-11 (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 must submit a Questionnaire for National Security Positions, (SF 86) along with fingerprints.

b. Civilian personnel must 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).

c. For DoD Contractor CAC issuance procedures, refer to enclosure (6).

16. Building Access

a. The Pentagon building access is controlled by the Pentagon Force Protection Agency (PFPA). Personnel requiring access to the Pentagon must first contact their Staff Agency/Activity Security Coordinator to receive the appropriate forms to be issued a DoD Badge. To be issued a DoD Badge, an individual must present the DD Form 2249 (DoD Building Pass Application), and one (1) form of identification (refer to Figure 4-11) to the Pentagon Badge Office (room #1F1084). Personnel must fall into one of the below categories to obtain a DoD Badge:

(1) Permanent personnel that fall under the HQMC Staff Agency/Activity and work in an approved DoD facility.

(2) Individuals visiting DoD Facilities at least 3-5 times a week.

(3) To be issued a National Capital Region Badge, justification must be stated on the DoD Badge Request Form (refer to Figure 4-1) indicating that the individual requires recurring, unescorted access to at least 3 DoD Buildings (other than the Pentagon), outside of the normal working hours of 0600-2000, Monday through Friday, and/or on the weekend.

(4) 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.

(5) To be issued an NCR “A” (Armed) Badge, Security Coordinators must submit a request via PPICSS utilizing Figure 4-12.

(6) To sponsor personnel not attached to HQMC for DoD Building Badge **ONLY**, Staff Agency/Activity Security Coordinators will submit a memorandum to Pentagon Access Control Division (PACD) via DirAR (ARS), providing the name, SSN or DoD ID#, DOB, citizenship, type of investigation, reason for the visit and the duration. The memorandum, DoD Badge Agreement (refer to Figure 4-4) and the DoD Badge Acknowledgement Form (Figure 4-14) will be submitted to the HQMC Security Office via PPICSS.

b. Personnel requiring continuous access to Marine Corps Agencies/Activities aboard the Naval Support Facility Arlington (NSF-A) must have their CAC associated with the office space of the agency/activity they continuously visit or are assigned to. CAC associations are performed on Thursdays between the hours of 1000-1100. Security Coordinators must notify ARS in advance as outlined below. In the event of an emergency contact the ARS help desk, at (703) 614-3609.

(1) Submit an e-mail to the ARS organizational mailbox, SMB.HQMC.SECURITY@usmc.mil, NLT 0800 on the Thursday morning.

(2) In the subject line of the e-mail, state “NSF SWIPE ACCESS REQUEST”.

(3) In the body of the e-mail include the Full Name, e-mail Address, Building #, Room # and indicate the need for ARM/DISARM privileges for the individual requiring building access.

17. Office Space Swipe Access

a. To be granted office space swipe access at the Pentagon personnel must contact their Staff Agency/Activity Security Coordinator. The Security Coordinator will submit a PFPA Control Access Form [Identification Code (PIC)/ Personal Identification Number (PIN) Request] (refer to Figure 4-13) to the HQMC Security Section via PPICSS. Requests will normally be processed within 72 hours of receipt. E-mail confirming completion will be forwarded to the Security Coordinator.

b. To be granted office space swipe access at the NSF-A, personnel must contact their Staff Agency/Activity Security Coordinator. The Security Coordinator should follow the instructions listed under paragraph 16.b.

18. Visitor Control. For security purposes, the term “visitor” is defined as any person not assigned to or employed by HQMC. 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 building access and visitor controls apply to HQMC Staff Agencies/Activities:

a. Visitors who require access to any DoD facility, (e.g., Pentagon, Crystal City Gateway and Presidential Towers) 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:

(1) The sponsoring Staff Agency/Activity Security Coordinator will submit a memorandum to Pentagon Access Control Division (PACD), via DirAR (ARS), providing the name, SSN or DoD ID#, DOB, Citizenship, type of investigation, reason for the visit and the duration.

(2) Submit Agreement (refer to Figure 4-4) and the DoD Badge Acknowledgement Form (Figure 4-14) to the HQMC Security Office via PPICSS.

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 (5), paragraph 6.

Print Form

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

PRIVACY ACT STATEMENT

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.

DATE	CHECK ONE: ☐ INITIAL REQUEST	☐ RENEWAL	
LAST NAME	FIRST NAME	MI	
RANK/ GRADE	SSN	AGENCY	OFFICE CODE
PHONE NUMBER	**BUILDING ACCESS: CHECK ONE**	☐ FOB2 (FEDERAL OFFICE BUILDING #2)	
		☐ PENT (PENTAGON)	
		☐ NCR (NATIONAL CAPITAL REGION)	
JUSTIFICATION FOR NCR			

CONTRACTOR CAC REQUIRED:	☐ YES ☐ 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 4-1--DoD Building Pass Request

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 ☒	NO ☐	ACTIVE ☐	RESERVE ☐	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)	☐	
CLASSIFIED INFORMATION	☐	☐
NATO	☐	☐
COSMIC ATOMAL	☐	☐
ACCESS TO CLASSIFIED INFO NOT REQUIRED	☐	

☐
☐

Signature _____ (Agency Security Manager) Date _____

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

SIGNATURE: _____ (Individual Requiring Access) **DATE:** _____

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

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

_____ Level and Date _____ Basis

Signature _____ **Date:** _____
HQMC SPECIAL SECURITY OFFICERS (SSO)

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

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

Level and date: _____ **Basis:** _____

Signature: _____ **Date:** _____
(HQMC Security Manager)

PART D - (To be completed by the individual when detached or reassigned)

SECURITY DEBRIEFING 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 4-2--Classified Information Access Authorization

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, *952 and 1924, title 18, United States Code; *the provisions of section 783(b}, title 50, United States Code; and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

(Continue on reverse.)

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

STANDARD FORM 312 (Rev. 7-2013)
Prescribed by ODNI
32 CFR PART 2001.80 E.O. 13526

Figure 4-3--Classified Information Nondisclosure Agreement

Enclosure (4)

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

12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001 , section 2001 .80(d)(2)) so that I may read them at this time, if I so choose.

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

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See Notice below)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		**THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.**	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or print)*		NAME AND ADDRESS *(Type or print)*	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

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

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

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

STANDARD FORM 312 BACK (Rev. 7-2013)

Figure 4-3--Classified Information Nondisclosure Agreement-Continued

Enclosure (4)

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 the Pentagon, room 2A288A.

4. Permanent Badge holders may escort individuals inside of buildings designated as part of the Pentagon Reservation. Individuals serving as escorts may not leave their visitors unattended at any time.

5. Badges will be returned to the Security Office, room 2A288A, 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 2A288A UPON TRANSFERRING FROM THE PENTAGON RESERVATION.

MEMBER SIGNATURE_____ DATE_____

WITNESS SIGNATURE_____ DATE_____

Figure 4-4--DoD Badge Agreement

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) to the HQMC Security Office (ARS).

2. **Classified Information:** Classified information, as well as computers (including laptops) may not be removed from the DoD buildings (e.g. Pentagon) without a proper courier authorization and without proper packaging and protection. Requests for courier cards must be provided to the HQMC Security Office via the appropriate Agency/Activity Security Coordinator (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. While inside a DoD building (e.g. Pentagon), 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 Agency/Activity Coordinator 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 (e.g. STE, etc.). 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 as copiers for the purpose of copying classified information, or for the transmission of classified information.

Figure 4-5--HQMC Security Orientation/Awareness Briefing

7. **Computers:** Classified information may only be processed on approved secure computers. All approved computers and removable media 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 Coordinator. If unavailable, the security violation is to be reported to the HQMC Security Manager in **room 2A288A** of the Pentagon.

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. **Checking Out:** All personnel departing HQMC due to PCS/PCA, Terminal Leave, retirement/EAS, Transfer, etc. are required to checkout with their Agency/Activity Security Coordinator. External personnel not assigned to HQMC Agencies/Activities must checkout with the HQMC Security Office (ARS) in room 2A288A located at the Pentagon.

12. **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.

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 Defense, Central Adjudication Facility (DoD CAF).

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

15. **For Official Use Only (FOUO):** Information marked as FOUO should be destroyed by shredding or by placing in a burn bag. Official use means that only individuals with the U.S. Government are to be provided the information.

Figure 4-5--HQMC Security Orientation/Awareness Briefing-Continued

16. **Security Education Training:** Individuals are required to complete annual security training. The training is comprised of the required annual security refresher, anti-terrorism/force protection, and counter-intelligence briefs. The training is available on ARS's website listed below.

17. **HQMC/ARS/Security Website address is:**

http://www.hqmc.marines.mil/ar/Branches/SecurityProgramsandInformationManagement.aspx

Signature: _____

Witness: _____

Figure 4-5--HQMC Security Orientation/Awareness Briefing-Continued

BRIEFING/REBRIEFING/DEBRIEFING CERTIFICATE

SECTION A - GENERAL

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

SECTION B - BRIEFING

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

SECTION C - ATOMAL REBRIEFING

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

SIGNATURE AND DATE SIGNATURE AND DATE

_____
_____
_____
_____
_____

SECTION D - DEBRIEFING

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

SIGNATURE OF INDIVIDUAL: _____ DATE: _____

SIGNATURE OF CONTROL OFFICER:_____ DATE: _____

Figure 4-6--NATO Briefing Certificate

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers 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: None.
DISCLOSURE: 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
☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ 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. ORGANIZATION
3. OFFICE SYMBOL/DEPARTMENT
4. PHONE *(DSN or Commercial)*
5. OFFICIAL E-MAIL ADDRESS
6. JOB TITLE AND GRADE/RANK
7. OFFICIAL MAILING ADDRESS
8. CITIZENSHIP ☐ US ☐ FN ☐ OTHER
9. DESIGNATION OF PERSON ☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
☐ 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:
☐ AUTHORIZED ☐ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED *(Specify category)*
☐ OTHER _____

16. VERIFICATION OF NEED TO KNOW
I certify that this user requires access as requested. ☐
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, AUG 2009 PREVIOUS EDITION IS OBSOLETE. Adobe Professional 8.0

Figure 4-7--System Access Authorization Request

26. NAME *(Last, First, Middle Initial)*

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 any 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.

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 ☐ LEVEL I ☐ LEVEL II ☐ 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), AUG 2009

Figure 4-7--System Access Authorization Request-Continued

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 includesany 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

Figure 4-7--System Access Authorization Request-Continued

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 Signature

Figure 4-7--System Access Authorization Request-Continued

U.S. Marine Corps
For Official Use Only

USMC ECSD 009: NATO Information on the MCEN
Version 3.0

APPENDIX A: NATO BRIEFING and DEBRIEFING FOR ACCESS TO SIPRNET COMPUTERS

This briefing does not constitute an indoctrination to handle NATO classified material. This briefing is verifying that the user understands the responsibilities of the handling and protection of NATO information on the MCEN SIPRNet.

SECTION I – GENERAL INFORMATION

NAME: _____
(Last, First, MI)

DUTY POSITION: _____ PHONE NUMBER: _____

ORGANIZATION: _____

E-MAIL ADDRESS: _____

SECTION II - BRIEFING

I understand that I am authorized use of SIPRNet computers but I am not authorized to print or otherwise handle NATO classified material without prior authorization. I also understand that violation of this will subject me to prosecution under applicable laws and regulations.

SIGNATURE OF INDIVIDUAL: _____
DATE: _____

SIGNATURE OF SECURITY MANAGER: _____
DATE: _____

SECTION III - DEBRIEFING

I have been debriefed from this organization and no longer require use of SIPRNet computers. I certify that I have not printed or handled any NATO classified material without prior authorization. I understand that I must not disclose any other classified information that I have obtained in my assignment to this organization or in connection therewith. I also understand that I must not make any such classified information available to the public or to any person not lawfully entitled to that information. I further understand that any unauthorized disclosure of such classified information, whether public or private, intentional or unintentional, will subject me to prosecution under applicable laws.

SIGNATURE OF INDIVIDUAL: _____
DATE: _____

SIGNATURE OF SECURITY MANAGER: _____
DATE: _____

Figure 4-8--NATO Briefing Certificate

SUBSCRIBER	DEPARTMENT OF DEFENSE (DOD) PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATE OF ACCEPTANCE AND ACKNOWLEDGEMENT OF RESPONSIBILITIES

1. CERTIFICATE ACCEPTED BY

a. NAME *(Typed or printed) (Last, First, Middle Initial)*		b. UNIQUE IDENTIFICATION *(e.g., EDIPI, UID)*
c. ORGANIZATION	d. TELEPHONE NUMBER *(Include Area Code)*	e. E-MAIL ADDRESS

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. 301, Departmental Regulation; 44 U.S.C. 3101.

PRINCIPAL PURPOSE(S): To collect personal identifiers during the certification registration process, to ensure positive identification of the subscriber who signs this form.

ROUTINE USES: Information is used in the DOD PKI certificate registration process.

DISCLOSURE: Voluntary; however, failure to provide the information may result in denial of issuance of a token containing PKI private keys.

You have been authorized to receive one or more private and public key pairs and associated certificates. A private key enables you to digitally sign documents and messages and identify yourself to gain access to systems. You may have another private key to decrypt data such as encrypted messages. People and electronic systems inside and outside the DoD will use public keys associated with your private keys to verify your digital signature, or to verify your identity when you attempt to authenticate to systems, or to encrypt data sent to you. The certificates and private keys will be issued on a token, for example a Common Access Card (CAC), another hardware token, or a floppy disk. The certificates and private keys on your token are government property and may be used for official purposes only.

Acknowledgement of Responsibilities: I acknowledge receiving my PKI private keys and will comply with the following obligations:

- I will use my certificates and private keys only for official purposes;
- I will comply with the instructions described to me today for selecting a Personal Identification Number (PIN) or other required method for controlling access to my private keys and will not disclose same to anyone, leave it where it might be observed, nor write it on the token itself;
- I understand that if I receive key management (encryption/decryption) key pairs on my token, copies of the private decryption keys have been provided to the key recovery database in case they need to be recovered; and
- I will report any compromise (e.g., loss, suspected or known unauthorized use, misplacement, etc.) of my PIN or token to my supervisor, security officer, Certification Authority (CA), Registration Authority (RA), Local Registration Authority (LRA), Trusted Agent (TA), or Verifying Official (VO), immediately.

Liability: I will have no claim against the DoD arising from use of the Subscriber's certificates, the key recovery process, or a Certification Authority's (CA's) determination to terminate or revoke a certificate. The DoD is not liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by a DoD CA.

Governing Law: DoD Public Key Certificates shall be governed by the laws of the United States of America.

f. IDENTIFICATION 1		g. IDENTIFICATION 2	
(1) TYPE *(DoD ID, Passport, etc.)*	(2) NUMBER	(1) TYPE *(DoD ID, Passport, etc.)*	(2) NUMBER

h. SUBSCRIBER'S SIGNATURE *(The signature provided may be a digital signature if a good fingerprint or other adequate biometric has been collected. Otherwise the subscriber must provide a handwritten signature.)*	i. DATE SIGNED *(YYYYMMMDD)*

2. REGISTRATION OFFICIAL PER CPS

I have personally verified the identity of the person above in accordance with the applicable CPS and have personally witnessed that person sign the form.

a. NAME *(Typed or printed) (Last, First, Middle Initial)*	b. ORGANIZATION
c. TELEPHONE NUMBER *(Include Area Code)*	d. E-MAIL ADDRESS
e. REGISTRATION OFFICIAL'S SIGNATURE	f. DATE SIGNED *(YYYYMMMDD)*

DD FORM 2842, AUG 2009 PREVIOUS EDITION IS OBSOLETE. **A copy of this form shall be provided to the Subscriber.**

Adobe Professional 8.0

Figure 4-9--DoD Public Key Infrastructure (PKI) Certificate

AGREEMENT TO HANDCARRY CLASSIFIED MATERIAL

BASIC POLICY

Individual's handcarrying classified information or material, either within or outside of a command, must take every precaution to prevent the unauthorized disclosure of that information or *material.*

HAND CARRYING WITHIN A COMMAND OR IMMEDIATE ENVIRONS

1. When classified material is being carried within the command or its immediate environs as part of normal duties, an individual will take reasonable precautions to prevent inadvertent disclosure. Reasonable precautions include using a cover sheet or file folder or whatever covering is needed to protect against casual observation of the classified information. The precautions are to be taken when the movement is within a building, an elevator, or through public areas.

2. When classified material is being carried between buildings (i.e. between the Pentagon and the Naval Annex), the classified material will be double-wrapped. Use of large manila envelopes is authorized. A briefcase may be considered as a second layer.

3. When classified material being carried, is actually being transferred to another command, the requirements of DoD M-5200.1 will be followed for wrapping, addressing, receipts, etc.

AUTHORIZATION TO HANDCARRY CLASSIFIED MATERIAL IN A TRAVEL STATUS

4. Because of the inherent security risk, handcarrying of classified material while in a travel status requires that approval be granted judiciously and only when mission essential. Security Managers will authorize handcarrying only when:

a. The classified material is not available at the destination;

b. The classified material is needed urgently for a specific official purpose; and

c. There is specified reason that the material cannot be transmitted by other approved means to the destination in sufficient time for the stated purpose.

Under no circumstances will the handcarrying of classified material involving overnight stops; be authorized, unless a secure storage site at a U.S. Government activity or a cleared contractor facility has been arranged in advance.

PROTECTION DURING HANDCARRYING IN A TRAVEL STATUS

5. Before departure, a traveler authorized to handcarry classified material will be briefed as follows:

a. All classified material must be in your physical possession at all times, unless proper storage at a U.S. Government activity or appropriately cleared contractor facility (Continental U.S. only) is available. Handcarrying classified material on trips that involve an overnight stopover is not permitted without advance arrangements for proper overnight storage on a government activity or cleared contractor facility. When you surrender any package containing classified material for temporary storage (e.g. overnight or during meals) you must obtain a receipt signed by an authorized representative of the contractor facility or Government installation accepting responsibility for safeguarding the package.

b. You may not read, study, display, or use classified material in any manner on a public conveyance or in a public place.

c. When the classified material is carried in a private, public or government conveyance, you will not store it in any detachable storage compartment such as an automobile luggage rack, aircraft travel pod or drop

Figure 4-10--Agreement to Hand Carry Classified Material

tank. YOU MAY NOT LEAVE CLASSIFIED MATERIAL UNATTENDED UNDER ANY CIRCUMSTANCE.

d. A list of all classified material carried or escorted by you will be maintained by your command. UPON YOUR RETURN, YOU MUST ACCOUNT FOR ALL CLASSIFIED MATERIAL.

e. Whenever possible you should return the classified material to your command by one of the other approved methods of transmission.

6. Knowing that handcarrying is generally discouraged, contractors are frequently reluctant to allow visitors to handcarry classified material back to their duty stations. To resolve this problem, travel orders of visit requests to contractor facilities should state whether the visitor is authorized to handcarry classified material.

****UPON DETACHMENT, PCA, PCS, OR REASSIGNMENT YOU MUST RETURN YOUR COURIER CARD TO YOUR STAFF AGENCY/ACTIVITY SECURITY COORDINATOR.**

Print Name: _____

Signature: _____

Date: _____

Witness: _____

Figure 4-10--Agreement to Hand Carry Classified Material-Continued

LISTS OF ACCEPTABLE DOCUMENTS

LIST A Documents that Establish Both Identity and Employment Eligibility	OR	LIST B Documents that Establish Identity	AND	LIST C 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		
9. Unexpired Refugee Travel Document *(Form 1-571)*		9. Driver's license issued by a Canadian government authority		6. ID Card for use of Resident Citizen in the United States *(Form I-179)*
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:**		7. Unexpired employment authorization document issued by DHS *(other than those listed under List A)*
		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)

Form I-9 (Rev. 05/31/05)Y Page 3

Figure 4-11--List of Acceptable Identifications

SAMPLE MEMORANDUM TEMPLATE

MEMORANDUM FOR THE PENTAGON FORCE PROTECTION AGENCY, INVESTIGATIONS AND THREAT DIRECTORATE, OPERATIONS DIVISION

From: AGENCY, OFFICE, AND DIVISION

Subj: ARMED BUILDING ACCESS BADGE

1. First and last name is assigned to the office as the Agent, Officer, Special Agent, Director, Deputy Director, Special Agent in-Charge (provide basic summary of duties will conduct protective services, criminal investigations, counterintelligence) in, around, or on the Pentagon, Pentagon Reservation and other Department of Defense facilities. Last name requires building access on a daily basis, multiple times a week.

Name: Last, First, Middle
Title: Special Agent, Police Officer, Agent, Criminal Investigator DOB: Month/Day/Year
SSN: xxx-xx-xxxx
Clearance: TS, TS/SCI, S
Date of Clearance: Month/Day/Year
Email: xxxx.xxx@xxxx.xxx
Cell Phone: xxx-xxx-xxxx
Weapon Serial Number: xxxxxxx
Badge and Credential Number: xxxxxxx
Office Location: Pentagon, other

2. I am requesting that last name be issued an armed building pass for the Pentagon, NCR in order to have access to the Pentagon Reservation and other Department of Defense Facilities in the course of his/her duties. (If COOP required) I am requesting last name to be issued a COOP identifier in order to perform his/her duties. Last name is assigned to the (describe HRP or specific office assigned to) as the (describe specific protection or COOP required duties)

Figure 4-12--Request Issuance of NCR “A” Badge

3. Last name acknowledges he/she will turn-in or relinquish the use of the access badge if their use is not used on a frequent basis; they depart their assignment, retire, separate, move or are re-assigned.

4. The point of contact for this matter is/are Mr., Ms., Mrs. or Special Agent Xxxxx Xxxxx, xxx-xxx-xxxx, or via email xxxxxxxxx@xxxx.xxx.

_____
Name of Requester **(Leave Blank for ARS Use)**

_____
Title of Requester (**Leave Blank for ARS Use)**

Figure 4-12--Request Issuance of NCR “A” Badge-Continued

PFPA-Security Services Directorate
Alarmed Space Access Request Form

Date of Request:

A. Alarmed Space - Information

Building Name		Building cont.		System	
Agency		Zone(s)# requested			
Room(s)# requested		Room(s)# requested Cont.			
Room/Zone Contact telephone #		Room/Zone alternate telephone #			
Security Manager (SM)		SM phone #			
Alternate Security Manager (ASM)		ASM phone #			
*NOTE: Room/Zone contact # is a phone that rings within the protected area					

B. Alarmed Space - Duty/Operating Hours
Modified/Changed/Updated? Yes ☐ No☐

Monday Open-Close	Tuesday Open-Close	Wednesday Open-Close	Thursday Open-Close	Friday Open-Close	Saturday Open-Close	Sunday Open-Close	Holiday Open-Close

C. Emergency Points of Contact (During Duty and Non-Duty Hours)
Modified/Changed/Updated? Yes ☐ No☐

Add	Del	Name (Last, First MI)	SSN	Home Telephone/ Work Telephone
☐	☐			
☐	☐			
☐	☐			
☐	☐			
☐	☐			

D. Personnel Authorization

JS (Please place an (x) in box, if the person already has JS access rights)
ADD = Add this person DEL = Delete this person PIC = issue a PIC number ACS = Grant swipe access

Add	Del	PIN	PIC	ACS	Name (Last, First MI)	SSN	Home or Work phone	JS
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐
☐	☐	☐	☐	☐				☐

Privacy Act Statement:
Title 5 U.S.C. 6311 and Executive Order 9397. Information contained in this correspondence may be subject to the Privacy Act of 1974 (5 U.S.C. 552a). Personal information contained in this correspondence may be used only by authorized persons in the conduct of official business. Any unauthorized disclosure or misuse of personal information may result in criminal and/or civil penalties. If you are not the intended recipient of this correspondence please destroy all copies of this correspondence after notifying the sender of your receipt of it.
Furnishing requested information is voluntary, but failure to do so may delay or prevent action on the application.

Figure 4-13--Alarmed Space Access Request Form

DoD Badge Acknowledgement Form

PRIVACY ACT STATEMENT

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

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

PRINCIPAL PURPOSE: Information collected by this form will be used to issue a DoD building pass or Visitor "No Escort Required" building pass to eligible persons.

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

ROUTINE USES: None other than the blanket routine uses established by the Department of Defense Privacy Office and posted at ***http://www.defenselink.mil/privacy/notices/blanket-uses.html***.

DISCLOSURE: Providing information on this form is voluntary. However, failure to provide may result in you not being issued a DoD building pass or "No Escort Required" building pass.

Principal Purpose

To ensure that Department of Defense (DoD) and non-DoD personnel are informed of the Headquarters U.S. Marine Corps (HQMC) eligibility requirements and conditions associated with issuance of a DoD Building Pass and Visitor, No Escort Required Building Pass to gain access to the Pentagon and Pentagon Reservation under HQMC sponsorship.

General

In accordance with DoD Administrative Instruction 30 (Force Protection of the Pentagon Reservation), you are being issued a DoD Building Pass or Visitor, No Escort Required Building Pass, for access to the Pentagon and Pentagon Reservation because an appropriate HQMC Staff Agency/Activity has chosen to sponsor you for access. In accepting this DoD Building Pass or

Figure 4-14--DoD Badge Acknowledgement Form

Visitor, No Escort Required Building Pass, your signature on this document indicates your understanding that you have been granted access to the Pentagon and Pentagon Reservation for the sole purposes of conducting, participating in, or facilitating official U.S. Government business.

Misuse

Using your DoD Building Pass or Visitor, No Escort Required Building Pass to gain access to the Pentagon, the Pentagon Reservation or any part thereof and to engage in activities outside the scope of the official business for which your access was granted, is grounds for the immediate removal of your building pass, withdrawal of HQMC sponsorship of your visitor access and denial of continued and future access to the Pentagon and Pentagon Reservation.

Control

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

Acknowledgement

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

_____/_____

Signature Date

Figure 4-14--DoD Badge Acknowledgement Form-Continued

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 requirements must be met:

a. All personnel who conduct derivative classification by means of reproducing, extracting, or summarization of classified information, or who apply classification markings derived from source material, or as directed by classification guide shall:

(1) Be identified by name and position or by personal identifier on the “Classified By” line, in a manner that is immediately apparent for each derivative classification performed.

(2) Observe and respect original classification decisions.

(3) Carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(a) The date or event for declassification that corresponds to the longest period of classification among the sources.

(b) A listing of the source materials.

(4) Receive training in the proper application of the derivative classification principles, with an emphasis on avoiding over classification, at least once out of every 2 years. Derivative classifiers who do not receive such training at least one out of every 2 years shall have their authority to apply derivative classification marking suspended until they have received such training. A waiver may be granted by the staff Agency/Activity Head or Deputy Head if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable. The

Derivative Classification Training can be accessed at the Center for the Development of Security Excellence at the following link: https://stepp.dss.mil/SelfRegistration/Login.aspx.

b. 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 identify 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.

c. 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. Examples of such media include, but are not limited to, CD, DVD, Tape, removable hard-disk-drives, 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) Top Secret Information: All Top Secret information, including copies originated or received by HQMC shall be continuously accounted for, individually serialized, and entered into the Classified Document Control Section of PPICSS. 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 (ARS) 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 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 the conditions required by this SOP. Approval will be granted 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 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. The room perimeter is protected 24 hours a day, 7 days a week by access control devices. Personnel must ensure that all external doors of this room shall remain closed at all times.

(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, 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 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 workers present. Escorts should alert fellow workers announcing their presence when visitors or workers 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.

d. NATO Information. Per references (b) and (d), the following policies and procedures will be followed for the proper handling and safeguarding of NATO material:

(1) Access. Staff Agency/Activity Security Coordinators shall ensure a proper security clearance is held prior to requesting NATO access. For access to NATO classified material, a final security clearance at the same level is required (e.g., Cosmic Top Secret requires Final U.S. Top Secret). All requests for access will be submitted to the HQMC Security Manager for approval. Security Coordinators will conduct briefings and debriefings as required and will be documented on Figure 4-6.

(2) Distribution. NATO Secret documents will be distributed from the Central United States Registry (CUSR) to the Marine Corps Sub-registry to the HQMC Control Point via SIPRNet. Staff Agency/Activity inventory of NATO classified material is managed by HQMC Control Point (ARS) who will perform and report inventories as required to the Sub-registry. No one shall send NATO classified material directly to individuals

and/or outside activities. All incoming and outgoing delivery of NATO material will be completed via the HQMC, Control Point located at:

3000 Marine Corps Pentagon
Room 2A288A
Washington, DC 20350-3000

(3) Handling. NATO classified messages will be handled in the same manner as NATO material of the same classification. Authority to hand-carry any NATO classified material within the NCR, CONUS and OCONUS, must be approved by the HQMC Security Manager. NATO Restricted is similar in relation to For Official Use Only (FOUO) or Controlled Unclassified Information (CUI). NATO Restricted will be controlled in a manner that would prevent unauthorized disclosure but is not held to the same requirements as NATO Secret or NATO COSMIC TOP SECRET.

(4) Safeguarding. Staff Agencies/Activities will maintain a roster of personnel authorized access to NATO material. Place the roster visibly upon entry of the area. Reproduction of NATO material is not authorized without prior approval of the HQMC Security Manager. Extracts of NATO material must be clearly identified with the orginiating documents safeguards. NATO Classified material will be stored in containers approved for the storage of equivalent U.S. material. NATO material may be stored in the same container but must be filed separately from U.S. material.

(5) Destruction. All NATO classified material will be destroyed by the HQMC Control Point (ARS). NATO classified information will be destroyed using the same methods as U.S. classified information, (e.g., crosscut shredding, burning, pulverizing). All destruction of NATO classified material will be afforded two-person integrity (TPI) by appropriately cleared personnel, at the same level of the information to be destroyed. The NATO Classified Material Control Form & Destruction Report will be utilized to document destruction and will be forwarded to the Marine Corps Sub-Registry (PP&O PS).

3. Reproduction of Classified Information

a. In accordance with reference (b), reproduction of classified material (e.g. paper copies, electronic files, and other materials) shall only be conducted as necessary to

accomplish the staff agency/activity mission or to comply with applicable statutes or directives.

b. Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced, including e-mailing, scanning and copying, to the extent operational needs require.

c. Staff agencies/activities shall establish procedures that facilitate oversight and control of the reproduction of classified information and the use of equipment for such reproduction, including controls that ensure:

(1) Reproduction is kept to a minimum consistent with mission requirements.

(2) Personnel reproducing classified information are knowledgeable of the procedures for classified reproduction, are aware of the risks involved with the specific reproduction equipment being used, and of appropriate countermeasures that are required to be taken.

(3) Reproduction limitations, special controls and special categories of information are fully and carefully observed.

(4) Reproduced material is placed under the same accountability and control requirements that are applied to the original material. Extracts of documents will be marked according to content and may be treated as working papers if appropriate.

(5) Reproduced material is conspicuously identified as classified at the applicable level and copies of classified material are reviewed after the reproduction process to ensure that the required markings exist.

(6) Waste products generated during reproduction are protected or destroyed as required.

(7) Classified material is reproduced only on approved and, when applicable, properly accredited systems.

(8) Foreign government information (FGI) is reproduced and controlled pursuant to guidance and authority granted by the originating government.

d. Reproduction equipment approved and designated for processing classified information to include copiers; facsimile machines; computers, and other IT equipment, and peripherals; display systems, and electronic typewriters, shall be identified with the proper classification level of the information being processed. Staff agencies/activities security procedures shall prescribe the appropriate safeguards to:

(1) Ensure equipment repair procedures do not result in unauthorized dissemination of, or access to classified information.

(2) Replace and destroy equipment parts in the appropriate manner when classified information cannot be removed. The products list that meets National Security Agency (NSA) performance requirements for sanitizing, destroying, or disposing of equipment containing sensitive or classified information is available at: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

(3) Ensure that appropriately cleared and knowledgeable personnel inspect equipment and associated media before the equipment is removed from the protected area.

(4) Ensure classification markings and labels are removed from sanitized equipment and media after inspection and prior to removal from the protected area.

4. Annual Review of Classified Material Holdings

a. All Staff Agencies who possess classified material must complete an annual review of classified material and report compliance to HQMC Security Manager no later than 1 December of the current year per reference (b). The purpose of this mandatory review of classified holdings is to reduce the inventory of classified documents to “what is absolutely essential.” This tasking can be satisfied during your annual “Clean Out” day.

b. All Staff Agencies/Activities must continually strive to reduce the amount of classified material on-hand. This active reduction effort will concurrently reduce the potential of security violations. Moreover, it will decrease the amount of man-hours required to maintain classified holding.

c. As directed by the HQMC Continuity Of Operations Plan (COOP) Order, all Staff Agencies are required on an annual basis to review classified holdings held at the Alternate Headquarters.

d. Report compliance to the HQMC Security Manager via the organizational mail box at SMB.HQMC.SECURITY@USMC.MIL, stating that the staff agency "clean out" has been completed. Documentation of this completion will be reviewed during the Security Assessment Program.

5. Dissemination

a. Classified information originating in another DoD Component or in a department or agency other than the Department of Defense may be disseminated to other DoD Components, to other U.S. departments or agencies, or to a U.S. entity without the consent of the originating Component, department, or agency, as long as:

(1) The criteria for access as outlined in enclosure (4) are met.

(2) The classified information is NOT marked as requiring prior authorization for dissemination to another department or agency. The marking Originator Consent "ORCON" may be used to identify information requiring prior authorization for dissemination to another department or agency.

(3) The document was created ON or AFTER 27 June 2010, the effective date of Part 2001 of Title 32, Code of Federal Regulations.

b. Documents created BEFORE 27 June 2010 may not be disseminated outside of the Department of Defense without the originator's consent. Additionally, documents created on or **after** 27 June 2010, whose classification is derived from documents created prior to that date, and where the date **before** 27 June 2010 of the classified source(s) is readily apparent

from the source list, shall not be disseminated outside of the Department of Defense without the originator's consent.

c. Classified information originating in, or provided to or by, the Department of Defense may be disseminated to a foreign government or an international organization of governments, or any element thereof, pursuant to Executive Order (EO) 13526, "Classified National Security Information", Part 2001 of Title 32, Code Federal Regulations, and DoD Directive 5230.11, "Disclosure of Classified Information to Foreign Governments and International Organizations".

d. Dissemination of classified information to state, local, tribal and private sector officials pursuant to EO 13549 "Classified National Security Information Program for State, Local, Tribal and Private Sector Entities" shall be in accordance with implementing guidance issued by the Department of Homeland Security.

6. Foreign Disclosure

a. While public domain information, authorized and approved by the HQMC Public Affairs Office, can be freely shared with foreign governments and interest, classified information 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 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 Coordinators 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 identified within the receiving agency. Identify the expected level of CMI or CUI to be disclosed or released in conjunction with the visit. Conduct verification of identification (ID) 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.

7. Security Review of DoD Information Intended for Public Release of DoD Information

a. Reference (j) directs the Security Programs and Information Management Branch (ARS) to maintain liaison with the HQMC Public Affairs Office (PAO) to ensure that proposed press releases and information intended for public release are subjected to a security review.

b. DoD Directive 5230.9 “Clearance of DoD Information for Pubic Relaease”, requires that a security and policy review be performed on all official DoD information intended for public release that pertains to military matters, national security issues, subjects of significant concern to the Department of Defense and information intended for placement on publicly accessible websites or computer servers. Documents proposed for public release shall first be reviewed at the Staff Agency/Activity levels as required by SECNAVINST 5720.44B “Public Affairs Policy and Regulation” and may or may not be found suitable for public release without higher level consideration.

c. The following actions will be taken before the release of DoD information to the public:

(1) Staff Agencies/Activities are authorized to release information to the public that is entirely within the staff agnecy/activity misson and scope. Each staff agency/activity is responsible for ensuring that a review of material proposed for public release is completed.

(2) Once the staff agency/activity has indentified information to be released to the public, that information must be forwarded to the Director, Public Affairs Division, Media Branch for review. This review is part of an overall public release process and is coordinated by ARS in consultation with command subject matter experts.

8. 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 mail will be done through the HQMC Security Section. The following guidelines will be followed when dropping off items to be mailed:

(1) Envelopes with address labels (not affixed to the envelope) for the organization and the recipient.

(2) Recipient 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 Coordinators will ensure that all personnel are aware of this prohibition.

(5) All incoming registered mail must be sent to the following address: COMMANDANT OF THE MARINE CORPS HQMC (CODE ARS) 3000 Marine Corps Pentagon, Room 2A288A, Washington, DC 20350-3000

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

(7) Further guidance can be obtained by contacting the ARS Information Security Specialist at (703) 614-3609.

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 FAX equipment located within HQMC.

c. Hand-Carry

(1) Appropriately cleared and briefed personnel may be authorized to escort or carry classified information between locations when other means of transmission or transportation cannot be used. Staff Agencies/Activities shall establish procedures to ensure that hand-carrying of classified material is minimized to the greatest extent possible and does not pose an unacceptable risk to the information.

(2) All personnel that courier COMSEC material and equipment must be designated in writing and receive specific written instructions for the safeguarding of the COMSEC material and equipment entrusted to them. Further, courier personnel must also comply with the storage, safeguarding, transmission and transportation requirements. Contact the HQMC EKMS manager for additional instructions for the transporting of COMSEC material.

(3) Classified material may not be removed from the Pentagon, NSF, and Marsh Center without a proper courier card and without proper packing and protection. Furthermore, no material may be carried outside of an office space unless it is properly covered and safeguarded, per the daily control measures outlined in this SOP.

(4) Hand-carrying may be authorized only when:

(a) The information is not available at the destination and operational necessity or a contractual requirement requires it.

(b) The information cannot be sent via a secure e-mail, facsimile transmission or other secure means.

(c) The appropriate official authorizes the hand-carry according to procedures the Head of the DoD component establishes.

(d) The hand-carry is accomplished aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available, and the U.S. escort retains custody and physical control of the information at all times.

(e) Arrangements have been made for secure storage of the information at a U.S. Government or cleared U.S. contractor facility.

(5) Requests for a Courier Authorization Card (DD Form 2501) (military and civilian) and Courier Letter (DoD Contractor) are submitted through the Staff Agency/Activity Security Coordinator to the HQMC Security Branch (ARS). Security Coordinators will verify security clearance information using JPAS prior to submission of the request. The DD Form 2501 will be issued for no more than 2 years at a time and the courier letter will be issued to contactor personnel for no more than one year. The requirement for authorization to hand-carry classified information shall be reevaluated and/or revalidated once every 2 years, and a new form issued, if appropriate. Authorization to hand-carry Compartmented Information (SCI) and Special Access Programs (SAP) information must be routed through Special Security Office (SSO) for approval.

(6) All personnel authorized to hand-carry classified material must read and sign the “Agreement to Hand-Carry Classified Material” (Figure 4-10). By signing the agreement personnel will acknowledge the following responsibilities:

(a) Liable and responsible for the material being carried or escorted.

(b) The material is not, under any circumstances, to be left unattended. During overnight stops arrangements shall be made for storage of the classified material at a U.S. military facility, embassy, or cleared contractor facility. Classified information shall not be stored in hotel safes.

(c) The material shall not be opened en route except in the circumstances described in reference (b) paragraph 11.d of volume 3, enclosure (4).

(d) The material shall not be discussed or disclosed in any public place.

(e) The individual shall not deviate from the authorized travel schedule.

(f) In cases of emergency, the individual shall take measures to protect the material.

(7) Preparation of Material. When transferring classified information, it shall be enclosed in two opaque, sealed envelopes, wrappings, or containers, durable enough to properly protect the material from accidental exposure and facilitate detection of tampering. A briefcase may be used as the outer wrapping except when traveling via commercial airline.

(a) Prepare, package, and securely seal classified material in ways that minimize risk of accidental exposure or undetected deliberate compromise. To minimize the risk of exposure of classified information, package documents so that classified material is not in direct contact with the inner envelope or container (e.g., fold so classified material faces together).

1. Address the outer envelope or container to an official U.S. Government activity or to a DoD contractor with a facility clearance and appropriate storage capability and show the complete return address of the sender. **DO NOT** address the outer envelope to an individual. Office codes or phrases such as “Attention: Research Department” **WILL NOT** be used.

2. Show the address of the receiving activity, the address of the sender, the highest classification of the contents (including, where appropriate, any special dissemination or control markings such as “Restricted Data” or “NATO”), and any applicable special instructions on the inner envelope or container. The inner envelope may have an attention line with a person’s name.

3. Do not place a classification marking or any other unusual marks on the outer envelope or container that might invite special attention to the fact that the contents are classified.

4. Address classified information intended only for U.S. elements of international staffs or other organizations specifically to those elements.

(b) When classified material is hand-carried outside an activity, a locked briefcase or zippered pouch may serve as the outer wrapper.

(8) Hand-Carrying or Escorting Classified Information on Commercial Aircraft. Although pre-coordination is not typically required, in unusual situations advance coordination with the local Transportation Security Administration (TSA) field office may be warranted to facilitate clearance through airline screening processes.

(a) The individual designated as a courier shall possess a DoD or contractor-issued identification card and a government-issued photo identification card. (If at least one of the identification cards does not contain date of birth, height, weight, and signature, include these items in the written authorization.)

(b) The courier shall have a courier authorization letter prepared on letterhead stationary signed by the HQMC Security Manager, authorizing the carrying of classified material, which shall:

1. Give the full name of the individual and his or her employing agency or company.

2. Carry date of issuance and an expiration date.

3. Give the name, title, signature, and phone number of the official issuing the letter.

4. Carry the name of the person and official U.S. Government telephone number of the person designated to confirm the courier authorization.

(c) The courier shall go through the same airline ticketing and boarding process as other passengers. Upon arrival at the screening checkpoint the individual designated as courier shall ask to speak to the TSA Supervisory Transportation Security Officer and shall present the required identification and authorization documents. **If the courier does not present all required documents, including valid courier authorization, DoD or contractor-issued identification card, and government-issued photo identification card, TSA officials will require the classified material to be screened in accordance with their standard procedures.** TSA personnel may insist the courier bag be opened to physically verify its contents. The courier will request to speak to the supervisor and be taken to a private

screening area where the cover sheet of the contents therein can be verified. Only the U.S. Government classified material is exempted from any form of inspection; the courier and all of the courier's personal property shall be provided for screening. The classified material shall remain within the courier's sight at all times during the screening process.

(d) Hand-carrying items aboard international commercial aircraft shall be done only on an exception basis. DoD travelers requiring access to classified materials at an overseas location shall exhaust all other transmission options (e.g., electronic file transfer, advance shipment by courier) before hand-carrying items aboard international commercial aircraft. Reference (b), paragraph 11.d, provides further guidance regarding hand-carry classified information aboard international commercial aircraft. In addition to the requirements in this subparagraph, for international travel the authorization letter shall describe the material being carried [e.g., "three sealed packages (9" x 8" x 24")," addressee and sender] and the official who signed the authorization letter shall sign each package or carton to be exempt to facilitate its identification.

d. Write-to-Media. The use of removable media on the SIPRNet is of great concern. "WRITE" privileges (downloading) to all forms of removable media have been banned at HQMC, except through an approved waiver. Removable media is defined as CD, DVD, Tape, removable hard-disk-drive, etc. Staff agencies /activities requiring SIPRNet "write-to" removable media capability must submit a waiver request.

(1) Personnel requesting a waiver for "write-to" removable media capability must complete the following:

(a) The director or head of the staff agency /activity shall utilize Figure 5-1, for submission to the Head, Security Programs and Information Management Branch (ARS), those individuals authorized to perform "write-to" removable media.

(b) Content Locator, Examination, Analysis, and Reporting (CLEAR) Tool Data Transfer Training located at: https://dodiisclear.dia.mil/Navy_Clear_Short/launchPage.htm.

(c) The “Write-to Removable Media Exemption Request” form (refer to Figure 5-2), for each individual who will have access to the capability.

(d) Security Coordinators will submit items (a) through (c) to: SMB.HQMC.SECURITY@usmc.mil.

(2) When using this capability, the authorized user must follow the procedures as outlined below:

(a) Two Person Integrity (TPI) will be accomplished during the initial “write” and “accountability” process. Authorized users will obtain a witness to physically view the write-to-media action and entry of the media record into the CDCC portal. A witness is defined as any individual who is cleared to the same level of the classified information and possesses a valid need-to-know.

(b) Label the media prior to writing, with the highest classification of the material to be written.

(c) Document media in the Classified Document Control Section of PPICSS.

(d) Download/Copy the information to the media.

(e) Specific instructions for the handling, storage, transportation and destruction of the media shall be accomplished in the same manner as required for classified information at the same level as outlined in reference (b) and this SOP.

9. 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 5-3) 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).**

d. Classified notes, 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 5-4) 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 701s and 702s may be destroyed 30 days after the last entry unless they are used to support an ongoing investigation.

10. Storage

a. Classified information shall be secured under conditions adequate to deter and detect access by unauthorized persons. Classified information not under the personal control and observation of an authorized person shall be locked in a General Services Administration (GSA) approved security container with metal tag affixed, vault or open storage area or a secure room.

b. There shall be no external mark revealing the level of classified information authorized to be or actually stored in a given container or vault, or indicating the priority assigned to the container for emergency evacuation and destruction. This does not preclude placing a mark or symbol (e.g., a bar code) on the container for other purposes (e.g., identification and/or inventory purposes) or from applying decals or stickers the DNI requires for containers and equipment used to store or process intelligence information. If a GSA container or vault door recertification is required, such labels and markings must be removed, but may be reapplied as needed after recertification.

c. The requirements specified by reference (b) represent acceptable security standards. Do not store weapons or items such as funds, jewels, precious metals, or drugs in the same container used to safeguard classified information. Additionally, placing items on top of the security container is prohibited.

d. **Top Secret** information shall be stored under one or more of the following conditions:

(1) In a GSA-approved security container with one of the following supplementary controls:

(a) An employee cleared to at least the Secret level shall inspect the security container once every 2 hours.

(b) The location that houses the security container is protected by an intrusion detection system (IDS) with a personnel response time of no more than 15 minutes from the alarm annunciation.

(2) In a GSA-approved security container equipped with a lock meeting Federal Specification FF-L-2740 (Locks, Combination, Electromechanical), provided the container is located within an area that has been determined to have security-in-depth as defined by reference (b).

(3) In an open storage area (also called a secure room) constructed according to reference (b) physical security standards and equipped with an IDS with the personnel responding to an alarm within 15 minutes of the alarm annunciation if the area has been determined to have security-in-depth. Without a security-in-depth determination, personnel response time must occur within 5 minutes of alarm annunciation.

(4) In a vault, or GSA-approved modular vault, meeting the requirements of Federal Standard (FED-STD) 832 and the physical security standards outlined in reference (b).

e. **Secret** information shall be stored by one of the following methods:

(1) In the same manner as prescribed for Top Secret information.

(2) In a GSA-approved security container or vault built to FED-STD 832 specifications, without supplementary controls.

(3) In an open storage area meeting the requirements of reference (b), provided DirAR (ARS) has determined in writing that security-in-depth exists, and one of the following supplemental controls is utilized:

(a) An employee cleared to at least the Secret level shall inspect the open storage area once every 4 hours.

(b) An IDS meeting the requirements of reference (b) with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

f. **Confidential** information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

g. Security Container Information. Staff Agency/Activity Security Coordinators will maintain a record for each security container, or vault or secure room door, used for storing classified information. Security Coordinators will ensure the following takes place:

(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, unless other sufficient controls exist to prevent that individual's access to the lock or when the combination has been subjected to compromise.

(3) Use Security Container Information (SF 700) (refer to Figure 5-5) 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 SF 700 is not classified, but contains personally identifiable information (PII) that shall be protected by sealing Part 1 in an opaque envelope (not provided as part of the SF 700) conspicuously marked "Security Container Information" and stored in accordance with SF 700 instructions. If the information must be accessed during non-duty hours and a new opaque envelope is not available to replace the opened one, the original envelope should be temporarily resealed, to the extent possible, until Part 1 can be placed in a new envelope the next working day.

(5) Part 2 of SF 700, when completed, is classified at the highest level of classification authorized for storage in the security container. It shall be sealed and stored in accordance with SF 700 instructions. The classification authority block shall state “Derived From: 32 CFR 2001.80(d)(3),” with declassification upon change of combination.

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

h. Access Rosters

(1) Access rosters that identify those persons authorized to enter a controlled access area in the performance of their duties will be signed by the Staff Agency/Activity Deputy Commandant/Director or By Direction Authority. Rosters will be posted on the interior wall of a designated space adjacent to the main entry point and will not be visible from the exterior.

(2) Unaccompanied access rosters identify those persons authorized to enter a controlled access area in the performance of their duties. Unaccompanied access is limited to persons for essential operations and requires those persons to be cleared and/or screened prior to access being granted. These rosters will be signed by the Staff Agency/Activity Deputy Commandant /Director or By Direction Authority of the functional area. Rosters will be posted on the interior wall of a designated space adjacent to the main entry point and will not be visible from the exterior.

11. Destruction. Classified documents and material identified for destruction shall be destroyed completely, to prevent anyone from reconstructing the classified information, according to procedures and methods the DoD Component Head prescribes. Methods and equipment used to routinely destroy classified information include burning, crosscut shredding, wet pulping, mutilation, chemical decomposition or pulverizing. Methods used for clearing, sanitization or destruction of classified IT equipment and media include overwriting, degaussing, sanding, and physical destruction of components or media.

a. Documents and other material identified for destruction shall continue to be protected as appropriate for their classification until actually destroyed.

b. Staff Agencies/Activities with classified holdings shall establish at least 1 day each year when specific attention and effort is focused on disposing of unneeded classified material ("clean-out day"). Staff Agencies/Activities will report compliance to the HQMC Security Manager via the organizational mailbox at SMB.HQMC.SECURITY@USMC.MIL, stating that the "clean out" has been completed.

c. Effective 1 January 2011, only equipment listed on an evaluated products list (EPL) issued by NSA may be used to destroy classified material. EPLs currently exist for paper shredders, punched tape destruction devices, optical media destruction devices [for compact discs (CDs) and digital video discs (DVDs)], degaussers (for magnetic media sanitization), and disintegrators (for paper and punched tape material).
The EPLs may be obtained by calling (410) 854-6358, or at: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

(1) Equipment approved for use prior to 1 January 2011, and not found on the appropriate EPL may be used for destruction of classified information until 31 December 2016.

(2) Unless determined otherwise by NSA, whenever an EPL is revised, equipment removed from the EPL may be utilized for destruction of classified information for up to 6 years from the date of its removal from the EPL.

(3) In all cases, if any such previously approved equipment needs to be replaced or otherwise requires a rebuild or replacement of a critical assembly (e.g., shredder blade assembly), the unit must be replaced with one listed on the appropriate EPL.

d. Destruction Procedures. Staff Agencies/Activities shall establish procedures to ensure that all classified information intended for destruction is destroyed by authorized means and appropriately cleared personnel.

(1) Classified information that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to a designated record center.

(2) Classified information shall be controlled in a manner designed to minimize the possibility of unauthorized removal and/or access. A burn bag may be used to store classified information awaiting destruction at a central destruction facility. Seal and safeguard each burn bag per this SOP until actually destroyed.

(3) Records of destruction are not required for Secret and Confidential information except for special types of classified information (see paragraph 17.c) of reference (b). For Top Secret the following procedures will be followed:

(a) Use OPNAV 5511/12, “Classified Material Destruction Report”. Refer to Figure 5-6.

(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 (ARS).

e. Burn Bag Disposal. Burn bags shall be safeguarded in accordance to the classification level of the information contained. Burn bag destruction at the Pentagon is held Monday through Friday from 0800-0900 and again from 1100-1200. Burn Bags shall be brought to the Remote Delivery Facility (RDF) located in the basement of Corridor 6. Burn bag destruction at the NSF-A is held every Thursday from 0815-0825. Burn bags shall be brought to NSF-A, Building #12 loading dock. A burn bag receipt Figure 5-7 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.

12. Hosting Classified Meetings. Meetings and conferences involving classified information present special vulnerabilities to unauthorized disclosure. The Heads of the DoD components shall establish specific requirements for protecting classified information at DoD Component-sponsored meetings and conferences, to include seminars, exhibits, symposia, conventions, training classes, workshops, or other such gatherings, during which classified information is disseminated.

a. Staff Agencies/Activities hosting a classified meeting in support of a conference, seminar or working group are required to utilize spaces within DoD cleared facilities whenever possible. The use of these cleared spaces helps reduce the risk associated with classified sessions such as, unauthorized disclosure, or loss or compromise of classified information. The guidance below is provided to aid those responsible for the coordination of such meetings and provides instruction for such cases when DoD facilities are inadequate or unavailable.

b. The term “visitor” is defined as any person not permanently attached to the hosting command. The Joint Personnel Adjudication System (JPAS) is the application used for Visitor Requests.

(1) All visiting personnel who are scheduled to attend a HQMC sponsored classified meeting or conference, must have command sponsored visit requests submitted through JPAS to the HQMC Security Management Office (SMO) Code: 540080084.

(2) Visit requests must list a start and end date, POC for the meeting and reason for visit. Prior to gaining access

into the meeting, visit requests will be verified in JPAS by the hosting agency/activity.

(3) In situations where meetings or conferences will contain both classified and unclassified briefs, there must be a distinct separation between the two. Those individuals that do not possess the proper clearance level must be removed from the briefing before discussion of any classified information is conducted. The briefer must be aware of the specific time each classified period will begin.

(4) Ensure that attendance is limited to U.S. Government personnel and/or cleared DoD contractor employees. Any participation by foreign nationals or foreign representatives shall be approved, in writing, by the HQMC Foreign Disclosure Officer prior to attendance to ensure that the information to be presented has been cleared for foreign disclosure. The HQMC Foreign Disclosure Officer [Plans, Policy and Operations (PP&O)] can be reached at (703) 614-4342.

c. Notes taken during classified sessions must be treated as classified information and protected as outlined in the references. Note taking should be restricted during the classified portions of the brief. Individuals attending the brief, who wish to obtain the classified portion, may contact the briefer and request the information be sent via SIPRNet, mailed or faxed via secure means. If note taking is allowed, these working papers must be dated and marked at the top and bottom with the overall classification of the information and destroyed or converted into a final product within 180 days.

d. A security brief is often recommended at the beginning of each meeting day to remind those in attendance of their individual responsibilities to protect classified information which includes:

(1) No discussions of classified information disclosed at the meeting, in any area not designated at the same level of the information to be discussed.

(2) Ensure attendees do not allow personnel through the door if not recognized and no perimeter guard is present.

(3) All non-government issued electronic devices must be powered off and stored externally during classified briefings.

(4) After any classified session, personnel hosting the meeting will ensure that the area has been thoroughly searched to prevent classified material from being left in the room. Burn bags should be available in cases where classified information is discovered, to ensure proper disposal.

(5) An information package should be provided to each participant before the brief commences, to inform individuals of Department of the Navy and Commandant of the Marine Corps security policies and procedures.

e. Handling, Safeguarding and Storage

(1) Discourage briefers from hand carrying media for the brief. Instead, encourage them to send all briefs via SIPRNet or mailing. If someone must hand carry classified information, coordinate with the briefer for storage of the material once he/she has arrived. Stress that no information is to be left in automobiles or hotels and ensure courier authorization has been issued in card or letter form by the command Security Manager.

(2) Distribution of classified material is discouraged. If briefs or media will be handed out to participants, these items must be numbered (1 of xx) and collected upon the conclusion of the classified portion. Classified information should be distributed over the SIPRNet whenever possible.

(3) Classified information moving throughout a DoD cleared facility must bear a Standard Form cover sheet, (e.g., SF 703 Top Secret, 704 Secret, 705 Confidential). If leaving the DoD cleared facility, the information must be double wrapped and courier authorization must be carried at all times. Further guidance on the proper procedures to safeguard and transport classified information is outlined in reference (b) and paragraph 8c of this SOP.

f. Classified Meetings in Non-DoD Facilities

(1) Staff Agencies/Activities that have exhausted every means of hosting the meeting/conference at a U.S. Government agency or cleared DoD contractor facility which are subsequently unavailable or are unable to support specific requirements of the meeting/conference, may request a waiver to host the meeting/conference at a non-DoD facility.

(2) Staff Agencies/Activities requesting to host a meeting/conference at a non-DoD facility must receive prior approval from the Under Secretary of Defense for Intelligence [USD(I)]via the Director, Administration and Resource Management Division, (ARS) and the Deputy Commandant, Plans, Policies and Operations, (PS). Requests must be made at least **60 days** prior to any commitment or announcement of the event.

(3) Requests to conduct such meetings must include a detailed security plan as outlined in Figure 5-8. Due to the special classified nature of the request, **Staff Agencies/ Activities must coordinate with ARS** for additional security related guidance not mentioned in this SOP. Failure to comply with the provisions of this SOP will result in the denial of the request. Requests to conduct such classified meetings shall be addressed following the exmple found in Figure 5-9.

13. Compromise and Other Security Violations. Protection of classified information is essential to maintaining security and achieving mission success at HQMC. Prompt reporting of security incidents ensure that such incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of an actual loss or unauthorized disclosure of classified information and to preclude recurrence through an informed, properly tailored, and up-to-date security education and awareness program. In cases where compromise has been ruled out and there is no adverse effect on national security, a common sense approach to the early resolution of an incident at the lowest appropriate level is encouraged. All security incidents involving classified information shall involve a security inquiry, a security investigation, or both.

a. The terms associated with security incidents are:

(1) Infraction. An infraction is a security incident involving failure to comply with requirements [i.e., the provisions of EO 13526, Part 2001 of title 32, CFR, reference (b), this SOP or other applicable security policy] which cannot be reasonably expected to, and does not, result in the loss, suspected compromise, or compromise of classified information. An infraction may be unintentional or inadvertent. While it does not constitute a security violation, if left uncorrected, can lead to security violations or compromises. It requires an inquiry to facilitate immediate corrective action but does not require an in-depth investigation.

(2) Violation. Violations are security incidents that indicate knowing, willful, and negligent for security regulations, and result in, or could be expected to result in, the loss or compromise of classified information. Security violations require an inquiry and/or investigation.

(a) Compromise. A compromise is a security incident (more specifically, a violation) in which there is an unauthorized disclosure of classified information [i.e., disclosure to a person(s) who does not have a valid clearance, authorized access, or a need to know].

(b) Loss. A loss occurs when classified information cannot be physically located or accounted for (e.g., classified information/equipment is discovered missing during an audit and cannot be immediately located).

(3) Inquiry. An inquiry is fact-finding and analysis conducted to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had, or could have had, access to the information. The inquiry identifies the facts, characterizes the incident as an infraction or a violation, identifies if possible the cause(s) and person(s) responsible, reports corrective actions taken or to be taken, and makes recommendations as to the need for further corrective action or a more in-depth investigation. Generally, inquiries are initiated and conducted at the lowest echelon possible within the DoD Component.

(4) Investigation. An investigation is conducted for a security violation when the incident cannot be resolved via inquiry or for incidents where an in-depth and comprehensive examination of the matter is appropriate.

b. Anyone finding classified information out of proper control shall, if possible, take custody of and safeguard the material and their Security Coordinator who will inform the HQMC Security Manager. Secure communications should be used for notification whenever possible.

c. Heads of Staff Agencies/Activities will notify the DirAR (ARS) of all instances involving loss, compromise, or subjection to compromise of classified information or material. Upon report of a security incident involving classified information, the Staff Agency/Activity will conduct a security inquiry to

discover the facts and circumstances of the possible disclosure and the extent to damage of national security and recommendation of appropriate corrective action.

d. Security Inquires. Heads of Staff Agencies/Activities shall initiate an inquiry into the actual or potential compromise promptly to determine the facts and circumstances of the incident, and to characterize the incident as an infraction or a violation. The following procedures will be followed for each security inquiry:

(1) Deputy Commandant's/Director of Staff Agencies/ Activities will appoint in writing an official (other than the security coordinator or anyone involved with the incident) to conduct the inquiry. This individual shall have a security clearance eligibility and access commensurate to the classification level of the information involved. Figure 5-10 is an example of the Security Inquiry Appointment Letter. A copy of the appointment letter will be provided to DirAR (ARS).

(2) The inquiry shall be initiated and completed within **72 hours** upon initial discovery of the incident, as directed by reference (b). If circumstances exist that would delay the completion of the inquiry within 72 hours, notify the HQMC Security Manager, immediately, for an extension.

(3) Every effort should be made to keep the security inquiry report unclassified. The inquiry shall completely and accurately identify the classified information, material and/or equipment lost or compromised. This identification shall include the information's unclassified subject, or title; classification of the information (including any relevant warning notices, or intelligence control markings, downgrading and declassification instructions) serial numbers; the date of the information; the originator; the Original Classification Authority (OCA); the number of pages, or amount of material involved; a point of contact from the command, along with a telephone number of the custodial command. Figure 5-11 is an example of the report.

(4) Upon conclusion of the report, it will be endorsed and forwarded to the DirAR (ARS) by the Deputy Commandant/Director Staff Agency/Activity, stating the concurrence or nonoccurrence with the recommendations of the inquiry and if additional action is warranted.

(5) DirAR (ARS) will review the inquiry, carefully considering the circumstances surrounding the loss or compromise, and provide additional guidance as needed to the Staff Agency/Activity. Additionally, when circumstances meet the criteria for suspension of access as mentioned in reference (a), the recommendation for suspension will be forwarded from the Staff Agency/Activity to the DirAR for final decision.

(6) A copy of the inquiry will be provided to the Commanding Officer, Headquarters and Service Battalion, HQMC, Henderson Hall to determine if disciplinary actions are warranted.

e. Security Investigations. If the circumstances of an incident require a more detailed or additional investigation, then an individual shall be appointed by the Staff Agency/Activity Deputy Commandant/Director in writing, to conduct that investigation and, as appropriate, provide recommendations for any corrective or disciplinary actions.

(1) The individual appointed shall be sufficiently senior to ensure a successful completion of the investigation and should be commensurate with the seriousness of the incident; have an appropriate security clearance; have the ability to conduct an effective investigation; and shall be someone unlikely to have been involved, directly or indirectly, in the incident.

(2) As an investigation may lead to administrative or disciplinary action, the evidence developed should be comprehensive in nature and gathered in such a manner that it would be admissible in a legal or administrative proceeding. Consult local legal counsel as needed for procedural guidance on conduct of the investigation.

(3) The investigation should be accomplished promptly following appointment of the investigating officer. The results of the investigation shall be documented in writing. Figure 5-11 is an example of the report.

f. Data Spills

(1) Classified data spills occur when classified data is introduced either onto an unclassified information system or to

an information system with a lower level of classification, or to a system not accredited to process data of that restrictive category. Although it is possible that no unauthorized disclosure occurred, classified data spills are considered and handled as a possible compromise of classified information involving information systems, networks, and computer equipment until the inquiry determines whether an unauthorized disclosure did or did not occur.

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

(a) Immediately inform the HQMC Security Manager and HQMC Cyber Security Manager (ARI).

(b) Conduct a security inquiry to discover the facts and circumstances of the possible disclosure and the extent to damage of national security and recommendation of appropriate corrective action.

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

IN REPLY REFER TO:
5000
OFFICE CODE
Date

From: Director/Head, **Staff Agency/Activity**
To: Head, Security Programs and Information Management Branch (ARS)

Subj: REQUEST FOR WAIVER TO MARADMIN 226/11 AND AUTHORIZATION TO ENABLE SIPRNET "WRITE-TO" REMOVABLE MEDIA CAPABILITY WITHIN **STAFF AGENCY/ACTIVITY**

Ref: (a) MARADMIN 226/11

1. In accordance with the reference, I request a SIPRNet "write-to" removable media capability within the **Staff Agency/Activity**.

2. **Provide justification outlining the mission criticality of this capability for your organization**. "Write-to" removable media capability will not be granted where SIPRNET electronic file transfers can accomplish the same objective.

3. I understand, should this request be approved, Headquarters Marine Corps (HQMC), Information Systems Management Branch (ARI), shall modify SIPRNet hardware and user profiles for the specific purpose of enabling this capability; that the individuals listed below are authorized to perform "write-to" removable media for **Staff Agency/Activity**, and that this capability will be granted for a limited period, with re-verification required every (6) months.

Name	Rank
I. M. MARINE	MAJ

4. Point of contact for the request is (Name, Rank, Telephone Number and E-mail address).

SIGNATURE

Copy to: ARI

Figure 5-1--Request for Waiver to Enable SIPRNet "Write-to" Removable Media

Enclosure (5)

WRITE TO REMOVABLE MEDIA EXEMPTION REQUEST

REQUESTOR INFORMATION

1. NAME (LAST, FIRST, MI) / RANK	2. SECTION (i.e. G1, G2, PAO, ALD, etc.)	3. DATE
4. MACHINE NAME	5. MACHINE SERIAL NUMBER	
6. PHYSICAL LOCATION OF COMPUTER		
7. MILITARY BILLET DESCRIPTION / CIVILIAN POSITION DESCRIPTION	8. REQUESTED MEANS OF DATA WRITING ☐ USB ☐ OPTICAL DRIVE (CD)	
9. JUSTIFICATION		
10. BY MY SIGNATURE HEREUNDER, I FULLY UNDERSTAND THE RESPONSIBILITIES ASSOCIATED WITH THE TRANSFER OF INFORMATION FROM ONE SYSTEM TO ANOTHER. I FURTHER UNDERSTAND THAT ALL MEDIA REMOVED FROM THE SYSTEM WILL BE PROPERLY ACCOUNTED FOR, CLEARLY MARKED ACCORDING TO CLASSIFICATION LEVEL, STORED, TRANSPORTED, AND DESTROYED IN ACCORDANCE WITH SECNAVINST M-5510.36 (DON IPSP).		
11. DATE	12. REQUESTOR SIGNATURE	

SECURITY MANAGER

13. RECOMMENDATION ☐ APPROVE ☐ DISAPPROVE	14. DATA TRANSFER TRAINING COMPLETED (YYYYMMDD)	
15. COMMENTS		
16. DATE	17. PRINT NAME / RANK	18. SECURITY MANAGER SIGNATURE

G-6 IAM

19. RECOMMENDATION ☐ APPROVE ☐ DISAPPROVE		
20. COMMENTS / SUGGESTIONS FOR ALTERNATIVE METHOD		
21. DATE	22. PRINT NAME / RANK	23. IAM SIGNATURE

DAA (APPROVED AUTHORIZER)

24. DECISION ☐ APPROVED ☐ DISAPPROVED		
25. COMMENTS		
26. DATE	27. PRINT NAME / RANK	28. APPROVING AUTHORITY SIGNATURE
29. COPY TO: ☐ MITSC ☐ MIDPAC ☐ RNOSC ☐ MCNOSC		

*THIS FORM WILL BE RETAINED ON FILE FOR A MINIMUM OF FIVE YEARS.

Figure 5-2-—Write to Removable Media Exemption Request

ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO *(If required)* FROM *(If required)* THROUGH *(If required)*

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security containers have been locked and checked.																															
2. Desks, wastebaskets and other surfaces and receptacles are free of classified material.																															
3. Windows and doors have been locked (where appropriate).																															
4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.																															
5. Security alarm(s) and equipment have been activated (where appropriate).																															
INITIAL FOR DAILY REPORT																															
TIME																															

701-101
NSN 7540-01-213-7899

Form designed using PerForm Pro software.

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

Figure 5-3--Activity Security Checklist

SECURITY CONTAINER CHECK SHEET

TO (if required) | **THRU** (if required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

FOLD HERE - REVERSE FOLD FOR FULL USE OF BOTH SIDES - FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM | ROOM NO. | BUILDING | CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

STANDARD FORM 702 (8-85) (EG)
Prescribed by GSA/ISCO
32 CFR 2003
Designed using Perform Pro, WHS/DIOR, Jul 94

Figure 5-4--Security Container Check Sheet

CLASSIFICATION LEVEL

SECURITY CONTAINER INFORMATION INSTRUCTIONS 1. Complete Part 1 and Part 2A (on end of flap). 2. Detach Part 1 and attach to the inside of the control drawer of the security container. 3. Mark Parts 2 and 2A with the highest classification level stored in this security container. 4. Detach Part 2A, insert in envelope (Part 2) and seal. 5. See Privacy Act Statement on reverse.	1. AREA OR POST *(If required)*	2. BUILDING *(If required)*	3. ROOM NO.
	4. ACTIVITY *(Division, Branch, Section or Office)*		5. CONTAINER NO.
	6. MFG. & CLASS OF CONTAINER	7. MFG. & LOCK MODEL	8. SERIAL NO. OF LOCK
9. DATE COMBINATION CHANGED	10. PRINT NAME/ORGANIZATION SYMBOL WITH SIGNATURE OF PERSON MAKING CHANGE.		
11. *Immediately notify one of the following persons, if this container is found open and unattended.*			

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

1. ATTACH TO INSIDE OF SECURITY CONTAINER

700-102
NSN 7540-01-214-5372

STANDARD FORM 700 (REV. 4-01)
Prescribed by NARA/ISOO
32 CFR 2003

Figure 5-5--Security Container Information

CLASSIFIED MATERIAL DESTRUCTION REPORT

TO:

CLASSIFICATION *(Indicate when title or other identification is classified)*

FROM *(Name and address of activity)*

The classified material described below has been destroyed in accordance with regulations established by the Department of the Navy Information Security Program Regulation, OPNAV INSTRUCTION 5510.1E.

The purpose of this form is to provide activities with a record of destruction of classified material. Also, copies may be utilized for reports to activities originating material, where such reports are necessary.

DESCRIPTION OF MATERIAL

SERIAL/LOG	ORIGINATOR	DATE	COPY NO.	LOG/ ROUTE SHEET	ENCLOSURES (IDENT. & NO.)	TOTAL NO. PAGES

OFFICER OR INDIVIDUAL AUTHORIZING DESTRUCTION *(Signature, Rank/Rate/Grade)*

DATE OF DESTRUCTION

WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)*

WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)*

OPNAV 5511/12 (Rev. AUG 1975)

Figure 5-6--Classified Material Destruction Report

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** *(Include Area Code)* (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) *(Delivery person be cleared at the same level of, or higher than the material delivered.)*

7. RECEIVED BY *(To be completed by incinerator plant personnel/driver)*

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 5-7--Burn Bag Receipt

Security Plan

Overview:

(U) Host:

(U) Meeting Dates and Times:

(U) Attendees:

(U) Level:

(U) Staff:

(U) Logistics: Who is responsible for coordinating and implementing all security requirements?

(U) Physical Security: Detailed description of the facility to include:

-Location
-Parking
-Lodging
-Entrance/Exit
-Electrical and Emergency Power
-Water Source
-HVAC
-On-Site Security Force
-Security Systems (Intrusion Detection, Alarms, X-Ray)
-Additional conferences to be held at the facility

(U) Emergency Response:

-Local Law Enforcement
-Ambulance/Emergency Medical Services
-Fire and Rescue

(U) Information & Personnel Security:

-Access eligibility verified through JPAS.
-Badging
-Verification of Identity
-Note taking
-Security Briefing
-Storage
-Transportation

(U) Conference Security Officer: Full name, office, address and telephone number of the event security officer. The event security officer must possess a thorough understanding of security policy and protocol.

Figure 5-8--Security Plan (Template)

(LETTER HEAD)

5527
XXXX
Date

From: Staff Agency/Activity Command Address
To: Under Secretary of Defense for Intelligence [USD (I)]
Via: (1) Director, Administration and Resource Management Division (ARS)
(2) Deputy Commandant for Plans, Policies and Operations, Security Division (PS)
(3) Deputy Under Secretary of Navy for Plans, Policy, Oversight and Integration (DUSN PPOI)

Subj: REQUEST FOR HOSTING CLASSIFIED MEETING IN NON-DOD CLEARED FACILITY

Ref: (a) DoD M5200.1
(b) HQMC IPSP SOP

1. Per the references this agency request to conduct a classified meeting in a Non-DoD cleared facility.

2. Provide detailed information regarding this request in this paragraph. Sub-paragraphs authorized as needed.

3. Agency point of contact regarding this request is, INSERT NAME, TITLE, AND COMMERCIAL PHONE NUMBER.

SIGNATURE

Figure 5-9--Request for Hosting Classified Meeting in Non-DoD Cleared Facility Letter

(LETTER HEAD)

5527
XXXX
Date

From: **Deputy Commandant/Director, Staff Agency/Activity Name**
To: **Investigating Official**

Subj: APPOINTMENT TO CONDUCT A SECURITY INQUIRY

Ref: (a) DoD M-5200.01
(b) HQMC IPSP SOP

1. Per the references, you are appointed to conduct an inquiry as soon as practical into circumstances surrounding the possible compromise of classified information that occurred at **Staff Agency/Activity Name** on **Date of Incident**.

2. You are to investigate all the facts, circumstances and the cause of possible compromise and provide identification of all compromised information and any potential impact on national security. You should recommend appropriate actions needed to prevent future violations of the type of investigated. No recommendations should be made with regard to punitive action against the individual(s) responsible for the violation. Particular attention should be given to enclosure (6), volume 3; section 6 of reference (a).

3. Report your findings of fact, opinions, and recommendations by _____, unless an extension of time is granted.

4. This appointment will remain in effect until you are formally relieved. By return endorsement, you will indicate that you have assumed the duties associated with this appointment.

SIGNATURE

_____

Date

FIRST ENDORSEMENT

From: **Investigating Official**
To: **Deputy Commandant/Director, Staff Agency/Activity Name**

1. I have assumed the duties outlined in the basic letter and have familiarized myself with enclosure (6), volume 3; section 6 of reference (a).

SIGNATURE

Figure 5-10--Appointment to Conduct a Security Inquiry Letter

(LETTER HEAD)

5527
XXXX
Date

From: **Investigating Official**
To: **Deputy Commandant/Director, Staff Agency/Activity Appointed By**

Subj: REPORT OF SECURITY INCIDENT INQUIRY OR INVESTIGATION

Ref: (a) DoD M-5200.01
(b) HQMC IPSP SOP

Encl: (1) **(If any)**

1. Incident: Per references (a), on **Date of the Incident** a inquiry was conducted into the possible loss or compromise of classified information at **Location of the Incident**.

2. Statement of Facts:

a. Identification of Information or Equipment Lost or Compromised:

(1) CLASSIFICATION:

(2) IDENTIFICATION/SERIAL NO(S):

(3) DATE:

(4) ORIGINATOR:

(5) OCA(S):

(6) SUBJECT OR TITLE:

(7) DOWNGRADING/DECLASSIFICATION INSTRUCTIONS:

(8) NUMBER OF PAGES OR ITEMS OF EQUIPMENT INVOLVED:

(a) Pages:

(b) Equipment:

Figure 5-11--Report of Security Incident Inquiry or Investigation

Subj: REPORT OF SECURITY INCIDENT INQUIRY OR INVESTIGATION

(9) COMMAND POINT OF CONTACT AND PHONE NUMBER

(10) UIC CUSTODIAL COMMAND: 54008.

b. Assessment of Likelihood of Loss or Compromise.

c. Notification of Local NCIS Office.

d. Circumstances Surrounding the Incident.

(1) NARRATIVE:

(2) INTERVIEWS CONDUCTED:

e. Individuals Responsible (If any).

f. Determination of Security Weakness(es) or Vulnerability(ies).

3. Conclusion.

4. Corrective Measures Taken as a Result of the Incident.

a.

b.

5. Further Action: No further action is required.

SIGNATURE

Copy to:
(As required)

FOR OFFICIAL USE ONLY (or if classified insert classification and add other markings as required)

Figure 5-11--Report of Security Incident Inquiry or Investigation-Continued

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 (j) 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 Intelligence Department, 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).

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

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 that all required forms for DoD Contactors reporting to their staff agency/activity are completed within the PPICSS application and submitted to the Security Section: DoD Badge Request (refer to Figure 4-1), HQ NAVMC 512 (Classified Information Access Authorization) (refer to Figure 4-2), SF 312 (Non-Disclosure Agreement) (refer to Figure 4-3), DoD Badge Agreement (refer to Figure 4-4), and HQMC Security Orientation/Awareness Briefing (refer to Figure 4-5), 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; telephone number; 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 6-1). If the contactor 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: DoD Badge Request (refer to Figure 4-1), Visitor Request [must be 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. DD 254, with 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 request contractor personnel to be processed for NACI via PPICSS. Upon receipt of the request ARS will initiate the NACI via e-QIP. Once the investigation is submitted, DoD contracts located within NCR, will have their fingerprints taken at DirAR (ARS), room 2A288A. DoD contracts located outside the NCR will submit to ARS two fingerprint cards (SF-258) [provided by the Facility Security Officer (FSO)] and Report of Separation (DD 214) (if applicable) in both cases to the HQMC Security Manager.

c. A CAC will be issued when the investigation questionnaire has been submitted to OPM for processing. In order to be issued a CAC, a contractor must present two forms of identification listed in Figure 4-11. If issues exist which prevent favorable adjudication of the investigation, the DirAR Division (ARS) will receive an Investigative Form 79A “Report of Agency Adjudicative Action” from OPM requesting that a suitability determination be made in accordance with OPM Homeland Security Presidential Directive (HSPD) 12 “Credentialing Standards”. Contractors not receiving a “favorable” suitability determination will have their CAC revoked.

7. For DoD contractor check-out procedures, refer to enclosure (4).

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

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort))

1. CLEARANCE AND SAFEGUARDING
a. FACILITY CLEARANCE REQUIRED:
b. LEVEL OF SAFEGUARDING REQUIRED:

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
	c. SOLICITATION OR OTHER NUMBER	DUE DATE *(YYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

	a. ORIGINAL *(Complete date in all cases)*		Date *(YYMMDD)*
	b. REVISED *(Supersedes all previous specs)*	Revision No.	Date *(YYMMDD)*
	c. FINAL *(Complete item 5 in all cases)*		Date *(YYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☐ NO, If yes, complete the following
Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract

5. IS THIS A FINAL DD FORM 254? ☐ YES ☐ NO, If yes, complete the following:
In response to the contractors request dated _____, retention of the identified classified material is authorized for a period of: _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTORS FACILITY OR GOVERNMENT ACTIVITY		
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 *(Specify)*		
k. OTHER *(Specify)*					

DD Form 254, DEC 99 (EF) *Previous editions are obsolete.* (DISA IRXDTS, Inc.)

Figure 6-1--Contract Security Classification Specification

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

☐ DIRECT ☐ THROUGH *(Specify)*

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

14. ADDITIONAL SECURITY. Requirements, in addition to NISPOM requirements, are established for this contract. *(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is required.)* ☐ YES ☐ NO

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. *(If yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if more space is needed.)* ☐ YES ☐ NO

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*

d. ADDRESS *(Include Zip Code)*	17. REQUIRED DISTRIBUTION
	☐ a. CONTRACTOR
	☐ b. SUBCONTRACTOR
	☐ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
	☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	☐ e. ADMINISTRATIVE CONTRACTING OFFICER
e. SIGNATURE	☐ f. OTHERS AS NECESSARY

DD FORM 254 Reverse, DEC 99 *Previous editions are obsolete.* (DISA IRXDTS, Inc.)

Figure 6-1--Contract Security Classification Specification-Continued