UNITED STATES MARINE CORPS
MARINE CORPS BASE
3250 CATLIN AVENUE
QUANTICO VA 22134 5001

IN REPLY REFER TO
5510
B 013
6 Dec 13

MARINE CORPS BASE ORDER 5510.1D w/CH 1

From: Commander
To: Distribution List

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM

1. Situation. To ensure changes are made to provide clarity within Chapter 2 of the subject Order.

2. Mission. Change Chapter 2, Section 2002 and reflect the intent behind the assignment of security personnel aboard Marine Corps Base Quantico.

3. Execution. To direct the following changes to the subject Order.

a. Change page 2-2, Section 2002 Title line to reflect “COMMAND” vice “ACTIVITY”.

b. Change page 2-2, Section 2002, paragraph 1 to read, “In addition to the appointments made at the MCBQ level, one security manager will be appointed in writing by each major subordinate command and all tenant commands that hold classified material, see (*figure 2-1*).” vice “activity and all activities that hold”.

c. On page 2-2, Section 2002, add a new sub-paragraph 2 to read as follows, “2. Commanding officers will obtain formal training for their security managers as soon as practical upon being assigned. The Headquarters Marine Corps Security Managers course is the authorized course for Marine Corps personnel. This course of instruction is offered aboard Quantico twice annually and coordinated through the Base Headquarters command security branch. Prerequisite on-line training courses are required prior to scheduled attendance. It is further recommended that all efforts be made to fill available seats in an effort to train as many security personnel as may be qualified within your security teams.”

d. Update page 2-2, Section 2002 by moving the old sub-paragraph 2 down to become sub-paragraph 3 and deleting paragraph 3 of the original Order.

e. PROVMAIN.

4. Administration and Logistics. This change is issued for clarity of substance as it relates to the functional support and assignment of a Security Manager.

5. Command and Signal

a. Command. This Order is applicable to all Marines, Reservists, Civilians, and sailors attached to this command.

b. Signal. Effective date signed.

/s/
R. L. ANDERSON
Chief of staff

Distribution List: A

LOCATOR SHEET

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM

Location: _____
(Indicate the location(s) of the copies of this Order).

THIS PAGE INTENTIONALLY LEFT BLANK

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS
PART I
PERSONNEL SECURITY

TABLE OF CONTENTS
PART II
INFORMATION SECURITY

Chapter 6: MARKING

Chapter 7: SAFEGUARDING

Chapter 8: DISSEMINATION

Chapter 9: TRANSMISSION AND TRANSPORTATION

Chapter 10: STORAGE AND DESTRUCTION

Chapter 11: INDUSTRIAL SECURITY PROGRAM

Chapter 12: LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

APPENDICES

PART I

PERSONNEL SECURITY PROGRAM

CHAPTER 1

BASIC PROGRAM POLICY and AUTHORITIES

1000. BASIC POLICY. The Marine Corps Base, Quantico (MCBQ) Personnel Security Program is established in compliance with the Department of the Navy Program to ensure that information classified under the authority of Executive Order 13526 is protected from unauthorized disclosure and that appointment of military personnel in the Navy and Marine Corps and granting access to classified information or assignment to sensitive duties is in compliance with Executive Order 10450 and 12968, Security Requirements for Government Employees, Department of Defense (DoD) 5200.2-R, DoD Personnel Security Program Regulations.

1001. AUTHORITY

1. The Commander, MCBQ is responsible for establishing and maintaining a Personnel Security Program in compliance with reference (a) and an Information Security Program in compliance with reference (c).

2. The responsibility for security and proper handling of classified material extends directly to the individual having knowledge or possession of such material and to activity heads within whose purview classified material is utilized.

3. Individual request for guidance or interpretation of this publication should be addressed to the Commander, MCBQ (B 054) Attn: Command Security Manager.

1002. APPLICABILITY OF THIS PUBLICATION

1. This Order establishes coordinated policies for the security of classified information and for personnel security matters incorporating the policies of numerous DoD/Navy Directives. It is not expected that these directives will or can ensure absolute security at this Base. Rather, they permit the

accomplishment of essential tasks while affording selected items of information reasonable degrees of security with a minimum risk.

2. This Order establishes coordinated policies for maintenance of the Information and Personnel Security Program (IPSP) at MCBQ and is applicable to all organizations and activities under the purview of the Commander. References (a) thru (e) and this Order provide the basis for implementing the IPSP.

1003. RESPONSIBILITY FOR COMPLIANCE

1. Activity heads are responsible for compliance with and implementation of this Order within their activity.

2. Each individual, military, civilian or contractor, in or employed through the Navy or Marine Corps, is responsible, for compliance with this Order in all respects.

1004. SPECIAL ACCESS PROGRAMS. These programs will be handled per the guidelines contained in reference (a) thru (d). The Base Special Security Officer will act as coordinator for the special access programs and sensitive compartmented information in cooperation with the Commander, MCBQ (B 054).

PERSONNEL SECURITY PROGRAM

CHAPTER 2

COMMAND SECURITY MANAGEMENT

2000. BASIC POLICY. Commanding officers, directors, and activity heads are responsible for compliance with and the implementation of the Department of the Navy Information and Personnel Security Programs (IPSP) within their organizations.

2001. BASE MANAGEMENT

1. The base management program establishes a network of personnel throughout this base to supervise and ensure effective security control and utilization of classified materials.

2. To ensure proper security procedures are in place for Marine Corps Base, Quantico (MCBQ) and its tenant commands the following appointments will be made in writing, setting forth the requirements that are familiar with the specific portions of references (a) through (e) and other directives as they may pertain (*See Appendix C*).

a. Command Security Manager - Security Specialist/0080. (*Appointed by, Commander/Acting*)

b. Assistant Command Security Manager - Security Specialist/0080. (*Appointed by, Commander/Acting/By direction*)

c. Head Classified Material Control Center (CMCC) – Security Specialist/0080. (*Appointed by, Commander/Acting/By direction*)

d. Primary Custodian of Classified Material - Security Specialist/0080. (*Appointed by, Commander/Acting/By direction*)

e. Communications Security Material System (CMS) Responsible Officer – Security Specialist 0080. (*Appointed by, Commander/Acting)*

f. Publications, Control Officer - Security Specialist/0080. (*Appointed by, Commander/Acting/By direction*)

g. North Atlantic Treaty Organization (NATO) account holder and the Critical Nuclear Weapons Design Information (CNWDI) Control Officer - Security Specialist/0080.(*Appointed by, Commander/Acting/By direction*)

h. Information Security Officer - Security Specialist/0080. (*Appointed by, Commander/Acting/By direction*)

l. Personnel Security Officer - Security Specialist/0080. (*Appointed by, Commander/Acting/By direction*)

m. Contracting Officers Security Representative (COSR) Security Specialist/0080. (*Appointed by, Commander/Acting/By direction*)

2002. APPOINTMENT OF COMMAND SECURITY MANAGERS

1. In addition to the appointments made at the MCBQ level, one security manager will be appointed in writing by each major subordinate activity and all activities that hold classified material, see (*figure 2-1*). This appointment will be, an officer or a civilian GS-11, or above (*Appointed by, Commanding Officer/Acting*). Waivers may be requested when necessary. These managers will serve as direct representatives of the MCB command security manager. As such, they will receive guidance from and work with the command security manager on various issues that pertain to the IPSP. They will keep the Command Security Manager informed of all security violations and/or security concerns.

2. Assistant security manager (*appointed as required*) appointments (*figure 2-1*) will be an officer or warrant officer, enlisted person E-6 or above, civilian GS-07 or above (*Appointed by, Commanding Officer/Acting/By direction*). He/she will in turn be responsible to their respective security manager.

3. Heads of tenant activities will appoint a security manager. The appointee will be an Officer or a civilian GS-11 or above (*Appointed by, Commanding Officer/Acting*). This appointee

will serve as a direct representative of the Command Security Manager. They will receive guidance from and work with the Command Security Manager (B 054) on various issues that pertain to the IPSP. They will keep the Command Security Manager informed of all security violations and/or security concerns.

4. Activity heads will not appoint or assign contractor personnel as security managers, nor will they be assigned other security duties unless stated in their contract or statement of work.

2003. OTHER APPOINTMENTS

1. Each activity that anticipates the handling of Top Secret information will appoint a Top Secret Control Officer (TSCO) in writing. Individuals appointed must be an E-7, a civilian GS-07 or above and have a final Top Secret security clearance and access.

2. Activity heads may, as needed, designate Top Secret Control Assistant (TSCA) or TSCO. Personnel so designated must be an E-5, a civilian GS-06 or above and have a final Top Secret security clearance and access. The requirements and duties of the assistant are contained in Chapter 2 of reference (b) and (d), which will be referenced in the letter of appointment, with a copy forwarded to the command security manager (B 054). The designation of a TSCA does not relieve the TSCO of any responsibility for the control and protection of Top Secret material.

3. Activities that hold classified material will appoint a classified material custodian in writing, (*Figure 2-2*) and any number of assistants as required. Individuals so assigned are responsible for ensuring that the control, handling, and security procedures for classified material within their respective activities are conducted per the provisions of references (a) through (e) and this Order. A custodian appointed by the activity must complete training prescribed by the Head, CMCC prior to assuming the unit’s classified holdings. The appointee must be an E-4, a civilian GS-05 or above.

4. All activities certified as Secondary Control Points will designate in writing personnel who are authorized to receipt for classified material at the CMCC or from the CMCC courier (*Appointed by, Commanding Officer/Acting/By*

direction/Security Manager), *(Security personnel are authorized to perform this task by appointment. Do not include them again on this authorization letter)*. Personnel authorized to receipt for classified material (*Figure 2-3*) must also be listed on at least one of the unit's SF 700 envelope(s) (*Figure 6-1*). Reasoning is that individuals authorized to sign for classified material must be able to properly secure it.

5. All activities assigned a Security Management Office code (SMO code) from SMO code 300015 are required to join all persons assigned to them, active duty and civilian, regardless whether or not they are expected to be granted access to classified information.

a. The primary purposes for issuing SMO codes is for security personnel to monitor investigation status, clearance eligibility, verify access, submit visit requests, and to take part in the continuous evaluation program, etc.

b. It is intended for subordinate SMOs to process incoming visit requests and grant access. Per Part I, Chapter 9 of this Order, Command Security Personnel, MCBQ are the only authority that can grant visitor access.

c. Only Common Access Card (CAC) eligible contractor personnel occupying government spaces aboard Quantico will be joined as "serviced" within a subordinate SMO's Personnel Security Management Network (PSM Net). Contractors that are joined will always have an end date indicated in Joint Personnel Adjudication System (JPAS) with no visit period exceeding 1 year from the visit begin date.

d. Subordinate SMOs will grant, remove or alter accesses recorded in JPAS for personnel they have joined in their PSM Net.

2004. DUTIES OF THE SECURITY MANAGER. There are duties out of the jurisdictional control of activity and division security managers that are held only by the Command Security Manager, however, the doctrinal duties of a Security Manager are contained in Chapter 2 of references (b) and (d) and must be reviewed upon appointment.

2005. COMMAND SECURITY PROCEDURES. Each activity will publish as required, written procedures (LOI/SOP) specifying how the requirements of references (a) through (d) and this Order will be accomplished. Necessary changes will be written when required to reflect changes in the activity's functions. Each activity's security procedure will specify the responsibilities of appointed security personnel and procedure to be followed for the control and handling of classified material. Guidelines are contained in reference (b), (d) and this Order.

2006. INTER-SERVICE SUPPORT AGREEMENTS (ISSA)

1. Overall security at MCBQ is the responsibility of the Commander. Security servicing of various tenant activities will be performed pursuant to ISSA. These services will be coordinated through the Comptroller and approved by the MCB Command Security Manager.

2. Tenant activity heads will keep the Commander, MCBQ (B 054) informed of any matters that may have a direct affect on the security procedures of this Base.

2007. EMERGENCY PLANS. Each activity that handles classified information will develop an emergency plan for the protection of classified material in case of natural disaster, civil disturbance, or enemy action. This plan must be detailed with specific procedures and responsibilities. Emergency destruction plans, if required, will be incorporated into the emergency plan.

(*Letter Head*)

5500
(*Originator Code*)
(*Date*)

From: Commanding Officer
To: Individual Appointment

Subj: DESIGNATION OF SECURITY MANAGER

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) MCBO 5510.1C

1. In compliance with the provisions of references (a) through (c), you are designated as the Security Manager for (*Unit /Activity*).

2. You are directed to familiarize yourself with the duties of the Security Manager, utilizing paragraph 2-3 of reference (a) and paragraph 2-2 of reference (b) and other directives as required in the performance of your duties.

3. Previous appointments as Security Manager are revoked.

SIGNATURE
(*Commanding Officer/Acting*)

Copy to:
Files
Commander, MCB (B 054)

Figure 2-1.--Sample Security Manager Appointment Letter

Enclosure (1)

(*Letter Head*)

5500
(*Originator Code*)
(*Date*)

From: Commanding Officer
To: Individual Appointment

Subj: APPOINTMENT AS CLASSIFIED MATERIAL CUSTODIAN

Ref: (a) SECNAV M-5510.36
(b) MCBO 5510.1C

1. In compliance with the provisions of references (a) and (b), you are appointed as the Classified Material Custodian for (*Unit/Activity*).

2. You are directed to familiarize yourself with the duties of the Secondary Control Point Custodian utilizing references (a) and (b) and other directives as are required in the performance of your duties.

3. Previous appointments as Classified Material Custodian are revoked.

SIGNATURE
(*Commanding Officer/Acting/By direction*)

Copy to:
Files
Commander, MCB (B 054)

Figure 2-2.--Sample Classified Material Custodian Appointment

Enclosure (1)

Letter

(*Letter Head*)

5510
(Originator Code)
(Date)

From: Commanding Officer/Security Manager
To: Commander, Marine Corps Base (B 054) (Attn: Head, Classified Material Control Center)

Subj: DESIGNATION OF AUTHORIZED RECIPIENTS FOR CLASSIFIED MATERIAL

Ref: (a) MCBO 5510.1C

1. Per the reference, the following person(s) whose name(s) and Specimen signature(s) appear below are authorized to receipt for classified material for (*Unit/Organization*) up to and including the classification indicated.

Name/Grade/SSN(Last 4)	Classification Authorized	Signature

2. This designation letter cancels and supersedes all previous designation letters.

SIGNATURE
(*Commanding Officer/Acting/By direction/Security Manager*)

Copy to:
Files

Figure 2-3.--Sample Designation of Authorized Recipients, For Classified Material Letter

Enclosure (1)

PERSONNEL SECURITY PROGRAM

CHAPTER 3

COUNTERINTELLIGENCE MATTERS

3000. BASIC POLICY. Certain matters affecting National Security must be reported to a Resident Agent, Naval Criminal Investigative Service (RA NCIS) so that counterintelligence measures can be taken. All Department of the Navy military and civilian personnel at Quantico, whether they have access to classified information or not, will report to their Security Managers, the base Security Manager, the Commanding Officer or to the nearest command, any activities described below involving themselves, their immediate relatives, co-workers or others. Those individuals will in turn immediately notify the RA, NCIS Quantico or the Director, NCIS (DIRNAV CRIMINVSERV) Washington D.C. by classified IMMEDIATE message, with CNO (NO9N) as an Information addressee.

a. Sabotage, Espionage, International Terrorism or Deliberate Compromise

b. Known individuals with, or without clearance eligibility seeking illegal access to classified materials.

c. Report personnel who have access to classified information and commit or attempt to commit suicide.

d. Report unauthorized absentees who have access to classified information.

e. Report death or desertion of a DON person who has access to classified information.

3001. FOREIGN TRAVEL. Foreign Travel briefings are normally provided by a RA, NCIS, Marine Corps Base, Quantico prior to travel overseas.

3002. COUNTERINTELLIGENCE. Refer to Chapter 3 of reference (a) for additional guidance on counterintelligence matters.

PERSONNEL SECURITY PROGRAM

CHAPTER 4

SECURITY EDUCATION

4000. BASIC POLICY. Each commanding officer/director of a Secondary Control Point (SCP) holding classified information will establish and maintain an active security education program to instruct all personnel, regardless of their position, rank or grade, in security policies and procedures. The Marine Corps Base, Quantico (MCBQ) Command Security Manager will provide guidance and support in this matter. Chapter 4 of reference (b) explains the requirements for developing a security education program.

4001. MINIMUM REQUIREMENTS. The following are the minimum requirements for security education.

1. The MCBQ, Command Security Manager through command/division Security Managers is responsible for ensuring that all personnel granted access to classified material receive an orientation briefing (*the brief is provided by the Command Security Managers office on site when access is granted*).

2. Security Managers will ensure that annual security refresher training and counter-espionage briefings for personnel that have been granted access to classified information are completed prior to the beginning of each new Calendar Year.

NOTE: *Failure for individuals to complete the training requirements mentioned above could result in the loss of access until compliance is achieved.*

3. Security Managers will ensure debriefing and termination statement requirements are met per paragraph 4-11 and 4-12 of reference (b), so that the individuals name can be removed from access rosters and his/her Joint Personnel Adjudication System account can be updated to reflect their new status.

4. Security Managers will request that persons traveling to foreign countries receive a foreign travel brief by a member of the Naval Criminal Investigative Service (NCIS) Quantico prior to departure. NCIS personnel will determine if a foreign travel brief/debrief is necessary.

5. Special Category (SPECAT) publication briefings will be given by the command security manager's office, e.g. North Atlantic Treaty Organization/Critical Nuclear Weapons Design Information, at the Classified Material Control Center. Special Compartment Information indoctrination will be through the Marine Corps Intelligence Activity (MCIA), Special Security Officer.

4002. TRAINING AND EDUCATION

1. Every appointed Security Manager must complete a set of prerequisite on-line courses which qualify the individual to attend the HQMC Security Managers course. Registrations for both are through the Command Security Manager's office (B 054).

2. All appointed SCP custodians will make arrangements with the Command Security Manager's office (B054), located in Building 3250, Room 27, for classified custodian training prior to assuming their commands classified holdings.

3. On-the-job training is the phase of security education when security procedures for the assigned position are learned. Security Managers will assist supervisors in identifying appropriate security requirements. Supervision of on-the-job training process is critical. Supervisors are ultimately responsible for procedural violations or for compromises that result from improperly trained personnel. Expecting subordinates to learn proper security procedures by trial-and-error is not acceptable.

4003. SECURITY AWARENESS. Signs, posters, and bulletin board notices will be posted in conspicuous areas to ensure continuous and frequent exposure to security awareness measures. Materials may be obtained from the Command Security Managers Office. Notices should be placed throughout your surroundings identifying your Command Security Manager, office numbers and procedures for reporting incidents or suspicious personnel or packages.

PERSONNEL SECURITY PROGRAM

CHAPTER 5

SENSITIVE AND INFORMATION TECHNOLOGY POSITIONS

5000. BASIC POLICY. Commanding officers are required to designate each national security position within their command per reference (b). Criteria for designating sensitive and Information Technology positions are contained in Chapter 5 of reference (b).

5001. MAINTENANCE PROCEDURES. Security Managers will maintain a record of sensitive and IT position designation decisions to ensure all investigations and updates are submitted per current guidelines.

5002. SUITABILITY AND SECURITY INVESTIGATION AND ADJUDICATION

1. Personnel security investigations are conducted to gather information to meet OPM requirements for employment suitability and to satisfy executive branch requirements for making personnel security determinations. After determining the position sensitivity level, the appropriate investigation may be requested.

2. The focus of a suitability investigation is for employment purposes. Employment suitability investigations/adjudications are based on standards and criteria established by EO 12968 and are normally handled by the servicing Human Resources and Organizational Management (HROM) Office on behalf of the Command.

3. The focus of a security determination is for security clearance eligibility/suitability for assignment to sensitive duties. These are requested based on criteria established by EO 12968 and are handled by Department of Defense, Central Adjudication Facility (DOD CAF) and the local Command Security Manager.

4. Civilian investigations for non-sensitive or public trust positions will be forwarded to HROM for processing and suitability for employment determinations.

5. Unless otherwise directed, military and civilian investigations for sensitive positions/clearance eligibility will be forwarded to the Command Security Manager for processing and a security determination.

5003. CONTRACT SUPPORT PUBLIC TRUST DETERMINATIONS

1. Background. In compliance with USD DTM 08-003 dated 1 December 2008 and CNO letter 5510 Ser NO9N2/8U223257 of 9 October 2008, uniformed service members, civilian employees, presidential appointees or Common Access Card (CAC) eligible contract employees under the terms of applicable contracts will need to initiate a National Agency Check with inquiries (NACI): National Agency Check, Law Checks, and Credit or an initiated national security investigation; and a favorable completion of a Federal Bureau of Investigation fingerprint check for credential issuance. The USD (P&R) and DoD lead for Homeland Security Presidential Directive - 12 will work with the Office of Personnel Management (OPM) to integrate the NACI status and fingerprint check information into the CAC issuance process.

2. Responsibilities

a. The responsibilities for supporting contract entities that require the CAC to perform their government contract duties will be further addressed upon receipt of additional clarification by higher authority. In the interim, the processing of the completed SF 85 when required will be accomplished by the contract entity and may be submitted by the Command Security Manager if required. Investigations returned by OPM for correction will be returned to the contract entity.

b. Contract trustworthiness determinations will be adjudicated by the (DOD CAF). Favorable trustworthy determinations will support public trust positions only. The scope of a NACI investigation does not meet the standards for clearance eligibility.

c. DOD CAF will enter the determination into the Joint Personnel Adjudication System (JPAS). Contract entities monitor JPAS to determine when adjudications have been entered for their respective personnel. When the determination is posted, the contract facility may request the issuance of the CAC using

Contract Verification System (CVS) procedures.

d. If issues are discovered, the DOD CAF will place a “no determination made” entry in JPAS/JCAVS and forward the investigation to the submitting office for the government to adjudicate. The contract entity should provide the government with mitigation of disqualifiers.

e. National security clearance eligibility determinations will be used in lieu of a public trust investigation NACI. When the person has clearance eligibility, the contract facility may request the issuance of the CAC using CVS procedures through the local Deers office.

f. The government will process the request for CAC using the CVS.

PERSONNEL SECURITY PROGRAM

CHAPTER 6

PERSONNEL SECURITY INVESTIGATIONS

6000. BASIC POLICY

1. No individual will be given access to classified information or be assigned to sensitive duties unless a favorable 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.

2. Only the Command Security Manager, Special Security Officer and/or those personnel specifically authorized to do so will request a PSI.

3. A PSI will not normally be requested for any individual who will be retired, resigned, or separated with less than 1 year of service remaining. Temporary Access and One-Time Access will be taken under review by the Command Security Manager per Chapter 9 of reference (b) for short-term access.

4. Investigations other than PSIs will be handled by the appropriate investigative agency i.e., Naval Criminal Investigative Service, Criminal Investigation Command, and reported to the Command Security Manager when they impact assignments to sensitive positions or granting of a security clearance.

5. Further guidance concerning a PSI is contained in chapter 6 of reference (b).

6001. REINVESTIGATIONS. Reinvestigations will be submitted as follows:

1. Single Scope Background Investigation (SSBI) – Periodic Reinvestigation (PR). SSBI-PR are conducted on personnel whose clearance/access to Service Corporation International (SCI)or Top Secret information is based on a investigation that is 5 years old or more. SSBI-PR is submitted 4 years and 11 months from their last closed investigation date. Other requirements are contained in paragraph 6-2.2.f.(1) of reference (b).

2. Phased PR (PPR). A limited SSBI-PR is conducted under the same circumstances as an SSBI-PR, as warranted by the case. Other requirements are contained in par 6-2.2.f.(2) of reference (b).

3. National Agency Check with Local Agency Checks (NACLC)/ Access National Agency Check with Inquiries (ANACI). A NACLC/ANACI is conducted at 10-year and 15-year intervals to support continued access to Secret and Confidential classified information, respectively. A NACLC/ANACI is also conducted at 5-year intervals for personnel with secret security clearance in a Special Access Program and those performing Explosive Ordnance Disposal or Personnel Reliability Program (PRP) controlled duties. Other requirements are contained in paragraph 6-2.2.f.3 of reference (b).

4. Reinvestigations will not be submitted earlier than 30 days prior to periodicity due date.

6002. SUBMISSION OF PERSONNEL SECURITY QUESTIONNAIRES

1. Personnel requiring security investigations may obtain assistance as follows:

a. Marine Corps Base, Quantico (MCBQ) and subordinate command personnel may contact their Command Security Manager to initiate their investigations.

b. Contractors should contact their Facility Security Officer. Contractors not aligned to classified duties as direct hires, may be coordinated between Human Resources Office and the MCBQ Command Security Manager (B 054).

2. All commanding officers/directors are directed to ensure periodic and meaningful audits of access rosters to ensure timely submission of reinvestigations for your personnel. Auditing the rosters will reduce the number of individuals failing to update security investigations thereby reducing the need to withdraw access for noncompliance.

6003. SENSITIVE POSITIONS. An SSBI is required for each civilian employee of the Department of the Navy appointed to a critical sensitive or special sensitive position.The Command Security Manager (B054) will be contacted for assistance.

6004. SECURITY MANAGERS. Security Managers must have a favorably adjudicated SSBI or PR completed within the past 5 years, Security Managers in this sense means at the Command level, e.g., Battalion or Company. While division and branch Secondary Control Points do provide input, actual recommendations for adjudication decisions are normally at the Command level through Command Security Managers.

6005. ELECTRONIC INVESTIGATION PROCESSING (e-QIP) DIRECT. e-QIP is the Federal government standard automated request tool for PSI; e-QIP direct is an Office of Personnel Management sponsored program in support of the e-government, e-clearance initiative. E-QIP direct allows applicants to electronically enter, update, and transmit their PSI data over a secure internet connection to their employing agency or security management office for review and approval in conjunction with the PSI request. Within Department of Defense, e-QIP direct has replaced the Electronic Personnel Security Questionnaire and the hard copy Standard Form 86, “Questionnaire for National Security Positions.”

6006. MAINTAINING QUESTIONNAIRE INFORMATION

1. If an individual refuses to complete a required PSI after being advised of the effect of the refusal, the PSI will be terminated and appropriate reporting procedures followed.

2. When an individual is separated, transferred, or no longer needs an investigation, notify the Command Security Manager so that the investigation can be canceled and local records can be closed.

PERSONNEL SECURITY PROGRAM

CHAPTER 7

PERSONNEL SECURITY DETERMINATIONS

7000. BASIC POLICY. Guidance concerning personnel security determinations such as security clearance eligibility and assignments to sensitive duties is contained in Chapter 7 of reference (b).

7001. RESPONSIBILITIES. The authority to determine access to classified information aboard Marine Corps Base, Quantico and subordinate activities serviced by inter-service support agreements is vested in the individual Command Security Managers. The Command Security Managers will:

1. Administer security clearance eligibility actions and access to classified information for all assigned personnel on behalf of their Commanders.

2. Request Personnel Security Investigation (PSIs) as appropriate.

3. Grant temporary clearance and access per paragraph 9-4 of reference (b).

4. Maintain a personnel security file on all cleared personnel to include a record of security briefings and record of clearance and access determinations.

5. Certify security clearance eligibility and access (*visit request*) for visiting personnel per chapter 11 of reference (b).

6. Administratively withdraw access and update Joint Personnel Adjudication System (JPAS)/Secondary Control Point (JCAVS) when an individual's requirements for access to classified information no longer exist. Ensure debriefing statements are completed by activity Security Assistants and forwarded to the Command Security Manager, when JPAS/JCAVS owned persons retire or leave Federal service.

7. Authorize and limit access according to requirements, lower access authorized, when appropriate.

8. Continuously evaluate command personnel with regards to their eligibility for access to classified information by

applying the standards contained in appendix G of reference (b). Notify the Department of Defense Central Adjudication Facility (DODCAF) when potential disqualifying information is known or discovered.

9. The command security managers office (only), will coordinate unfavorable personnel security determinations concerning personnel assigned to the various commands and direct personnel to command assistance programs as appropriate. Assist affected personnel by explaining the personnel security determination process; provide personnel with the instructions provided with the Letter Of Instruction (LOI), Letter Of Notification, and Personnel Security Appeals Board notification letters.

10. Deny access and/or restrict admittance to command areas as deemed appropriate when disqualifying information regarding an individual from another activity is revealed. Ensure the individual's parent command, agency or facility is notified of your action, to include the basis for the denial.

7002. ADJUDICATIVE MATTERS

1. In view of the significance that each adjudication decision can have on a person's career, and to ensure the maximum degree of fairness and equity in these actions, the Command Security Manager and Battalion Commanding Officers/Security Managers will ensure compliance with the guidelines as set forth in paragraph 7-3 of reference (b).

2. Local reviews of PSIs will be conducted by a security specialist 0080/GS-09 and above or military officer/Security Manager acting on behalf of the commanding officer. Note: Security Managers are not adjudicators.

7003. PERSONNEL SECURITY DETERMINATION. Commanding officers, the Office of the Staff Judge Advocate, Security Officer, Provost Marshall, Substance Abuse Officer, Director of Human Resources, managers and supervisors will ensure that questionable or unfavorable information is made available to the Command Security Manager in the performance of his duties in making Personnel Security determinations in accordance with paragraph 7-4 of reference (b).

7004. FACILITY ACCESS DETERMINATIONS (FAD) PROGRAM. Chapter 7 of reference (b) provides guidance concerning contractor employees.

7005. UNFAVORABLE DETERMINATION PROCESS

1. Unless otherwise directed, unfavorable personnel security determinations from and responses to the DON CAF will be processed and initiated by the Command Security Manager. Commanding officers, division directors and the Director of Human Resources will be kept informed on any actions taken with regards to personnel under their administrative jurisdiction.

2. LOI and other actions will be processed in such a manner as to ensure all deadlines are met and that the individual receives due process.

3. The Special Security Officer (SSO) may process a LOI for those personnel having Sensitive Compartmented Information access but will keep the Command Security Manager informed of the actions taken. This includes copies of correspondence, SF-86 and other correspondence documenting security actions taken.

7006. APPEALS. Appeals and Personnel Appearances resulting from a LOI will normally be coordinated through the Command Security Manager. The Command Security Manager’s act as the single focal point for the subordinate and tenants commands with outside agencies such as DOD CAF, Defense Security Service (formerly Defense Investigative Service) and the Office of Personnel Management.

7007. PERSONNEL SECURITY ACTIONS. When the DON CAF determines an unfavorable Personnel Security Action, the Command Security Manager/SSO will, based upon the DOD CAF guidance,

1. Deny or revoke security clearance eligibility.

2. Deny or revoke special access authorization.

3. Deny or revoke assignments to sensitive duties.

7008. CONTRACTOR ELIGIBILITY. Refer to paragraph 7-10 of reference (b) for guidance on contractor eligibility under the National Industrial Security Program.

PERSONNEL SECURITY PROGRAM

CHAPTER 8

UNFAVORABLE ELIGIBILITY DETERMINATIONS AND RESTRICTIONS

8000. BASIC POLICY. Policy and guidance for the processing of security clearances is contained in chapter 8 of reference (b).

8001. CLEARANCE PROHIBITIONS. In addition to the prohibitions contained in paragraph 8-3 of reference (b), clearances will not be requested for:

1. Persons pending legal action.

2. Mail Orderlies.

3. Permanent access when temporary access will do.

8002. RECORDING CLEARANCES

1. Department of Defense, Central Adjudication Facility (DOD CAF) certification messages are no longer provided. Commands will consult Joint Personnel Adjudication System (JPAS) to determine when investigations are completed and when DOD CAF adjudication is concluded. Commands must ensure they have properly registered (joined) the persons under their control Security Management Office in JPAS so they receive pertinent information and notices. The JPAS is the system of record for all Department of Defense clearance and access determinations.

2. The Command Security Manager grants access on behalf of the Commander, commanding officers will ensure that all accesses granted to individuals under their control were properly and promptly recorded in JPAS. The Command Security Managers office is accountable for the system administration and account creation for JPAS users within the command. JPAS user accounts will be kept to those necessary for mission accomplishment.

8003. UNIQUE SECURITY CLEARANCE REQUIREMENTS

1. Every commanding officer must have a favorably adjudicated Single Scope Background Investigation (SSBI) and access

equivalent to the highest level of classified information maintained at the command. Commanding officers will review the records of prospective subordinate commanding officers to ensure that this requirement is met. When the prospective commanding officer does not have the appropriate security clearance, an SSBI will be initiated prior to assuming command.

2. Navy and reserve personnel security clearances will be coordinated through the Command Security Manager.

3. Security investigation requirements for consultants and direct hire personnel in support of government contracting activities will be processed by the Facility Security Officer (FSO).

8004. CLEARANCES UNDER THE NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP)

1. Normal circumstances dictate that the contractor's Facility Security Officer (FSO) process contractor clearances. However, when questions arise, the Command Security Manager will act as the focal point to resolve security clearance issues.

2. Adverse or questionable information which concerns a cleared contractor employee assigned to a worksite under the control of Marine Corps Base, Quantico or one of its subordinates will be reported to the Command Security Manager who in turn will report action taken to the FSO and Defense Industrial Security Clearance Office. The Command Security Manager will keep the Special Security Officer (SSO) informed when Sensitive Compartmented Information (SCI) is involved.

8005. CLEARANCE WITHDRAWALS OR ADJUSTMENTS

1. Although clearances remain in effect, Division Security Managers will debrief their personnel having been granted access upon transfer. The debriefing form (Figure 9-5) provided by the Office of the Command Security Manager will be used for this purpose. In turn, this action will alert security personnel to remove the individual from base access rosters and update their JPAS/JCAVS information as appropriate. (OPNAV 5511/14 Security

Termination Statement is used by Commands upon separation and is completed by Instillation Personnel Administration Center personnel).

2. The administrative withdrawal or downgrading of a security clearance or access is not authorized when prompted by developed derogatory information. On recommendation by the Commanding Officer, the Command Security Manager may suspend the individual's access for cause and will report the suspension and/or the derogatory information to the DOD CAF. The suspension of access must be accomplished in accordance with paragraph 9-7 of reference (b). The SSO will coordinate this action when SCI access is at issue.

8006. DENIALS OR REVOCATION OF A SECURITY CLEARANCE

1. The DOD CAF grants and revokes all security clearances. The Command Security Manager is responsible for ensuring that the DOD CAF is apprised of any information that suggests an individual should have his clearance denied or revoked, and will act as the focal point in these matters, whereby ensuring that due process is given to all personnel affected under the continuous evaluation program.

2. Commanding Officers, Provost Marshall Office, Office of Staff Judge Advocate, Certified Substance Abuse Counselors and Human Resources and Organizational Management personnel will provide adverse information upon request to the Command Security Manager in the performance of his duties in implementing the Commands continuous evaluation program.

3. The Command Security Manager has cognizance over a Letter of Intent, Letter of Decision, and correspondence from the Personnel Security Appeals Board. Security related information that affects clearance eligibility and access or disqualifying information contained in Appendix G of reference (b) will be turned over to the Command Security Manager to ensure that proper procedures and follow up responses are completed in the times prescribed.

PERSONNEL SECURITY PROGRAM

CHAPTER 9

ACCESS TO CLASSIFIED INFORMATION

9000. BASIC POLICY

1. Access to classified information will be limited to the minimum number of individuals necessary to accomplish the mission and will be based upon “need to know”. Level of access will be restricted to the minimum level required. Per paragraph 9-1 of reference (b), no one will be granted access based upon rank, position, or clearance level alone.

2. If not previously recorded, A Classified Information Non-Disclosure Agreement SF 312 will be executed and recorded in Joint personnel Adjudication System (JPAS) by all persons requesting access.

3. Command/Division Security Managers will ensure that personnel under their jurisdiction are briefed in accordance with paragraph 4-5 of reference (b) prior to granting access.

9001. GRANTING ACCESS TO CLASSIFIED INFORMATION

1. The Commander has ultimate authority over those who have access. However, it is the servicing Special Security Officer (SSO) and the Command Security Manager who must implement the process to ensure fairness, uniformity of the program and due process. It is extremely important that they work as one.

2. Access involving Sensitive Compartmented Information issues may be granted per paragraph 9-3 of reference (b). The SSO must include the Command Security Manager in the administrative aspects of the program. Copies of clearance certifications, denials, and revocations must be forwarded to the Command Security Manager so that access rosters, security records and other matters are promptly updated.

9002. REQUESTING ACCESS

1. The Commander, Marine Corps Base, Quantico (MCBQ) (B 054) is responsible for the security of classified information and materials within the jurisdiction of his command and will grant

access to classified information to individuals who have an official “need to know” and meet the eligibility requirements with no known disqualifying information.

2. The authority of the Commander, MCBQ (B054) and its subordinate commands to grant access to classified information is subject to the restrictions as set forth in chapter 9 of reference (b).

3. Personnel requesting access to buildings, meetings, or spaces aboard MCBQ must submit visit request to the appropriate command SMO code. The visit request must be processed through your command security office and is required to identify a point of contact at the location to be visited. The point of contact is necessary to validate the need for access and for establishing escort requirements. Additional details may be required as the need for particular need to know is determined.

9003. TEMPORARY ACCESS

1. The Command Security Manager will grant temporary access for MCBQ and Inter-Service Support Agreement (ISSA) tenant activity personnel on a case-by-case basis based upon the guidance set forth in paragraph 9-4 of reference (b).

2. All temporary access requests require a submitted or open PSI for the security level requested and after a favorable review of the SF 86.

3. The Command Security Manager will withdraw temporary access upon receipt of a Letter of Intent in accordance with paragraph 9-4, 6, of reference (b).

4. Any person pending due process of a reported incident or a pending re-adjudication determination action from a previous incident by the Department of Navy Central Adjudication Facility will not be granted temporary access at any level.

9004. TERMINATION OF ACCESS. Paragraph 4-12 of reference (b), MCBQ and subordinate commanders will provide notification of any access termination by completing and submitting the Termination Statement form provided in (figure 9-4) to the Commander, MCBQ (B 054).

9005. INVESTIGATION. Should a request for access reveal the need for an investigation or reinvestigation, a request for access is placed in abeyance until such time a new investigation has been submitted to Office of Personnel Management. Temporary access may be authorized.

9006. ACCESS ROSTERS. Your Security Manager's Office maintains real-time military, civilian, and visitor access through the JPAS/JCAVS system of record. Clearance eligibility and access of persons listed therein have been verified and are approved for access at the level indicated for all organizations under the purview of the Commander, MCBQ and ISSA Tenants. The final approval and need- to-know requirement rests with the leadership of the visited organization.

9007. SUSPENSION OF ACCESS

1. When questionable or unfavorable information becomes available concerning an individual who has previously been granted a clearance/access, the Command Security Manager will advise the Commander if temporary removal of access or suspension of access is warranted for final determination by the Commanding Officer. Suspension of access for cause may only be used as a temporary measure until such time the individual's eligibility for access has been resolved by the DON CAF. Suspension of access will be based upon the criteria as set forth in paragraph 9-7 of reference (b).

2. When effecting suspensions of access, Commanding Officers, working with the Base Security Manager must:

a. Comply with the provisions of paragraph 4-11 and 9-6 of reference (b) for debriefing (figure 9-5).

b. Notify the Commander, MCBQ (B 054), division director, or activity head of the suspension actions taken against the individual under their charge.

c. Take steps to ensure that the individuals name is removed from all local access rosters, and that co-workers are notified of the limitations of suspensions.

d. Ensure the combinations to classified storage containers to which the individual has access are changed.

e. Post a notice of suspension of access in the individual’s personnel file, pending resolution of the individual’s eligibility status.

9009. ACCESS TO AND DISSEMINATION OF RESTRICTED DATA (RD) INCLUDING CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)

1. Access to RD/CNWDI will be processed by the Command Security Manager in accordance with paragraph 9-19 of reference (b).

2. Request for access to RD at other Department of Energy (DOE) facilities will be made utilizing the DOE Visit Request Form 5631.20, Request for Visit Approval or Access Approval. Activity Security Managers may prepare the form for signature of the Command Security Manager or Assistant Security Manager, who are the Department of Defense (DoD) certifying officials identified in DoD 5210.2.

PERSONNEL SECURITY PROGRAM

CHAPTER 10

CONTINUOUS EVALUATIONS

10000. BASIC POLICY. Commanding officers/directors and their Security Managers are responsible for establishing and administering a program of continuous evaluation to ensure that personnel with clearance eligibility and access, and those that are assigned to sensitive positions are an acceptable security risk. Under this program, they must establish internal channels for reporting information reflecting on an individual's loyalty, reliability, judgment, and trustworthiness, so that it may be assessed from a security perspective. There should be a complete understanding by the personnel officer, security officer, security manager, legal officer, medical officer, certified substance abuse counselors officer, and supervising personnel that information which places an individual's loyalty, reliability, judgment and trustworthiness in question must be evaluated for a security standard. They should be familiar with the continuous evaluation check sheet (Exhibit 10A) of reference (b) and the adjudication guidelines contained in appendix G of reference (b), and alerted that bad behavior indicating unexplained affluence, financial instability, alcohol and drug abuse, mental or emotional instability, or criminal conduct is potentially significant to an individual's security status. Activities should act to identify problem areas at an early stage and to direct personnel to programs designed to counsel and assist them when they are experiencing financial, emotional or medical difficulties.

10001. PERFORMANCE EVALUATION SYSTEM. Security Managers, security specialists, and all other personnel whose duties significantly involve the creating, handling or management of classified information, requires that the performance/rating system include the management of classified information as a critical element or job objective to be evaluated. Supervisors will comment on the continued security clearance eligibility of subordinates who have access to classified information in conjunction with regularly scheduled performance appraisals. Paragraph 10-4 of reference (b) contains specifics.

10002. COMMAND REPORTS OF LOCALLY DEVELOPED UNFAVORABLE INFORMATION

1. Co-workers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

2. When derogatory or questionable information is acquired on an individual who is eligible for or holds a security clearance or special access authorization or who is assigned to a sensitive position, it is forwarded to the Command Security Manager (B 054) who must reevaluate that individual's eligibility for access or assignment. Activity heads must make a determination upon initial receipt of credible derogatory information whether to suspend eligibility/access to classified information and/or continue assignment to a sensitive position and then notify the Commander, Marine Corps Base, Quantico (MCBQ)(B 054).

3. Supervisors will comment on the continued security clearance eligibility of subordinates who have access to classified information in conjunction with regularly scheduled performance appraisals. See paragraph 10-4 of reference (b) for guidance.

4. Patterns of foreign travel by cleared personnel, or their failure to report such travel in advance as required, may have counterintelligence implications. A report of such travel will be referred to the Commander, MCBQ (B 054).

10003. CONTINUOUS EVALUATION

1. When questionable or unfavorable information, as identified in appendix G of reference (b) becomes available concerning an individual who has been granted access to classified information or assigned to a sensitive position, commands will report that information to the Commander, MCBQ (B 054) for reporting to the Department of Defense Central Adjudication Facility (DOD CAF).

Commands will report all information, which meets the appendix F standards without attempting to apply or consider any mitigating factors that may exist. Use of exhibit 10A of reference (b) is encouraged to ensure that there is sufficient information upon which to base a determination.

2. If the Commander, MCBQ (B 054) determines that the developed information is significant enough to require a suspension of the

individuals access for cause, the suspension action will be accomplished in accordance with paragraph 9-7 of reference (b) using the proper administrative chain of command.

3. Sensitive Compartmented Information (SCI) access will be suspended by the Special Security Officer (SSO), Marine Corps Intelligence Activity per reference (a) and Director, Central Intelligence Directive regulations. The SSO will coordinate these activities with the Base Command Security Manager so that command records can be updated to reflect current status.

4. A command report of suspension of access for cause will automatically result in suspension of the individual's clearance eligibility by the DOD CAF. Once clearance eligibility is suspended (*or the individual is debriefed from SCI access for cause*), the individual may not be granted access or considered for re-indoctrination into SCI access until clearance eligibility has been reestablished by the DOD CAF.

5. The Command Security Manager will act as the "go between" in matters involving the DOD CAF, except in those instances where the SSO is required to go direct.

6. Subordinate Security Management Office (SMOs) to 300015 are responsible for coordinating with the Command Security Manager each case were incident reporting is required. Tenant commands are authorized to process incident reports and other continuous evaluation procedures with the assistance from the command security managers office.

PERSONNEL SECURITY PROGRAM

CHAPTER 11

VISITOR ACCESS TO CLASSIFIED INFORMATION

11000. BASIC POLICY

1. The term visitor applies as follows:

a. A visitor to Marine Corps Base, Quantico (MCBQ), its subordinate or its tenants is any person who is not attached to or employed by the activity or staff and is outside the realm of Security Management Office (SMO) 300015.

b. A person on temporary additional duty is considered a visitor. Personnel on temporary duty orders, reservist on active duty for training or those personnel assigned on a quota to a school or course of instruction are considered as visitors when not attached to this Command.

c. All cleared DoD contractor personnel are visitors.

2. Commanding officers and directors will establish procedures to ensure that only visitors with the appropriate security clearance level, access, and need-to-know are allowed access to classified information. If a visitor escort is required, a properly cleared and trained military, civilian or a contractor (*CAC privileged*) assigned to the command may be used. The activity receiving the visitor is responsible for ensuring that the visitor has proper identification. The preferred form of identification is a military, civilian or contractor card that positively confirms their official affiliation. Other acceptable forms will include a recent, recognizable photograph and legally given name of the bearer, e.g., state issued identification cards, or a valid driver’s license containing the above elements may be used. Report any attempt to gain access to classified information by persons using fraudulent identification to the Security Manager (B 054), or to the Naval Criminal Investigative Service (NCIS).

3. When commanding officers permit unclassified visits by the general public, a written statement of command safeguards will be prepared and implemented to address the possibilities of the presence of foreign agents among the visitors.

11001. VISIT REQUEST

1. All visit requests to SMO 300015 MCBQ will be in compliance with paragraph 11-2 of reference (b). Outside Department of Defense (DoD), and special access requests, should be addressed to the Commander, MCBQ, (B 054) attention Visitor Control. In all cases, it is extremely important that visit requests contain the name of the activity to be visited and the Point of Contact at the visit location so that the Command Security Manager can process the request in a timely fashion. Commands with subordinate SMO codes to 300015, are authorized to grant access. A subordinate SMO to 300015 or tenant/ISSA organizations can contact the Command Security Manager's Office for exemptions to this policy.

2. The SSO is located within the MCIA organization and serves as a tenant command aboard MCB, Quantico. The SSO does not process collateral visit requests for MCBQ. Please do not submit visit requests through back channels unless they are SCI related and require SSO interaction.

3. Visitor clearance procedures discussed in this chapter should not be confused with area clearances required for entrance into a foreign country.

4. Under no circumstances will personnel hand carry their own visit requests to the places being visited. Orders are hand carried and do not contain the required information, therefore orders cannot be used in lieu of visit requests.

5. Receipt of a fraudulent visit request will be reported to the nearest NCIS office and to the Command Security Manager (B 054).

6. Visits involving access to and dissemination of Restricted Data, or to facilities of the Department of Energy, are governed by the policies and procedures in DoD Directive 5210.2, Access to, and Dissemination of Restricted Data, 12 Jan 78 (NOTAL). The Base Security Manager's Office will sign, U.S. Department of Energy, Requests for Visit or Access Approval Form DOE F 5631.20.

7. Visits involving access to and dissemination of SCI are governed by the SSO, MCIA, and the procedures contained in central intelligence directives.

8. All visit requests involving DoD personnel will be submitted via Joint Personnel Adjudication System (JPAS). When JPAS is not available, a last resort visit request, may be transmitted by facsimile, message or by electronic mail, the visit request must be on official letterhead stationery. OPNAV form 5521/27 may also be used provided it is completed in its entirety.

11002. FOREIGN VISITS

1. SECNAVINST 5510.34, Manual for the Disclosure of Department of the Navy Military Information Foreign Governments and International Organizations, 4 Nov 93 (NOTAL) and references (a) and (b) provides guidance on Foreign Nationals and representatives of foreign entities.

2. Foreign visits are handled through the G-3 Command Visitor Control Coordinator MCBQ or the Protocol Officer, Visitor Control Coordination Center, MCCDC. Visitor Control will coordinate visits involving technical discussions or the disclosure of classified material through the Command Security Manager to ensure approval of these visits by the Navy International Programs Office, the Commandant of the Marine Corps and the Naval Criminal Investigative Service in matters involving security issues.

3. Except during general visiting, activities are required to maintain a record of all visits by foreign nationals, or by U.S citizens or immigrant aliens representing foreign governments, military services or private interests. The record will comprise the name and signature of the visitor, nationality, title, office and sponsor of the visitor, clearing authority if the visit includes disclosure of classified information, the date and duration of the visit and the name of the escort, if used. Retain these records for 2 years.

11003. VISITS TO FOREIGN COUNTRIES

1. Commanding officers and directors proposing sponsorship of an Official Visit to a foreign country will note the requirements of Chapter 11 of reference (b).

2. Visits to foreign countries in which classified information is involved will be coordinated through the Commander, MCBQ, Command Security Manager (B 054).

3. Foreign Travel Briefs will be conducted by NCIS. Level 1 force protection briefs will be given as required.

Part II INFORMATION SECURITY

PROGRAM CHAPTER 1

INTRODUCTION TO THE INFORMATION SECURITY PROGRAM (ISP)

1000. BASIC POLICY. The Marine Corps Base Quantico (MCBQ) Information Security Program is established in compliance with Marine Corps Orders and the Department of the Navy (DON) program to ensure that information classified under the authority of Executive Order 13526 is protected from unauthorized disclosure. The ISP applies uniform, consistent, and cost-effective policies and procedures to the classification, safeguarding, transmission and destruction of classified information. Part II of this Order also provides guidance on security education and the industrial security program. The term "classified information" is used throughout this Order to describe classified material in any matter or format, document, product, or substance on or in which classified information is recorded or embodied, including classified information that resides on classified Information Technology systems.

1001. AUTHORITY

1. The Commander, MCBQ is responsible for establishing and maintaining an ISP in compliance with references (a) through (e).

2. The responsibility for the security and proper handling of classified material extends directly to the individual having knowledge or possession of such material and to activity heads within whose purview classified material is utilized.

3. Individual requests for guidance or interpretation of this publication should be addressed to the Commander, MCBQ, (B 054). Attn: Command Security Manager.

1002. APPLICABILITY

1. This Order establishes coordinated policies for the security of classified information, incorporating the policies of numerous DoD/DON/HQMC directives. It is not expected that these

directives will or can ensure absolute security at this Base. Rather, they permit the accomplishment of essential tasks while affording selected items of information reasonable degrees of security with a minimum risk.

2. As this Order establishes coordinated policies for maintenance of the ISP it is applicable to all organizations and activities under the purview of the Commander. References (c), (d), (e) and this Order will provide the basis for managing the ISP.

1003. RESPONSIBILITY FOR COMPLIANCE

1. Activity heads are responsible for compliance with and implementation of this publication within their activity.

2. Each individual, military, civilian or contractor, in or employed through the Navy or Marine Corps, is responsible for compliance with this Order in all respects.

3. All activities that hold, handle, or otherwise come in contact with classified information are required to register as a Secondary Control Point with the Classified Material Control Center and have on-hand and maintain hard copies of references (c), (d), (e) and this Order.

1004. SPECIAL ACCESS PROGRAMS (SAP). These programs will be handled per the guidelines contained in reference (b), reference (d), and other directives as required. The base Special Security Officer will act as coordinator for the SAP and sensitive compartmented information in cooperation with the Commander, MCBQ (B 054).

INFORMATION SECURITY PROGRAM (ISP)

CHAPTER 2

COMMAND SECURITY MANAGEMENT

2000. COMMANDING OFFICER

1. Terminology. "Command" is used as a generic term for any organizational entity and may include a base, station, unit, laboratory, installation, facility, center, activity, detachment, squadron, ship, etc. "Commanding Officer" is used throughout this regulation as a generic term for the head of any Department of the Navy (DON) command and includes commanding general, commander, commanding officer, director, officer in charge, department head, etc.

2. Responsibility and Authority. Commanding Officers are responsible for the effective management of the ISP within their command. Authority delegated by this regulation to a commanding officer may be further delegated unless specifically prohibited.

3. Standards. This regulation establishes baseline standards, but the commanding officer may impose more stringent requirements within the command or upon subordinates if the situation warrants. The commanding officer shall not, however, unilaterally establish requirements that impact on other commands or cleared Department of Defense (DoD) contractors, or that contradict this regulation or references (a) through (e).

4. Risk Management. Commands confront different environments and sets of changing operational requirements. Therefore, each commanding officer shall apply risk management principles to determine how best to attain the required levels of protection. Employing risk management results in command decisions to adopt specific security measures given the relative costs and available resources.

5. Implementation. The commanding officer shall designate, in writing, certain security personnel directly involved in program implementation (*see paragraphs 2001 and 2002*). Additionally, the commanding officer shall:

a. Approve a Standing Operating Procedure for the commands security operations to include the internal flow of classified material not specifically regulated by this Order,

e.g., all secret and confidential, message traffic, secret and confidential working papers as regulations dictate.

b. Approve an emergency plan that includes provisions for the protection and destruction of classified information in emergency situations (*see exhibit 2B of reference (d)*).

c. Establish and maintain a self-inspection program. This may include security inspections, program reviews, and assist visits to evaluate and assess the effectiveness of the command's ISP.

d. Establish an industrial security program when the command engages in classified procurement or when cleared DoD contractors perform classified work and operate within areas under the direct control of the commanding officer.

e. Apply risk management, as appropriate, for the safeguarding of classified information, and monitor its effectiveness in the command.

f. Ensure that the security manager and other command personnel receive training as required and support the command security education program.

g. Inform command personnel that they are expected and encouraged to challenge the classification of information which they believe to be improperly classified and ensure that procedures for challenging and appealing such status are understood.

h. Ensure that the performance rating systems of all DON military and civilian personnel, whose duties significantly involve the creation, handling, or management of classified information, include an objective on which to be evaluated.

2001. SECURITY MANAGER. Refer to Part I, paragraph 2002.

2002. OTHER SECURITY ASSISTANTS

1. Assistant Security Manager. Personnel so designated must be an officer, E-6, civilian GS-07 or above and have a security clearance eligibility and access equal to the level of their classified holdings, (*Appointed by, Commanding Officer/Acting/By*

direction). Assistant Security Managers take direction from the Activity Security Manager and provide support as needed.

2. Classified Material Custodian. Refer to Part I, paragraph 2003.

3. Security Assistant or Secondary Control Point (SCP) Custodian. Individuals performing administrative functions under the direction of the security manager must be a U.S. citizen and have security clearance eligibility and access equal to the level of their classified holdings to perform their assigned duties and tasks.

2003. INTER-SERVICE SUPPORT AGREEMENT (ISSA)

1. Specified information security functions may be performed for other commands via ISSA, or Memoranda of Understanding or, Memoranda of Agreement, or Security Servicing Agreement. Such agreements may be appropriate in situations where security, economy, and efficiency are considerations, including:

a. A command provides security services for another command, or the command provides services for a tenant activity,

b. A command is located on the premises of another government entity and the host command negotiates an agreement for the host to perform security functions,

c. A senior in the chain of command performs or delegates certain security functions for one or more subordinate commands,

d. A command with a particular capability for performing a security function agrees to perform the function for another,

e. A command is established expressly to provide centralized service (*e.g., Personnel Support Activity or Human Resources Office*), or

f. Either a cleared contractor or a long-term visitor group is physically located at a DON command.

2. The ISSA shall be specific and shall clearly define the security responsibilities of each participant. The agreement shall include requirements for advising commanding officers of any matter that may directly affect the security integrity of the command.

2004. INSPECTIONS, ASSIST VISITS, AND PROGRAM REVIEWS

1. Commanding officers are responsible for evaluating and documenting the security posture of their command and subordinate commands. These self-inspections may be conducted using the checklists provided in the Information and Personnel Security Database under the Personnel Security tab or they may focus on one functional area or discipline.

2. Inspections will be conducted by qualified personnel who will inquire into overall security management and procedures for classification management, accounting and control of classified information, physical protection of classified information, personnel security, and security education.

3. A qualified representative from the Command Security Managers Office (B 054) will augment the Base Inspectors Office as a Subject Matter Expert for Information and Personnel Security in support of CDCO 5040.2A as required, utilizing the automated inspection reporting system (AIRS) checklist.

4. One Information and Personnel Security Program spot inspection *(announced or unannounced)* will be conducted annually by the Command Security Manager's Office for each Secondary Control Point (SCP), using the checklist provided in the Security Branch Information and Personnel Security database under the Personnel Security tab and then "Annual Spot."

5. At the end of each workday, an end of the day security inspection will be conducted by each SCP, of workspace areas where classified material is used and stored, SCP security personnel will provide instructions to coworkers so that all classified material (*to include classified waste*) is accounted for and properly stored in approved security containers, and that all such containers are locked. Additionally, all doors and windows to the space will be secured. Standard Forms 701 and 702 (*Figures 7-6 and 7-7*) will be utilized to record the fact that the end of the day security inspection was conducted; the last person to leave the workspace at the end of each workday is responsible for the end of day security inspection. For standardization purposes, all forms will have weekends and holidays highlighted in yellow and completed in accordance with the examples given (*Figure 7-7 and 7-8*), also see paragraph

7008.

6. Security Branch personnel periodically conduct unannounced and sometimes after-hour inspections as an adjunct to existing security programs, and are conducted to advise the Commander and activity heads of real time security practices.

7. Prior to commencing unannounced after-hour inspections, security management specialists will identify themselves to the duty officer/activity representative and request that the duty officer enter in their log the names of the inspection party, time inspection begins and ends, and the results thereof. The duty officer will accompany the inspection party on their inspection. Security specialists conducting the above inspections have instructions to:

a. Open for inspection such furnishings as unlocked desks, cabinets, lockers, and other containers not designated for storage of classified information, which could lead to compromise.

b. Locate any classified material or information not properly safeguarded and retain for safekeeping. The duty officer will record the event in his/her official log.

8. Unannounced inspections conducted during normal working hours will be walk-through cursory examinations of office spaces to ensure that classified material is not left adrift or unattended and may also include the opening of security containers for content verification.

9. All inspection results will be recorded and forwarded to the activity head by the Command Security Manager.

10. Organizations are required to correct discrepancies as soon as possible for all reported infractions, and are required to have on-hand, all inspection report results and corrective action taken for the last calendar year.

INFORMATION SECURITY PROGRAM

CHAPTER 3

SECURITY EDUCATION

3000. BASIC POLICY. Commanding officers shall ensure that all personnel of their command with information security responsibilities receive the appropriate level of security training.

3001. RESPONSIBILITY. The Chief of Naval Operation (CNO)N09N is responsible for policy guidance, education requirements and support for the Department of Navy (DON) security education program, see Chapter 4 of reference (b) and Chapter 3 of reference (d) for detailed guidance concerning the execution of the DON Security Education Program.

3002. ADDITIONAL INFORMATION SECURITY EDUCATION. In addition to the security education requirements of references (b) and (d), specialized training is required for the following:

1. Original Classification Authority (OCA) and officials acting in their absence, on an annual basis (see Chapter 4, paragraph 4-6 of reference (d)). *NOTE: The Commander, Marine Corps Systems Command (COMMARCORSYSCOM) is the only OCA aboard Marine Corps Base, Quantico.*

2. Derivative classifiers (*see Chapter 4, paragraph 4-9 of reference (d)*), security managers, security specialists or any other personnel whose duties significantly involve the management and oversight of classified information.

3. Classified Material Custodians (*see Part I Chapter 4 paragraph 4002.b*).

4. Classified couriers (*see Chapter 9, paragraph 9-11.5 of reference (d)*).

5. Declassification authorities (*see Chapter 4, paragraph 4-19 of reference (d)*).

INFORMATION SECURITY PROGRAM

CHAPTER 4

CLASSIFICATION MANAGEMENT

4000. BASIC POLICY

1. Executive Order 13526 is the prime basis for classifying information except as provided in the Atomic Energy Act of 1954, as amended. In keeping with the policy of the Department of Navy (DON) to make available to the public as much information as possible concerning its activities, information at MCB, Quantico (MCBQ) will be classified only to protect national security.

2. Unnecessary or higher than necessary classification will be avoided. If there is reasonable doubt about the need to classify information, it shall not be classified. When there is reasonable doubt about the appropriate level of classification, safeguard the information as if it were classified at the higher level until an Original Classification Authority (OCA) makes a determination. This determination must be made within 30 days. (*Chapter 4, of reference (d)*)

3. Reference (d), mandates the reporting of specific statistical data from 1st and 2nd echelon commands in support of the DON requirement for oversight of the information and Personnel Security Program. Data will be gathered by all subordinate commands and organizations designated as a Secondary Control Point. Submit to the Command Security Manager (B 054) the information requested in Figure 4-1 that is relevant to your organization, not later than 30 September of each fiscal year.

4001. CLASSIFICATION DESIGNATIONS. Information which requires protection against unauthorized disclosure in the interest of national security must be classified in one of three designations: “Top Secret,” “Secret,” or “Confidential.” The markings “For Official Use Only” and “Limited Official Use” cannot be used to identify classified information, nor can you use modifying terms in conjunction with authorized classification designations, such as “Secret Sensitive.”

1. Top Secret is the designation applied only to information the unauthorized disclosure of which could reasonably be

expected to cause exceptionally grave damage to national security.

2. Secret is the designation applied only to information the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security.

3. Confidential is the designation applied to information the unauthorized disclosure of which could reasonably be expected to cause damage to national security.

4002. CLASSIFICATION GUIDANCE. A determination to originally classify shall be made by an OCA only. For a clearer understanding of OCA responsibilities consult Chapter 4 of reference (d).

4003. DERIVATIVE CLASSIFICATION

1. While original classification is the initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, derivative classification is the incorporating, paraphrasing, restating, or generating, in new form, information that is already classified, and the marking of newly developed information consistent with the classification markings that apply to the classified source. This includes the classification of information based on duplication or reproduction of existing classified information. An estimated 98 percent of the classified information produced is derivatively classified.

2. Derivative classifiers shall:

a. Observe and respect the original classification determinations made by the OCA (*and as codified in classified source documents and security classification guides*).

b. Use caution when paraphrasing or restating information extracted from a classified source document(s) to determine whether the classification may have been changed in the process.

c. Carry forward to any newly created information the pertinent classification markings.

d. Properly mark the new paragraphs and pages.

e. Where multiple sources is indicated as the derived

source, attach to your new document as a permanent record of sources, a document source listing from where each portion of classified information was extracted.

f. Make an appropriate declassification decision based on the source listing. Derivative classifiers cannot use Originating Agency Determination Required (OADR) unless one of their source documents was previously marked OADR.

4004. ACCOUNTABILITY OF CLASSIFIERS. Classifiers are accountable for the propriety of the classifications they assign, whether original or derivative. Those with Command signature authority must ensure that classification markings are accurate before they sign classified documents or approve classified material. Commanding officers may designate the organizational Security Manager as the approver of assigned derivative classifications.

4005. FOREIGN GOVERNMENT INFORMATION

1. Information classified by a foreign government or international organization retains its original classification level or is assigned a U.S. classification equivalent (*see exhibit 6c of reference (d)*) to that provided by the originator to ensure adequate protection of the information. Authority to assign the U.S. classification equivalent does not require original classification authority.

2. Foreign Government Unclassified and RESTRICTED information provided with the expectation, expressed or implied, that it, the source, or both are to be held in confidence shall be classified confidential. It may be classified at a higher level if it meets the damage criteria of paragraph 4-2 of reference (d).

4006. SYSTEMATIC REVIEWS

1. Systematic declassification review is the review for declassification of classified information contained in records that have been determined by the Archivist of the U.S. to have permanent historical value per Title 44, U.S.C. chapter 33.

2. The CNO (N09N) is responsible for identifying to the Archivist of the U.S. that classified DON information 25 years old and older which requires continued protection. This

includes records of permanent historical value exempted from automatic declassification under Section 3.3 of Executive Order 13526. In coordination with the DON OCAs, the CNO (N09N) has developed OPNAVINST 5513.16 to be used by the Archivist in declassifying DON information.

3. Information classified by the OCA will be declassified as soon as national security considerations permit. Chapter 4 of reference (d) refers. Decisions concerning declassification or downgrading must be based on the loss of sensitivity of the information with the passage of time or the occurrence of an event that permits declassification or downgrading. Authority to downgrade or declassify should not be confused with the administrative responsibility of a holder of classified information to downgrade or declassify it as directed by a classification guide, continued protection guidelines, or the instructions on a document.

4007. CONTINUED PROTECTION GUIDELINES. Continued protection guidelines in OPNAVINST 5513.16A will be used in reviewing 25-year-old classified information held by MCBQ activities. DON information that is 25 years old and is not identified in the guidelines as requiring continued protection will be declassified.

4008. REQUESTS FOR MANDATORY DECLASSIFICATION REVIEW. Requests for mandatory declassification review are distinct from requests for records made under the Freedom of Information Act (FOIA). Requests received for mandatory declassification review will be forwarded to the Commander, MCBQ (B 054) for action per Chapter 4 of reference (d). Requests received for records made under the FOIA will be forwarded to the Commander, MCBQ (B 013).

4009. DECLASSIFICATION, DOWNGRADING, AND UPGRADING

1. A thorough review of Chapter 4 of reference (d) should be made prior to the declassification, downgrading, and upgrading of classified material.

2. The following information will not make a Subject Matter Expert on all facets of Classification Management, but it will provide Action Officers with the necessary information to correctly fill out the “Declassify On” line on a derivatively classified document.

3. OADR has been NOT AUTHORIZED for use since 15 Oct 1995. X codes, X1 thru X8, have been NOT AUTHORIZED since 22 Sep 2003. OCAs who "own" the various Security Classification Guides (SCGs) we use are required to update their SCGs to reflect current policy of inserting a date or event within 25 years in lieu of the outdated OADR or X codes, but have not done so. We rarely see SCGs prescribing OADR, but several are still out there prescribing one of the X codes.

4. Described below are examples where X Codes are prescribed in an SCG or other classified source document.

a. Source document dated before 22 Sep 2003 and prescribes X1 thru X8 as the duration of classification: Mark all new derivatively classified documents, Declassify On: Source Marked (*enter applicable X Code*), Date of Source: (*as applicable*).

Example: Source document is a PowerPoint presentation dated 5 Jul 2000 and is marked "Declassify On: X4". Mark the new derivatively classified document "Declassify On: Source Marked X4, Date of Source 5 Jul 00."

b. SOURCE DOCUMENT DATED ON OR AFTER 22 SEP 2003 AND ERRONEOUSLY PRESCRIBES X1 THRU X8 AS THE DURATION OF CLASSIFICATION: Mark all new derivatively classified documents with "Declassify On: 22 Sep 2028". 22 Sep 2028 represents 25 years from the last possible legal use of the X1 thru X8 marking.

Example: Source document is a classified letter dated 12 Nov 2005 and is erroneously marked "Declassify On: X4". Mark the new derivatively classified document "Declassify On: 22 Sep 2028."

c. AN OCA'S SCG PRESCRIBES X1 THRU X8: Mark all new derivatively classified documents with "Declassify On: 22 Sep 2028," when a SCG prescribes X1 thru X8 as the duration of classification. This applies regardless of when the SCG was issued, as long as it is still an active guide. Again, 22 Sep 2028 represents 25 years from the last possible legal use of X Code duration markings.

Example: Source document is the operation enduring freedom (OEF) SCG of 28 Mar 2002. The subject matter selected within this SCG indicates X4 for Military Plans as the duration of classification. The OEF SCG still has not been

updated after 22 Sep 2003 by the OCA to

reflect the new declassification guidance of a date or event 25 years or less, and still prescribes X1 thru X8 declassification codes. Mark all new derivatively classified documents that cite the OEF SCG as the derivative source with, “Declassify On: 22 Sep 2028.”

(*Letter Head*)

5510
(*Section ID*)
(*Date*)

MEMORANDUM

From: Commanding Officer
To: Commandant of the Marine Corps (PS)

Subj: DEPARTMENT OF THE NAVY COMMAND SECURITY PROGRAM REPORT

Ref: (a) SECNAV M-5510.36
(b) MCO 5510.18B
(c) MCBO 5510.1C

Encl: (1) Document Sampling Form

1. In accordance with Chapter 2 paragraph 2-11.1 of reference (a) the following information is provided as required.

a. Total number of inspections conducted ___.

(1) (Command inspected)
(2) (Command inspected)
(3) Etc.,

b. Significant trends (positive and negative.)

c. Corrective actions and anticipated completion date if significant security weaknesses discovered. Significant weaknesses are defined as issues that have or could lead to a compromise of classified information or an unauthorized release of controlled unclassified information.

d. Challenges that prevent or hamper the management of the command's security program. These may include policy constraints, resource limitations, etc. If this is already mentioned in the items above, it need not be listed again.

e. Total number of security violations. This includes Preliminary Inquiries (PI) and Judge Advocate General Manual Investigations (JAGMAN).

(1) List the command in which the PI/JAG was conducted.

Fig 4-1.--Sample, Marine Corps Information and Personnel Security Program Annual Reporting Requirement Format

(2) Define whether the violation was an Electronic Spillage (ES).

(3) Etc.

f. Random sampling of originally and/or derivatively classified documents. This sampling will be conducted at various times throughout the fiscal year to ensure compliance with marking requirements in Chapter 6. Documents are defined in paragraph 6-1.4. Commands shall use enclosure (1) to document the marking sampling, to ensure consistency throughout the Department of the Navy. Note the Information Security Program Data Report (SF-311) collected annually and reported to the Information Security Oversight Office (ISOO) is a separate requirement. The requirement to conduct random sampling only applies to commands that have significant classification activity. Significant is defined as 100 or more documents created within the command. When Commands, create less than 100 documents, are encouraged, but not required, to conduct a sampling to assess compliance with marking requirements as a part of the command's annual security review. In addition to the information contained on enclosure (1), include a summary of results that includes, total number of documents sampled, percentage of each type of discrepancy outlined in enclosure (1), and actions taken to improve marking if there is an error rate of at least 20%. Separate the summary of documents as originally or derivatively classified.

g. Confirmation of requirement for training for Original and Derivative classifiers per reference (d) paragraph 3-3.1.a. through d.

(1) Include copy of OCA Indoctrination Letter if applicable.

(2) Describe training efforts to ensure derivative classifiers are trained in the requirements to classify and mark documents.

(3) Describe training program for individuals who are allowed to hand carry classified information.

Fig 4-1.--Sample, Marine Corps Information and Personnel Security Program Annual Reporting Requirement Format - Continued

Enclosure (1)

(4) Describe training program for declassification authorities, if applicable.

2. Point of Contact is.

SIGNATURE BLOCK

Fig 4-1.--Sample, Marine Corps Information and Personnel Security Program Annual Reporting Requirement Format - Continued

Enclosure (1)

INFORMATION SECURITY PROGRAM

CHAPTER 5

SECURITY CLASSIFICATION GUIDE

5000. BASIC POLICY

1. Security Classification Guides (SCG) serve both legal and management functions by recording Department of Navy (DON) original classification determinations made under Executive Order 13526 and its predecessor Orders. SCGs are the primary reference source for derivative classifiers to identify the level and duration of classification for specific information elements.

2. The DON Original Classification Authority (OCAs) listed in exhibit 4A of reference (d) are required to prepare a SCG for each DON system, plan, program, or project under their cognizance that creates classified information. Updates to exhibit 4A can be found on the Chief of Naval Operations (CNO) SCGs and shall be issued as soon as practicable prior to initial funding or implementation of the relevant system, plans, program, or project. In support of this requirement, the CNO (NO9N2) manages a system called the Retrieval and Analysis of Navy Classified Information (RANKIN) Program, which manages and centrally issues SCG for the DON OCA.

5001. PREPARING AN SCG. SCGs shall be prepared, in writing, in the format described in Executive Order 13526, and approved personally by an OCA who has both cognizance (*i.e., program or supervisory responsibility*) over the information, and who is authorized to originally classify information at the highest classification level prescribed in their SCG(s).

5002. RANKIN. The primary element of the RANKIN Program is a computerized database that provides for the standardization, centralized management and issuance of all DON SCGs. After approval by an OCA, SCGs are forwarded to the CNO (N09N2) RANKIN Program Manager, and entered into the RANKIN database. Additionally, the RANKIN Program Manager maintains historical files for all DON SCG. Classification guides are detailed in Chapter 5, paragraph 5-3 of reference (d).

5003. PERIODIC REVIEW OF SCG(s). OCA(s) are required to review their SCG(s) for accuracy and completeness at least every 5 years and advise the CNO (N09N2) of the results. Proposed changes to, and cancellations of, existing SCG(s) shall be sent to the CNO (N09N2) in the format described in OPNAVINST 5513.1E.

5004. CONFLICT BETWEEN A SOURCE DOCUMENT AND AN SCG. In case of apparent conflict between an SCG and a classified source document about a discrete item of information, the instructions in the SCG shall take precedence.

INFORMATION SECURITY PROGRAM

CHAPTER 6

MARKING

6000. BASIC POLICY

1. All classified information shall be clearly marked with the date and office of origin, the appropriate classification level and all required "associated markings" (*see reference (d), paragraph 6-7 for exceptions to this policy*). "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; and warning notices, intelligence control markings and other miscellaneous markings (*see reference (d), of paragraph 6-7 for guidance on the placement of associated markings*). The purpose of marking classified material is to inform the holder of the classification level, the degree of protection required, and to assist in extracting, paraphrasing, downgrading, and declassifying actions. All classified material must be marked in a manner that leaves no doubt about the level of classification assigned to the material, which parts contain or reveal classified information, how long the material must remain classified, and any additional measures necessary to protect the material.

2. Classified material will be physically marked, annotated, or identified as specified in Chapter 6 of reference (d).

6001. BASIC MARKING REQUIREMENTS

1. Marking requirements and the application of markings vary depending on the kind of material. For purposes of uniformity and to avoid redundancy, paragraph 6000 above is applicable.

2. Marking is required on all information technology (IT) systems and electronic media, including removable components that contain classified information. IT systems include any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. Electronic media includes Universal Serial Bus drives, flash

drives, pen drives, compact disks, scanners, videotapes, floppy disks, recordings, etc. IT systems that process classified data, in forms other than traditional documents, such as weapon, navigation, and communication systems also require appropriate marking.

3. Classification markings will be stamped, printed, or written in capital letters, larger than those used in the text document or conspicuously on other material, and, when practical, in the color red.

4. The word "document" is used generically throughout this Order not only because it describes the most common form of classified material, but to make explanations more tangible. Documents take many forms, including publications (*bound or unbound*), reports, studies, manuals, emails, briefing slides (*such as PowerPoint presentations*), etc. Some types of classified material such as correspondence and letters of transmittal, recordings, photographs, file folders, and electronic messages, such as naval messages, have special marking requirements as described in this Chapter.

6002. FILES, FOLDERS, OR GROUPS OF DOCUMENTS

1. When a file, folder, or group of classified documents is removed from secure storage, it must be conspicuously marked with the highest classification of any classified document it contains, with an appropriate classified document cover sheet attached.

2. The only document cover sheets authorized for use by activities at Marine Corps Base, Quantico are as follows:

a. Top Secret Cover Sheet, SF 703 - NSN 7540-01-213-7901.

b. Secret Cover Sheet, SF 704 - NSN 7540-01-213-7902.

c. Confidential Cover Sheet, SF 705 - NSN 7540-01-213-7903.

3. In addition, the following forms are to be used by all activities at this Base:

a. Security Container Information Form, SF 700 - NSN 7540-01-214-5372 (*Figure 6-1*).

b. Activity Security Checklist, SF 701 - NSN 7540-01-213-7899 (*Figure 7-6*).

c. Security Container Check Sheet, SF 702 - NSN 7540-01-213-7900 (*Figure 7-7*).

d. Security Container Maintenance Record Form, OF-89.

6003. TRANSMITTALS. When a transmittal document or endorsement is added to classified material, it must carry the highest classification of the information it transmits, and a statement showing the classification, if any, of the transmittal document standing alone. An unclassified letter, which transmits a classified document as an enclosure, would carry the classification of the enclosure and the notation, "unclassified upon removal of the enclosure."

6004. ELECTRONICALLY-TRANSMITTED MESSAGES. Mark classified messages as prescribed in paragraph 6-26 of reference (d), and portion marked as prescribed for other documents. Due to black ink used in preparing messages, red ink is encouraged for marking classified messages.

6005. CHARTS, MAPS, AND DRAWINGS. Mark overall classification at the top and bottom of each document. Add additional markings that are clear when the document is rolled or folded.

6006. REMOVABLE AUTOMATED INFORMATION SYSTEM (AIS) AND WORD PROCESSING STORAGE MEDIA

1. External Markings. Removable information storage media and devices, used with AIS systems and word processing systems must be labeled using color-coded labels (*Standard Forms 706, 707, 708, 709, 710, and 711 see page 6A-18 of reference (d)*) that indicate clearly the classification, and associated markings of the information they contain. Media and devices that store classified information recorded in analog or digital form and are generally mounted or removed by the users, or operators, include magnetic tape reels, cartridges, cassettes, removable hard drives, CD ROM disks, disk cartridges, disk packs, diskettes, thumb/flash drives, and magnetic cards, etc. Each IT system shall be marked to indicate the highest classification level of the information processed by the IT system and the

network to which it is, or has been connected. Regardless of the electronic medium all Top Secret, Secret and Classified North Atlantic Treaty Organization AIS storage devices will be controlled and accounted for in the Automated Security Control Program.

2. Internal Markings. AIS and word processing systems will provide for internal markings to ensure that classified information, which is produced or generated, clearly shows the classification and associated markings. The Chief of Naval Operations (N09N) may exempt existing systems when internal marking requirements cannot be met without extensive system modification. Procedures must be established, however, to ensure that users and recipients of the media or information are clearly advised as to the classification and associated markings.

6007. DOCUMENTS PRODUCED BY AIS EQUIPMENT

1. These documents will be marked as prescribed in paragraph 6-35 of reference (d).

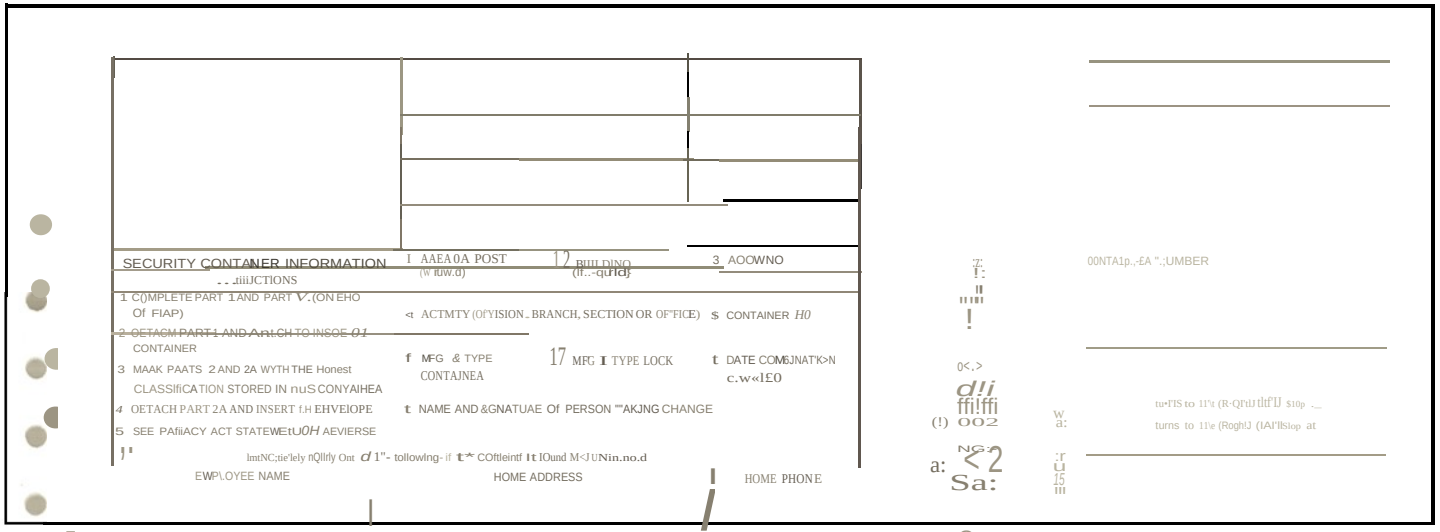
2. Mark documents produced on IT systems, to include emails generated on a classified IT system and those that function as word processing systems, in accordance with Chapter 6 of reference (d). Special provisions for marking some IT system generated classified documents are as follows:

a. Mark interior pages of fan-folded printouts with the highest overall classification level. These markings shall be applied by the system even though they may not be conspicuous from the text. Mark the face of the document with all required associated markings or mark them on a separate sheet of paper attached to the front of the printout.

b. Mark portions of printouts removed for separate use or maintenance as individual documents (*see exhibit 6A-22 of reference (d)*).

6008. STANDARD DOWNGRADING/DECLASSIFICATION MARKINGS. Mark this material in accordance with paragraph 6-10 of reference (d) and Chapter 4 of this Order.

6009. SECURITY DISCREPANCY NOTICE. When classified material is received which is improperly or incompletely marked, or which does not show proper downgrading or declassification information, the Command Security Manager (B 054) will in turn notify the sender of the material by utilizing OPNAV Form 5511/51, Security Discrepancy Notice (figure 6-2).



1. ATTACH TO INSIDE OF CONTAINER

>00-1o1 NSN 7540.012 14·5372

STANDARD FORM 700 (8·15) PriiCrld by CSA/1500 32 CFR 2003

2A INSERT IN ENVELOPE

SF 700 !8•8$) Pres.crlbed Dy GSA!ISOO 32 Cf R 2003

SECURITY DISCREPANCY NOTICE

FROM (Originating command) DATE

REF a. SECNAVINST 5510.36 (series) b. OPNAVINST 6610.1 SERIES
(Insert ref. (a))

ENCL

TO: (Forwarding command)

(Note - This form may be mailed in a window envelope.)

CLASSIFICATION

	BASIC CLASSIFICATION QUESTIONABLE		DOCUMENT SUBJECT MARKING		CHART, MAP OR DRAWING MARKING
	OVERALL MARKINGS		DOCUMENT TRANSMITTAL MARKING		PHOTO, FILM OR RECORDING MARKING
	PARAGRAPH/COMPONENT MARKINGS		MESSAGE MARKING		OTHER *(Specify)*

DOWNGRADING/DECLASSIFICATION

	CLASSIFICATION AUTHORITY NOT IDENTIFIED OR UNAUTHORIZED		DOWN GRADING DATA INCORRECT		DECLASSIFICATION (OR REVIEW) DATA OMITTED OR INCORRECT

OTHER *(Specify)*

Fold here with face of form in view

COMMENTS (Continue on reverse, if necessary)

COPY TO: N-0090 (WITH ADDRESSEE DELETED)

SIGNATURE TITLE

OPNAV 5511/51 (MAY 1980) This form replaces OPNAV 5511/B; 22 and 24 which are obsolete. Page 1 of 2 Pages

Figure 6-2.--Sample Security Discrepancy Notice OPNAV 5511/51

INFORMATION SECURITY PROGRAM

CHAPTER 7

SAFEGUARDING

7000. BASIC POLICY

1. To the extent possible, classified holdings will be consolidated to limit the areas where it will be used. The exact nature of open storage security requirements will depend on a thorough physical security survey of local conditions and circumstances provided by a Base Physical Security Specialist. Commanding officers shall ensure that classified information is processed only in secure facilities, on accredited Information Technology (IT) systems, and under conditions that prevent unauthorized persons from gaining access to it. This includes securing it in approved equipment or facilities whenever it is not under the direct control of an appropriately cleared person, or restricting access and controlling movement in areas where classified information is processed or stored. All personnel shall comply with the need-to-know policy for access to classified information and equipment.

2. In addition to safeguarding classified information, Commanding officers, directors, and activity heads shall ensure that controlled unclassified information (CUI) is safeguarded from unauthorized access by the public, and that measures are taken to protect IT systems that store, process, and transmit such information from unauthorized access.

3. Classified information is the property of the U.S. Government and not personal property. Military or civilian personnel, who resign, retire, separate from the Department of Navy (DON), or are released from active duty, shall return all classified information in their possession to the command from which received, or to the nearest DON command prior to accepting final orders or separation papers. Classified information provided to cleared contractor facilities (*Chapter 11 of reference (d)*) will be on a temporary loan basis only. Classified material may be retained beyond the expiration of the contract upon written request, not to exceed 1-year intervals. It will be returned in the same media format as received. Any loss or compromise will be reported to the Command Security Manager in accordance with Chapter 12 of reference (d).

4. Foreign national access to CUI shall be in accordance with SECNAVINST 5510.34A.

7001. RESPONSIBILITY

1. All persons granted access to classified material is responsible for safeguarding the material at all times and for its proper storage whenever the material will not be under the direct control of an appropriately cleared person. Holders of classified material must follow a procedure that ensures unauthorized persons do not gain access to classified material through visual or auditory means. Classified information will not be discussed or processed in common areas, work cubicles, elevators or places where un-cleared persons may be present.

2. Persons with access will not remove classified material from a designated office or working area except in the performance of official duties and under conditions providing the protection required by reference (b) and (d). Under no circumstances will a person remove classified material from designated work areas to work on it during off duty hours, or for any other purpose involving personal convenience without specific approval of the Commander, Marine Corps Base, Quantico.

7002. RESTRICTED AREAS

1. Do not designate a Secure Room (SR), for classified information and material in any way that would outwardly note their relative sensitivity. Identify any such area as a "Restricted Area." All designated restricted areas for classified information and material will be in writing by the Commander (B 054) in accordance with Chapter 3 of MCO P5530.14. Decisions regarding designations of restricted areas, their levels, and criteria for access are at the discretion of the commander.

2. Personnel permitted after hour access to classified work or storage areas will be required to sign in and out on a log sheet, with the exception of facilities that operate 24/7 or have implemented a level II access control system.

7003. CONTROL MEASURES

1. All Top Secret information in any format (*including copies*) originated or received by a command shall be continuously accounted for, individually serialized, and entered into the

Automated Security Control Program (ASCP) database. Any command with access to Top Secret information is required to have an appointed Top Secret Control Officer.

a. All hardcopy material classified secret, and secret information placed on mass media storage devices originated locally or received from other commands will be the only items entered into the ASCP database. This includes material coming in through official mail addressed to an activity or individual, material hand carried by personnel of this or other commands and organizations.

b. All controlled documents leaving the Classified Material Control Center (CMCC) to the Secondary Control Point (SCPs) will have with them two classified material control forms (*Figure 9-1*) that identify the document. One copy of the control form is to be signed and dated by the SCP, and retained as a receipt by the CMCC until that document appears on the next reported inventory. The second control form is for use by the SCP for their local accountability requirements. Document control forms are unclassified and may be reproduced locally.

c. The destruction of documents under ASCP control will be accomplished in accordance with Chapter 10 of this Order and reference (d).

2. Commanding officers, directors, and activity heads shall establish administrative procedures for the internal control of classified information (*including items controlled by the ASCP*) appropriate to their local environment, based on an assessment of the threat, location, and mission of their command. These procedures shall be used to protect secret and confidential information from unauthorized disclosure by access control and compliance with the marking, storage, transmission, and destruction requirements of this Order and reference (d).

7004. WORKING PAPERS

1. Secret and Confidential working papers include; original thoughts of the OCA/derivative classifier, classified notes from training courses or conferences, research notes, drafts, and similar items that are not finished documents and remain within the organization as a paper document or reside on the Secret Internet Protocol Router Network (SIPRNet) or other classified environments. Working papers that contain classified

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 page in letters larger than the text,

c. Protected per the assigned classification level, and

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

2. Top Secret Working Papers will be managed in accordance with paragraph 7-7 of reference (d).

3. Commanding officers, directors, and activity heads shall establish procedures to account for and control, all working papers in the manner prescribed for a finished document of the same security classification level when retained more than 180 days from date of creation or officially released outside the organization by the originator.

a. Classification marking of SIPRNet email and attachments will be in accordance with Chapter 6 of this Order and Chapter 6 of reference (d). Unlike the Non-classified Internet Protocol Router Network (NIPRNet), unclassified SIPRNet email and attachments **must** be plainly marked as “unclassified” prior to their removal from the SIPRNet regardless of the format used. If email and email attachments are not plainly marked, the Information removed will be marked as “tentative secret,” if North Atlantic Treaty Organization (NATO) information is present, it will be marked at the appropriate NATO classification level. The NATO control point officer located in the CMCC MCCDC is required to control all classified NATO documents received from all sources including the SIPRNet.

b. When SIPRNet email is classified secret or confidential, the classification level will be properly placed within the email and will include all associated warnings and intelligence control markings, all classified portions of the email will be marked per Chapter 6 of this Order and Chapter 6 of reference (d) prior to sending, printing or downloading.

c. If clarification is required on the overall classification of SIPRNet email or attachments, especially on missing portion markings, the originator of the information is the only authority that can clearly identify and mark/re-mark

any questionable information.

d. As well as the classification and portion marking, the originating source of the classified information must also be identified along with its appropriate declassification instructions (*refer to Chapter 4 and 5*). This also holds true where attached files are not plainly marked as unclassified. In the text of the email the sender must affirm that the classification of the attached file is in fact unclassified.

e. Further, all documentation identified in this category not conforming to the regulations provided will be considered a violation of security practices and will not be looked on favorably during inspections.

7005. **SPECIAL TYPES OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION**. If necessary control and safeguard classified SPECAT and controlled unclassified types of information as follows:

1. NATO classified documents will not be intermingled with U.S. documents in storage containers. NATO documents may be filed in the same drawer of a security container with U.S. documents if they are segregated and clearly identified as NATO files. Control and safeguard NATO classified information (*including NATO Restricted*) in accordance with USSAN 1-07.

2. Control and protect all other special category information (e.g., FGI, RD, CNWDI, FRD, COMSEC, SAP'S NNPI, SBU, DEASI, and DoD UCNI) in accordance with Chapter 7, paragraph 7-7 of reference (d).

7006. ID CARDS AND BADGES. Activities using an ID/badge systems will comply with the provisions of OPNAVINST 5530.14C, bearing in mind that classified information will not be disclosed or released solely on the basis of a card or badge.

7007. CARE DURING WORKING HOURS

1. Keep classified information under constant surveillance by an authorized person at all times. When classified documents are removed from storage for working purposes, keep them face down or covered when not in use with classified material cover sheets, Standard Forms 703, 704, and 705 (*See Figures 7-1, 7-2*

and 7-3).

2. Classified discussions shall not be conducted in public conveyances or places that permit interception by unauthorized persons. Classified material (*including laptop computers*) may not be opened or read in any area where unauthorized individuals can see it. This security precaution is applicable to cubical workspaces without access controls being in place. Take particular care when there are visitors or maintenance personnel present. Escorts should alert fellow workers when visitors or workmen are in the area. Practice the need-to-know principle.

3. Protect preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, and all similar items containing classified information. Further protect this material by taking it to secondary control points for proper destruction immediately after they have served their purpose, or by giving them the same classification and safeguarding them in the same manner as the classified material they provided.

4. Protect computer printers having residual memory and typewriter ribbons, computer storage media, and other classified items according to their security classification level.

5. In a mixed working environment (*i.e., classified and unclassified*), Automated Information System (AIS) media used for processing or storing classified information shall be marked with an SF 706, 707, 708, 709, 710, 711, or 712 (SCI), as applicable. In a totally unclassified working environment, SF labels are not required.

7008. END-OF-DAY SECURITY CHECKS

1. Commanding officers, directors, and activity heads will require a security check at the end of each workday to ensure that all classified material has been properly secured. The SF-701 (*Figure 7-6*) will be used to record that check. The "item column" can be modified to meet command needs/requirements (*e.g., check STE Phone for KSV card, power off to coffee pot, shredder, etc.*).

2. Sample procedures for activity security checks are in Figure 7-6, those conducting security checks will ensure that:

a. Security containers have been locked. The Security

Enclosure (1)

Container Check Sheet SF 702, (*Figure 7-7*) will be used as the opening and locking record for all General Services Administration (GSA) approved security containers and vaults/secure rooms.

Appropriate entries will be made on a single line of the SF 702 each time a security container, vault or secure room is opened and locked in accordance with the SF 702 instructions (*Figure 7-8*). The form will be displayed on the outside of the container and will not be predated; however, all days of the month will be accounted for. On days that have no activity (*secure room or a container was not opened*), entries will be recorded as "**NOT OPENED;**" weekend and holidays will be highlighted in yellow with nothing entered unless the space was occupied during the weekend/holiday period or guard checks were made.

b. The contents of desks, wastebaskets, and other surfaces and receptacles containing classified material have been properly stored or destroyed.

c. Windows and doors have been locked.

d. All classified material is stored in the manner prescribed and that burn bags are properly stored or destroyed.

e. Security alarms(s) and equipment have been activated.

f. Check other items as directed (*i.e., STE phones (Card removed), power off on shredders, copiers etc.*).

3. The SF 701 and SF 702 forms will be retained for a period of 1 month from the date of the last entry, or indefinitely if used as part of a Preliminary Inquiry (PI) or Judge Advocate General Manual Investigations.

7009. SAFEGUARDING DURING VISITS. Commanding officers, directors, and activity heads shall establish procedures to ensure that only visitors with an appropriate clearance level are granted access to classified information. At a minimum, these procedures shall include verification of the identity, clearance eligibility, and access level using Joint Personnel Adjudication System to verify that there is a current visit request; the need-to-know principle applies to all visitors. Refer to Part I, Chapter 11 and reference (b) for visit procedures.

7010. SAFEGUARDING DURING CLASSIFIED MEETINGS

1. Classified information will not be disclosed at conferences, symposia, exhibits, conventions, seminars, or other gatherings (*hereafter called meetings*) unless disclosure of the information serves a government purpose and adequate security measures are taken to control access to the information and prevent its compromise. Classified meetings may only be held at a U.S. Government agency or a cleared DoD contractor facility with an appropriate Facility Security Clearance.

2. A meeting conducted or sponsored by any activity at this Base in which classified information will be disclosed must be held at a cleared facility and only after determining that:

a. Disclosure of classified information at a meeting is in the best interest of national security.

b. The use of conventional channels for dissemination of classified information will not accomplish the purpose of the meeting.

c. The location selected facilitates proper control and dissemination of classified information including secure storage.

d. Adequate access and security measures/procedures will be imposed.

e. Attendance will be limited strictly to those persons whose presence is considered necessary in the interest of national security.

f. All persons to be invited who are not cleared members of the Executive Branch of the government or cleared DoD contractor employees have been identified so Limited Access Authorizations or Foreign Disclosure Authorizations may be processed.

3. The center, base, or activity head sponsoring a meeting at which classified information is to be disclosed is responsible for ensuring that visit requests for attendees have been processed prior to conducting the meeting. The center, base, or activity point of contact will coordinate with the Command Security Manager (*Visitor Control*) to verify access eligibility of attendees.

4. Marine Corps and Navy personnel at this Base must have the

approval of their division directors/commanding officers to disclose classified information at meetings conducted by or under security sponsorship of other bases or agencies of the Executive Branch of the government.

5. Marine Corps or Navy commands conducting or providing security sponsorship for classified meetings must ensure that:

a. Areas in which classified information is to be discussed afford adequate security against unauthorized access.

b. Adequate storage facilities are available.

c. Each person attending has been authorized access to information of equal or higher classification than the information being disclosed.

d. Admittance is limited to those on an approved access list and then only upon proper identification. Strict compliance with this requirement is especially critical when a classified meeting has been announced publicly.

e. The use or presence of wireless electronics is prohibited, cordless microphones and public address systems will not be used. The audio level of wired systems will be kept at the lowest possible attenuation level. In instances where audio systems and non electronic assisted speaking can be monitored from outside the confines of the meeting space, the space will not be used for classified discussions.

6. Each person who is to disclose classified information must be notified of the security limitations that must be imposed because of:

a. The level of access authorized for all attendees.

b. The “Need-to-know" of attendees.

c. Physical security conditions.

d. Provisions have been made to control and safeguard classified material given to those attending and to retrieve the material or effect transfer of control through approved methods.

e. Sessions are monitored to ensure discussions are limited to the level authorized.

f. Classified notes received or taken will be controlled in accordance with paragraph 7004 of this Order.

7. A person who is neither a cleared member of the Executive Branch of the government nor a cleared DoD contractor employee cannot attend a classified meeting sponsored by a Navy or Marine Corps command without approval by the Chief of Naval Operations (N09N2).
Authorization must be obtained before issuing an invitation.

8. All study groups being formed aboard this Base, to include HQMC activities will coordinate with the Commander, Marine Corps Base, Quantico (MCBQ) (B 054) prior to utilizing classified material. A 30-day period is required for security planning purposes when extended or non- routine support is requested.

9. Compromising emanations inspections and technical surveillance countermeasures inspections are mandatory for study groups utilizing Top Secret material, and when Secret material Is discussed on a continuous basis within the study group area. Technical surveillance countermeasures support is requested in accordance with SECNAVINST 3850.4.

10. Individuals assigned to any study group who will utilize any classified material will be placed on the MCB Access Rosters. The granting of temporary Top Secret clearance to gain access to Top Secret material is discouraged.

11. MCBQ Orders and applicable security directives will be used and followed by study groups.

12. In the event it becomes necessary to provide temporary storage of classified material after normal working hours, both MCB and MCCDC duty personnel have access to after hour recall numbers for command security personnel.

7011. <u>INVENTORY OF CLASSIFIED MATERIAL</u>

1. A change of custodian inventory must be conducted and submitted to the Information Security Officer at the CMCC, upon relief of an SCP custodian. When feasible, the incoming custodian must complete and sign the inventory prior to the departure of the outgoing custodian but always prior to the assumption of the SCP account. The SCP Security Manager verifies the inventory, (*Figure 7-4*).

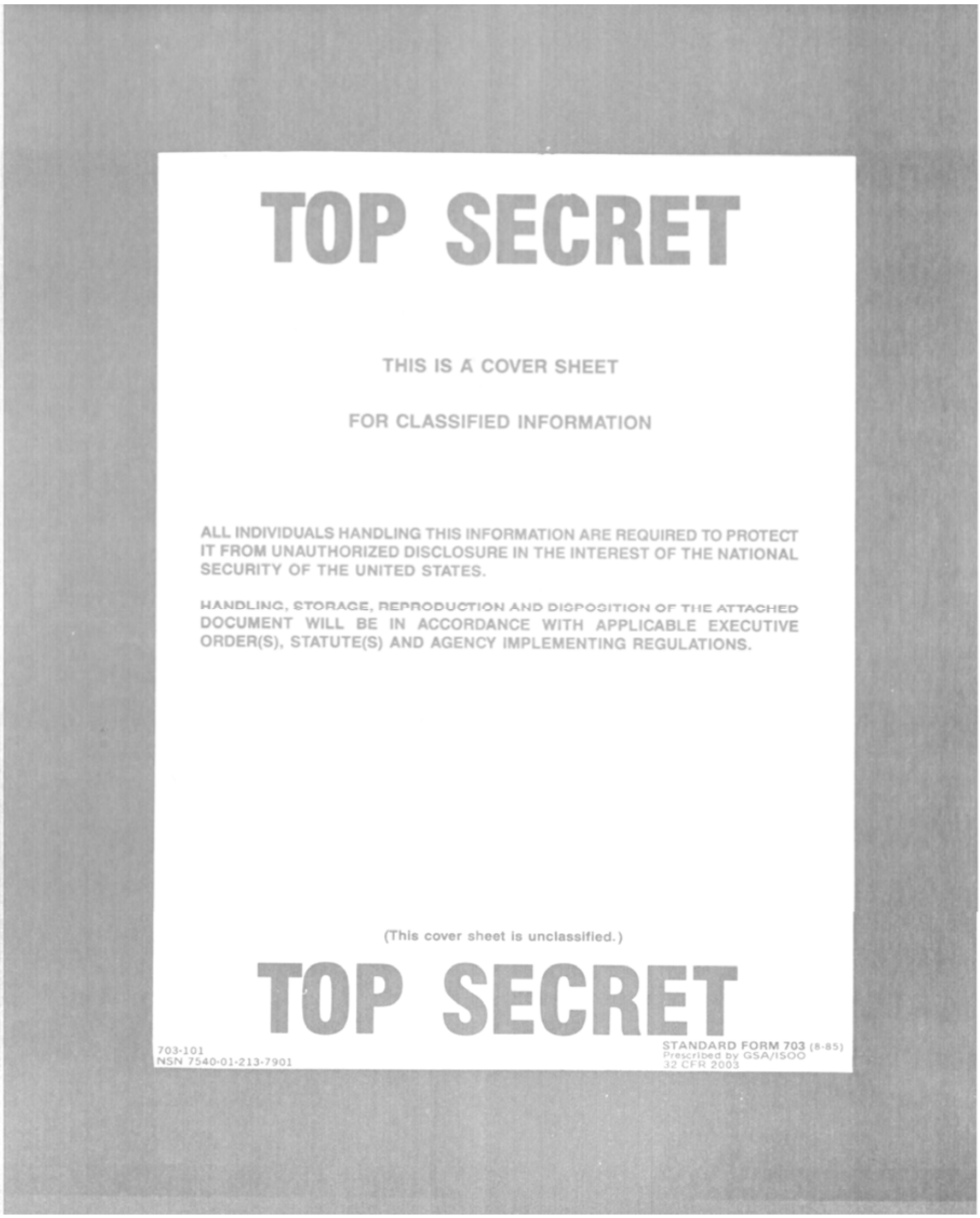
2. During the month of April all SCPs holding classified

material controlled by the CMCC will conduct an annual inventory. A locally printed inventory from the (ASCP) will be used to physically sight each controlled item held. The inventory will be verified by the SCP security assistant and submitted to the Head, CMCC, on or before the last working day in April, (*Figure 7-5*).

3. A random sampling inventory of controlled material on retention within an activity will be conducted annually during spot inspections by personnel from the CMCC; the inventory will be a physical sighting and examination of, or written evidence of proper accountability, destruction, transfer, etc. During these inventories, a random sample of documents will be audited to determine completeness, accuracy of markings, serial numbers (*bar codes*), declassification/downgrading instructions, and related control dates.

4. All inventories conducted by personnel from the CMCC, are based on the holdings listed in the Master Data Base of the ASCP.

7012. REPRODUCTION. The Information Security Officer located at the CMCC is the authorized agent for the reproduction of classified information. Classified information shall be reproduced only to the extent required by operational necessity unless restricted by the originating agency or for compliance with applicable statutes or directives. Only an authorized person having knowledge of reproduction procedures shall carry out the reproduction of classified information.



TOP SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT WILL BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

TOP SECRET

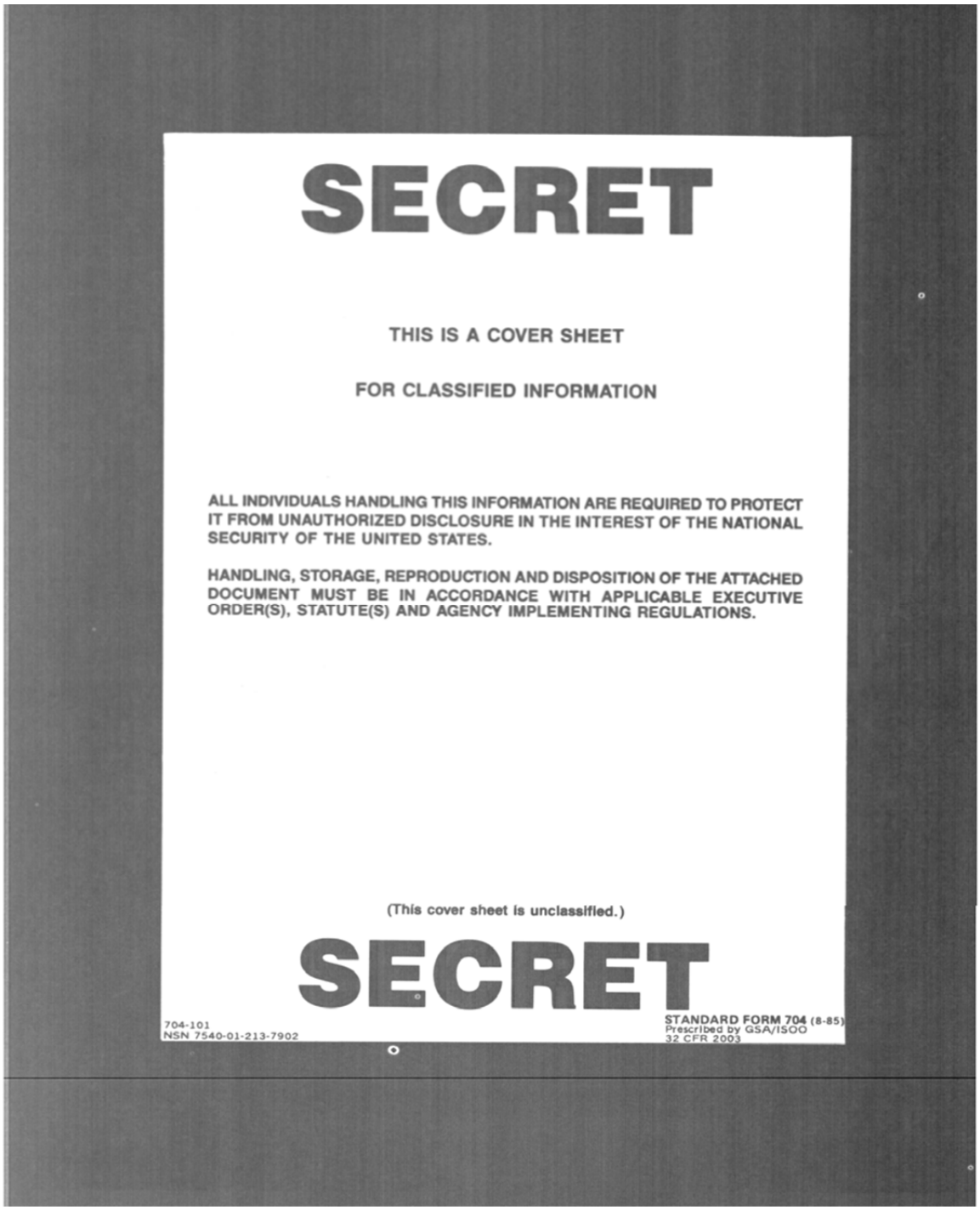
703-101
NSN 7540-01-213-7901

STANDARD FORM 703 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

COLOR ORANGE

Figure 7-1.--Sample Top Secret Cover Sheet

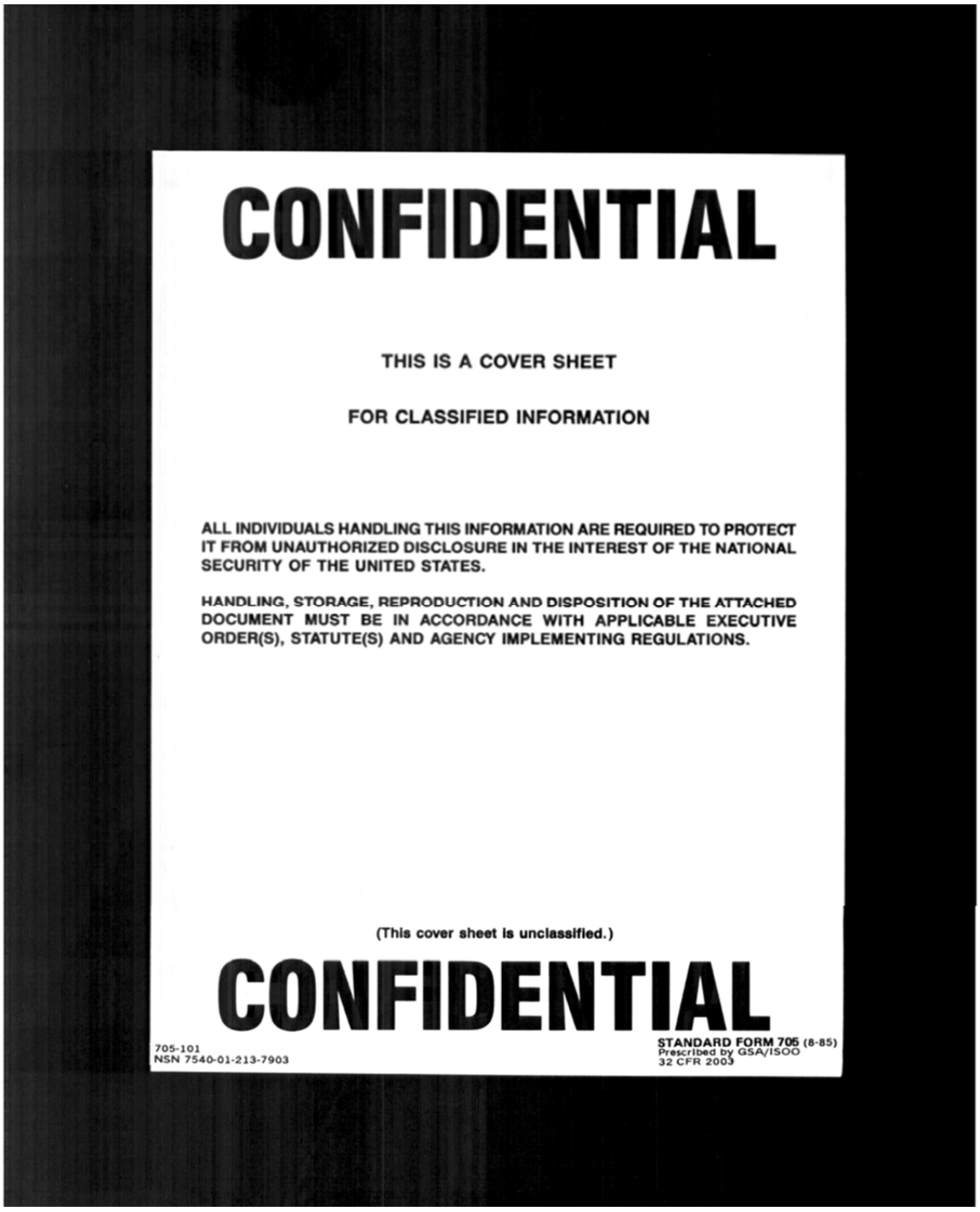
Enclosure (1)



COLOR RED

Figure 7-2.--Sample Secret Cover Sheet

Enclosure (1)



COLOR BLUE

Figure 7-3.--Sample Confidential Cover Sheet

Enclosure (1)

(*Letter Head*)

5510
(*Originator Code*)
(*Date*)

From: (*Activity Security Manager*)
To: Head, Classified Material Control Center (CMCC) (Attn: Document Control Section)

Subj: CHANGE OF CUSTODIAN INVENTORY OF CLASSIFIED MATERIAL

Ref: (a) MCBO 5510.1C

Encl: (1) ASCP, print out of material inventoried

1. In accordance with the reference, a change of Custodian inventory of all controlled SECRET/NATO SECRET and SPECAT holdings was conducted on (*DATE*). The enclosure is a detailed list of classified material held by this account.

2. Point of Contact for this matter is (*Primary Custodian or Alternate or Security Manager*), (*Telephone number*).

(*Incoming Custodian*)
SIGNATURE

(*Security Manager*)
SIGNATURE
Verified by

Copy to:
Files

Figure 7-4.--Sample Change of Custodian Inventory of Classified Material Cover Letter

Enclosure (1)

(*Letter Head*)

5510
(*Originator Code*)
(*Date*)

From: (*Activity Security Manager*)
To: Head, Classified Material Control Center (CMCC) (Attn: Document Control Section)

Subj: ANNUAL INVENTORY OF CLASSIFIED MATERIAL

Ref: (a) MCBO 5510.1C

Encl: (1) ASCP, print out of inventoried material

1. In accordance with reference (a), an annual inventory of all controlled SECRET/NATO SECRET and SPECAT holdings was conducted on (*DATE*). Enclosure (1) is a detailed list of classified material held by this account.

2. Point of Contact for this matter is (*Primary Custodian or Alternate or Security Manager*), (*Telephone number*).

(*Custodian*)
SIGNATURE

(*Security Manager*)
SIGNATURE
Verified by

Copy to:
Files

Figure 7-5.--Sample Annual Inventory of Classified Material Cover Letter

Enclosure (1)

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, waste baskets and other surfaces and receptacles are free of classified material.		1						1														1	1								
3. ~~Windows and doors~~ have been locked (where appropriate).																										1					
4. Typewriter ribbons and ADP devices (e.g., dish.taoes) containing classified material have been removed and properly stored.																				1	1										
5. ~~Security alarm(s) and equipment have been activated (where appropriate).~~																				1			1	1							
INITIAL FOR DAILY REPORT																															
TIME																															

701-101
NSN 7540-01-213-7899

•U.S. GPO. 1993-100-192/&0H!

STANDARD FORM 701{8-851
Prescribed by GSA/1500
32 em 2003

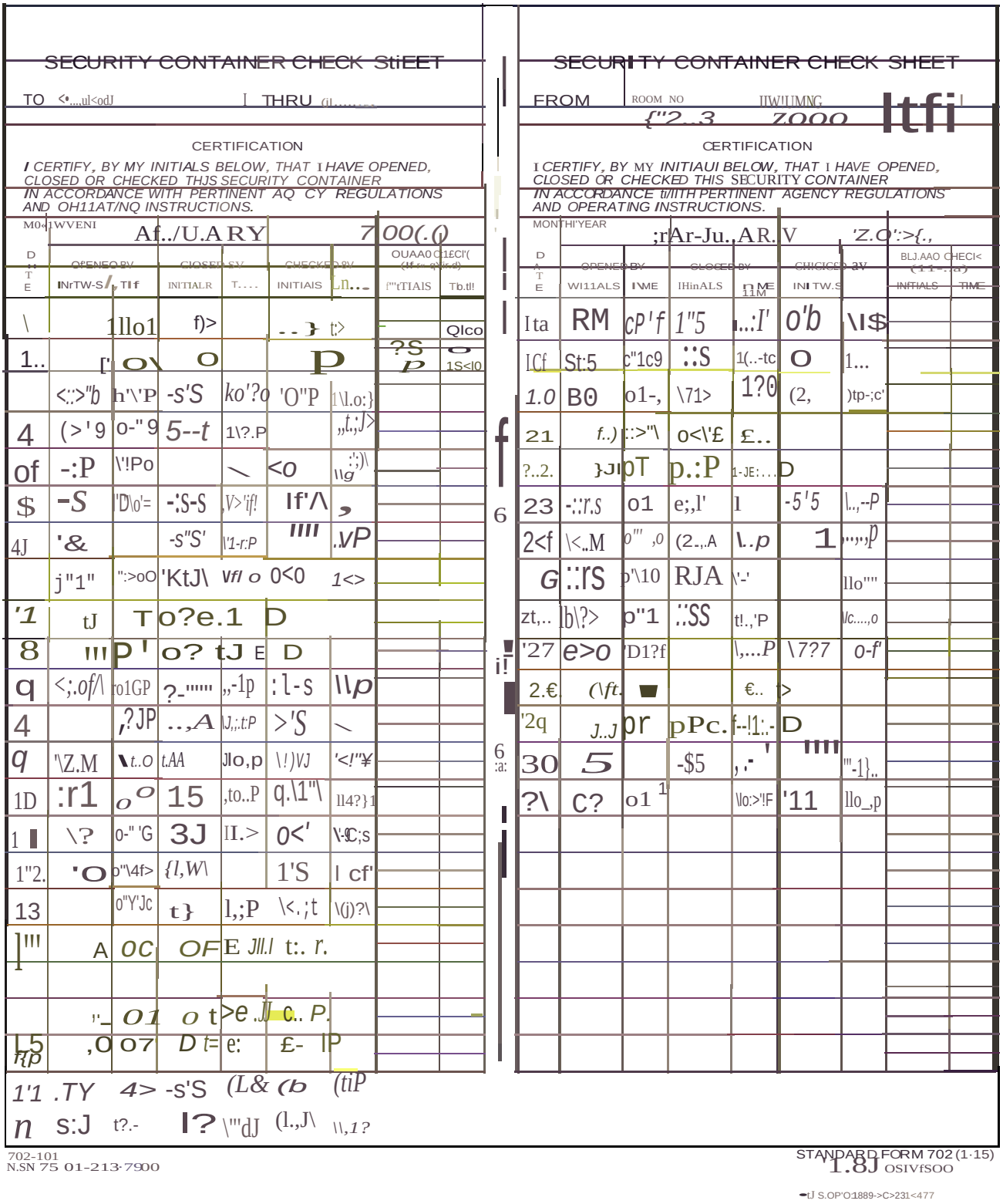


Figure 7-7.--Sample Security Container Check Sheet
Enclosure (1)

INSTRUCTIONS FOR SECURITY CONTAINER CHECK SHEET SF-702

The SF-702 is not a complex document; however, past inspections have shown that none of the SCPs completes the form in the same manner. To standardize its use, the guidance provided here is how the form is expected to look when completed by Secondary Control Point (SCP) and Local Element users serviced by MCBQ.

Each 8 ½ X 11 form represents 2 months, tear the form in half so there is only 1 month of information on each side; because ServMart may not always have the forms in stock, users have been using Xerox copies, an acceptable alternative when printed front to back or a single sheet folded in half. *(It's possible that more than one form will be needed during the month depending on how often the container is opened and closed).*

The form will be displayed on the outside of the container. **The form will not be predated**; however, all days of the month will be accounted for. On days the container is not opened, entries will be recorded as "**NOT OPENED,**" **weekend and holidays** will be highlighted in yellow and will have no entries except for the date and guard checks as appropriate. Required entries are as follows:

The **"TO"** field is only required if someone other than the SCP custodian is expected to review the form after completion, but generally *not required*.

The **"THRU"** field is the same as via, but generally *not required*, unless specified by your local command.

"ROOM NO.", **"BUILDING"**, and **"CONTAINER NO."** are required fields. The container number should be the serial number of the container and not safe 1, 2 etc. However, the only requirement is that the card can later be matched with its container. Front Door/Back Door is used for vaults and secure rooms.

The **"MONTH/YEAR"** field is a required entry.

Figure 7-8.--Instructions For Security Container Check Sheet SF-702

Enclosure (1)

The **"DATE"** field is required 1, 2, 3, etc. Do not include the month again.

"OPENED BY," the **"INITIALS"** and **"TIME"** are required fields.
Enter the initials of the person and time that he/she opened the X-O lock.

"CLOSED BY," the **"INITIALS"** and **"TIME"** are required fields.
Enter the initials of the person and time that he/she locked the X-O lock.

"CHECKED BY," the **"INITIALS"** and **"TIME"** are required fields.
Enter the initials of the person and time that he/she is checking behind the person that actually performed the locking of the X-O lock. This person can be anyone that is available and requires no security clearance or access to perform the check. Please note that too many security violations have been caused because this check was not completed at the time of closing.

Regardless of how many times the container(s) are opened and locked, this check is only required at the end of the day during the end-of-the-day security checks.

Containers with multiple control drawers are no different than any other GSA approved container. Each drawer must have an SF-702 for each drawer assignment and each must be checked.

If you are working alone in a vault or Secure Room (SR), you may omit making this entry provided that upon leaving, the exterior door vault or SR is checked as required.

To alleviate the SF-702 requirement for a container, the container must be taken out of service (all locks set to the factory combination 50-25-50, the drawers must remain open at all times with the locks in the locked position) and the new status of the container reported to the Command Security Manager's office.

"GUARD CHECK," the **"INITIALS"** and **"TIME"** fields are encouraged as to enhance the security posture of your organization; this check is *not required* for GSA approved containers at the secret level unless internal policy requires it. Open storage areas

Figure 7-8.--Instructions for Security Container Check Sheet SF-702 - Continued

must have an Intrusion Detection System (IDS), without an IDS, or at times the IDS is out of service a guard check is required every 4 hours for open storage secret and every 2 hours for top secret.

The SF-702 is retained for 1 month and must be made available for review during inspections.

REMINDER: (*Anytime a vault or SR is left unattended, all X-O locks must be locked and the action recorded on the SF-702. Cipher, swipe, proximity or any other type of access control device in its self, is not authorized for the protection of classified material and equipment, therefore if X-O locks are detected in the locked open position and the area is left unattended, the result is a wall-to-wall inventory and PI for the command committing the offense.*)

Figure 7-8.--Instructions For Security Container Check Sheet SF-702 – Continued

INFORMATION SECURITY PROGRAM

CHAPTER 8

DISSEMINATION

8000. BASIC POLICY

1. Dissemination of classified material will be limited to those activities having a need-to-know and will reflect all applicable restrictions imposed by the originator and higher authority.

2. Material prepared for public release will not contain classified material or prescribed technical data. Policies and procedures governing public release of official information and the circumstances under which a security review is required are detailed in SECNAVINST 5720.44B and MCO 5510.9B and will be coordinated through the Public Affairs Office.

3. For information and appropriate references pertaining to special access programs, material originating in a non-Department of Defense (DoD) department or agency, restricted and formerly restricted data, North Atlantic Treaty Organization material, cryptographic information, and Single Integrated Operational Plan information, refer to Chapter 9 of reference (b) and Chapter 8 of reference (d).

4. Distribution of all controlled unclassified information will be in accordance with Chapter 8 of reference (d).

8001. DISSEMINATION THROUGH JUDICIAL PROCEDURES

1. Convening authorities through judicial proceedings will make every effort to declassify that classified material which will be introduced as evidence.

2. If classified information is required for prosecution during a trial, the officer exercising general court-martial jurisdiction will notify the Command Security Manager (B 054) so that appropriate personnel security clearances can be granted in accordance with Chapter 9 of reference (b).

8002. DISSEMINATION TO DOD CONTRACTORS. Before disclosing any classified information to a DoD contractor, releasing activities

or contractor, commands must determine that the contractor has a current facility security clearance equal to or higher than the level of classified information to be disclosed. This may be done using DD 254 information provided by the Command Security Manager (B 054). All classified information from this Command held by a contracting facility, is on a temporary loan basis, not to exceed 2 years, and will be returned in the prescribed amount of time, extensions may be authorized by the Secondary Control Point lending the information.

8003. DISCLOSURE TO FOREIGN GOVERNMENTS, INTERNATIONAL ORGANIZATIONS, AND CONGRESS. Authority for disclosure of classified information to foreign governments has been centralized in the Navy International Program Office. Accordingly, the disclosure of classified information by oral, visual, or written communications, or by any other means, to foreign governments or international organizations must be authorized in writing. Requests and approvals/disapproval will be processed via the Command Security Manager (B 054).

8004. DISSEMINATION OF INTELLIGENCE. Prior to foreign dissemination of classified information or release of intelligence to contractors, Chapter 8 of reference (d) and other applicable directives will be reviewed and the Command Security Manager (B 054) notified.

8005. DISTRIBUTION STATEMENTS. All Commanding officers/directors will ensure that all personnel honor and apply distribution statements as prescribed in Exhibit 8A of reference (d).

INFORMATION SECURITY PROGRAM

CHAPTER 9

TRANSMISSION AND TRANSPORTATION

9000. BASIC POLICY. Classified information will be transmitted and or transported by or in the custody of an appropriately cleared individual or by an approved system or carrier in accordance with the provisions of Chapter 9 of reference (d).

9001. TOP SECRET. Top Secret material is received via the Defense Courier Service. The Base Trade Security Control Office and the designated assistant located at the Classified material Control Center (CMCC) are the official Top Secret couriers for this Base.

9002. SECRET. Secret material will normally be transmitted via the U.S. Postal Service (USPS) registered mail within and between the U.S. and its territories subject to the guidelines contained in Chapter 9 of reference (d). For overnight service, USPS Express Mail is permitted with prior approval from the Base Adjutant. Federal Express (FEDEX), United Parcel Service (UPS) can be used to transmit secret and confidential material and shall only be used when it is the most cost-effective method of transmission given the constraints of time, security, and accountability. To ensure that classified material is not stored at unsecured facilities over weekends and holidays; FEDEX, UPS, and registered USPS mail will only be shipped by 1000 on Monday through Thursday. This limitation includes any and all next day services.

9003. CONFIDENTIAL. Confidential material will normally be transmitted by Registered, First Class, or Certified mail in accordance with the guidelines contained in reference (d) and has the same shipping limitations identified in paragraph 9002 above.

9004. TELEPHONE TRANSMISSION. Classified information will not be transmitted over the telephone except as may be authorized on approved secure communication circuits. The practice of stating "This is not a secure line" is not a Department of Navy requirement. DD Form 2056 decals will be placed on all official base telephones to alert users not to discuss classified

Information and that the telephones are subject to monitoring at all times. Unless special equipment is being used, there is no reason to believe a line is secure. Therefore, any discussion of classified information or "talking around" classified material is prohibited and unnecessary with the availability of secure terminal equipment (STE) telephones.

9005. RECEIPT SYSTEM

1. Transmit Top Secret material under a continuous chain of receipts.

2. Secret material will be accounted for by a signed receipt when transmitted between commands and authorized addressees. Failure to sign and return a receipt to the sender may result in a report of a possible compromise. Receipts are in the form of a hard copy Classified Material Control Form, automated security control program (ASCP), (*Figure 9-1*), or OPNAV Form 5511/10 or an appropriate letter of transmittal.

3. Local receipts for confidential materials are not required.

4. Only secret hardcopy classified material and secret material on mass media storage devices will be turned in to the CMCC for processing and control. The CMCC is responsible for all receipts and transmittals accompanying the information. The receipt form will be unclassified and contain only the information necessary to identify the material being transmitted. Classified receipts and transmittals should be avoided when possible, except in the case of a classified subject line, a tracking number should be used with the subject line as “SUBJECT CLASSIFIED.”

9006. TRANSMISSION OF CLASSIFIED MATERIAL TO FOREIGN GOVERNMENTS. Refer to Chapter 9 of reference (d) EXHIBIT 9A.

9007. TRANSMISSION OF COMMUNICATIONS SECURITY MATERIAL. In accordance with the Electronic Key Management System (EKMS) 1 (NOTAL) Communication Security Material will be transmitted to and from Quantico by the EKMS Manager, alternate managers or designated persons ONLY. EKMS is located within the MCCDC Security Office. Consult the Commands Staff case management system (CMS) Responsibility Officer and EKMS Manager prior to the transmission of this material.

9008. PREPARATION OF CLASSIFIED MATERIAL FOR TRANSMISSION

1. When classified material is transmitted, enclose it in two opaque, sealed envelopes or similar wrappings, where size permits, except as provided in paragraph 9008.2 below.

a. Fold or pack classified written material so the text will not be in direct contact with the inner envelope or container.

b. Show, on the inner envelope or container, the address of the receiving activity, highest classification of the material enclosed including, where appropriate, the "Restricted Data" marking and any special instructions. Seal it carefully to minimize the possibility of access without leaving evidence of tampering. Attach the receipt required for top secret and secret material and confidential when a receipt is required.

c. Do not put on the outer cover a classification marking, or a listing of the contents divulging classified information, or any other unusual data or marks which might invite special attention to the fact that the contents are classified.

2. Whenever the classified material being transmitted is too large to prepare as in paragraph 9008.1 above, wrap item in two opaque sealed containers, such as boxes or heavy wrappings. If the classified material is an internal component of a packaged item of equipment, the outside shell or body may be considered as the inner enclosure, which means that the packaged item of equipment need only be wrapped once.

9009. ADDRESSING

1. Address classified material to an official government activity or Department of Defense (DoD) contractor and not to an individual. This requirement is not intended however, to prevent use of office code numbers or such phrases in the address as "Attention: Mr. Robert Allen," or similar aids in expediting internal routing, in addition to the organization address.

2. Consult the following publications for complete and correct mailing addresses and mailing instructions:

a. Standard Navy Distribution List, Part 1 contains the official list of fleet and mobile units and their administrative

addresses.

b. Catalog of Naval Shore Activities, including Standard Navy Distribution List, Part 2 contains the official list of shore activities with complete administrative addresses.

3. The inner envelope or container will show the address of the receiving activity, the address of the sender, the highest classification level of the contents, including all warning notices. (*See Chapter 6, paragraphs 6-11 and 6-12 of reference (d)*.)

4. An outer envelope or container will show the complete and correct address of the recipient and the return address of the sender.

5. Care must be taken to ensure that classified material intended only for the U.S. elements of international staffs or other organizations are addressed specifically to those elements and that the correct address for classified mail is used for overseas locations. At **NO** time will classified information of any type be mailed to a post office box.

9010. GUARD MAIL. The use of guard mail or any other unsecured method to transmit classified material of any kind is **strictly prohibited**, and will result in a Preliminary Inquiry. Do not hold or store classified materials in a guard mail envelope. See Chapter 12 of reference (d).

9011. ELECTRONIC TRANSMISSION. Transmission of classified material by standard naval telecommunications or the Defense Messaging System is under the cognizance of the Assistant Chief of Staff, G-6, Marine Corps Base, Quantico (MCBQ).

9012. GENERAL PROVISIONS FOR ESCORTING OR HAND CARRYING CLASSIFIED INFORMATION

1. The Command Security Manager’s Office (B 054) shall provide written authorization to all individuals required to escort or hand carry classified information. This authorization may be the DD 2501, Courier Authorization Card, or included on official travel orders, or a courier authorization letter. Any of these three written authorizations may be used to identify appropriately cleared DoD military and civilian personnel

approved to escort or hand carry classified information (*SAPs are excluded*) between DoD commands subject to the following conditions:

a. The individual has a recurrent need to escort or hand carry classified information,

b. The expiration date may not exceed 3 years from the issue date (*pertains only to DD 2501*),

c. The written authorization is retrieved upon an individual's transfer, termination of employment, or when authorization is no longer required.

2. The written authorization is intended for use between DoD commands worldwide and provides sufficient authorization to hand carry classified information aboard a U.S. military aircraft.

3. Only the Command Security Manager or the Assistant Command Security Manager will issue courier authorizations. Every precaution must be taken to prevent unauthorized disclosure when individuals are hand carrying classified material within this Base in the pursuit of daily duties or outside this Base in an official travel status.

4. Courier cards are required when classified material is being carried as part of normal duties, within the command, MCBQ and serviced commands. Information being couriered to organizations not owned or serviced by the MCBQ may be asked to present courier credentials. While transporting classified information locally, reasonable precautions will be taken to prevent inadvertent disclosure. Reasonable precautions include using an envelope, file folder, or other nontransparent covering so as not to draw attention to the classification level of the contents and to protect against casual observation of classified information. These precautions are to be taken when the movement is from one building to another, in an elevator, or through public area workspaces.

5. If the movement requires transportation other than walking, double wrap the classified material. A locked briefcase may be considered as the outer wrapping, except when hand carrying aboard commercial aircraft.

6. Because of the security risk inherent in hand carrying classified material while in a travel status, off Base authorization will only be given when:

a. The classified material is required at the traveler's destination,

b. The classified material is not available at the visited destination,

c. Because of time or other constraints, the classified material cannot be transmitted by another authorized means.

7. Requests to courier classified material aboard U.S. flag carrying commercial aircraft may be originated with department heads. Requests will then be forwarded to the Command Security Manager via the activity heads (*designated Security Manager*), and will contain the following:

a. Full name of the individual and their employing agency or command.

b. Have available for inspection, military/civilian picture identification card (DD Form 2) and (DD Form 2/OF55).

c. Dates classified material is to be carried, not to exceed 7 days.

d. Description of material to be carried (*e.g., three sealed packages, 9" x 8" x 24"*), address, and sender.

e. Itinerary of travel, listing points of departure, destinations, and known transfer points.

f. Level of classified material to be transported.

g. How the information be returned to Quantico.

h. Destination point of contact (*full name, address, and telephone number*).

8. Upon receipt of the request containing all information listed above and the information to be transported, a courier letter authorization will be completed. The designated courier will then personally receipt for the authorization at the time of package pick up at the CMCC, Bldg. 3250, and receive the

briefing as required by reference (d).

9. The Universal Courier Authorization Card, DD Form 2501, supersedes all other command developed courier authorizations except for the NAVINTCOM 5510-69 (Rev 9-86), Sensitive Compartmented Information Courier Card. Use of DD Form 2501 is mandatory and exceptions or waivers from their use will not be granted. DD Form 2501 is authorization for Continental United States and Outside Continental United States hand carry of classified material only and does not constitute authority for hand carrying classified material on commercial aircraft. In addition to DD Form 2501, a courier letter is necessary for hand carrying classified information on commercial aircraft.

a. The Command Security Manager is responsible for the procurement, accountability, and issuance of all DD Form 2501 cards for MCBQ and supported tenant personnel.

b. Activity Security Managers are responsible for ensuring accountability of all classified material given to couriers (*including working papers*). Activity Security Managers are also responsible for obtaining a signed briefing form for retention upon issuing classified material for hand carrying off station.

c. In all cases, couriers are required to sign a briefing form acknowledging their understanding of the regulations governing the hand carrying of classified material (*Figure 9-2*). They are also responsible for providing their activity Security Managers with inventories of classified material being hand carried from the confines of this Base to another destination prior to departure.

9013. ADDITIONAL GUIDANCE. For additional information pertaining to aircraft and the conduct of passengers, refer to Chapter 9 of reference (d).

UNCLASSIFIED ***Wednesday, January 28, 2011***

CMCC Document Control Form

Data Entered By ***(EXAMPLE)***

Secondary Control Point
Force Protection Integration Division, CDD

Control ID Number
386

OCA
NORTHROP GRUMMAN

Cross Reference Bar Code
BA08GW2

Short Title
TECHNICAL REPORT

Long Title
TECHNICAL REPORT STUDY SERVICES DD FORM 1494 FREQUENCY ALLOCATION FOR THE G/ATOR

Medium
HARD COPY DOC

Serial Number
N/A

Model or Type
N/A

Classification
SECRET

Reason Classified
1.4a //Mil Plans, Weapons Sys, Operations

Document Date
20-Mar-08

Date Received
25-Mar-08

Declassify on
Monday, September 30, 2024

Downgrade Interval
N/A

Remarks: ***(For Contractors, you must include Name, Address, Contact Phone Number and document return Date)***

I hereby acknowledge receipt for and take responsibility for the classified material listed.

Signature:

Printed Name: ***Date:***

Figure 9-1.--Sample Classified Material Control Form

Enclosure (1)

COURIER ADVISORY

(When hand carrying classified material/COMSEC in a travel status)

Person Assigned Courier Duty: _____
Last First MI SSN (complete)

Card Number: _____ Issue Date: _____

Special Instructions:

1. As an authorized courier, I have reviewed and understand the provisions of Chapter 9 of SECNAV M-5510.36 and Chapter 9 of MCBO 5510.1D (Information and Personnel Security Program).

2. I understand that I am liable and responsible for the information being escorted. An inventory of the document(s) to be transported and/or received from another agency or activity will be given to the respective security representative of the unit, activity or organization with a copy forwarded to the Command Security Manager (B054).

3. The information/equipment is not, under any circumstances, to be left unattended. The material must be placed in unmarked, double-sealed envelopes and remain in my physical possession at all times. The outer envelope will contain the address of the Command where the information originated and the name of an official to contact in the event of an emergency. The inner envelope will be marked with the highest classification of material contained within.

4. During overnight stops, classified information is to be stored at a U. S. embassy, military or appropriately cleared DoD contractor facility (continental U.S. only) and shall not, under any circumstances be stored unattended in vehicles, hotel rooms, hotel safes, etc. When I surrender any package containing classified material for temporary storage I must obtain a receipt signed by an authorized representative of the U.S. Embassy, military or appropriately cleared DoD contractor facility accepting responsibility for safeguarding the package.

5. The information shall not be opened except in the circumstances described in paragraph 9.

6. The information shall not be discussed or disclosed in any public place or conveyance. I may not read, study, display or use classified material in any manner on or in a public place. I will not store classified material in any detachable storage compartment such as an automobile luggage rack, aircraft travel pod or drop tank.

7. I shall not deviate from the authorized travel schedule.

Figure 9-2.--Courier Advisory

Enclosure (1)

8. I am responsible for ensuring that personal travel documentation (identification card, passport, courier authorization and medical documents) are complete, valid and current.

9. There is no assurance of immunity from search by security, police, customs and/or immigration officials on domestic or international flights. Carry-on bags and packages may be subject to x-raying and inspection by customs or airline/airport security officials. If there is a question about the contents of the package, the courier shall present the courier authorization to the official or to the official's supervisor, if necessary. If the official demands to see the actual contents of the package, it may be opened in his or her presence, in an area out of sight of the general public. However, under no circumstances shall classified information be disclosed. Immediately after the examination, the courier shall request that the package be resealed and signed by the official to confirm that the package was opened. Inform both the addressee and the dispatching security office, in writing, of the opening of the package.

10. Upon return, the courier shall return all classified material in a sealed package, with receipts for any material that is not returned. All material must be accounted for.

11. Refer to USSAN 1-07 of 5 April 2007 on the hand-carry of classified NATO information.

12. I hereby certify that I have been briefed on the special requirements of courier duty and that I have been given a copy of this advisory.

Individuals Signature: _____

Date: _____

Expiration Date: _____

Figure 9-2.--Courier Advisory - Continued

Enclosure (1)

INFORMATION SECURITY PROGRAM

CHAPTER 10

STORAGE AND DESTRUCTION

10000. BASIC POLICY

1. Commanding officers, directors, and activity heads are responsible for safeguarding all classified information within their organizations. They must ensure that it is stored as prescribed in Chapter 10 of reference (d). To the extent possible, areas in which classified material are stored will be limited.

2. Report any weakness or deficiency in equipment being used to safeguard classified material in storage to the Command Security Manager (B 054). Reports must fully describe the weakness or deficiency and how it was discovered.

3. Valuables such as money, jewels, precious metals, narcotics, etc., will not be stored in the same containers used to safeguard classified material.

4. There shall be no external markings revealing the classification level of information being stored in a specific security container, vault, or secure room. Priorities for emergency evacuation and destruction shall not be marked or posted on the security container. This does not preclude the placing of required decals and necessary information for other purposes.

10001. STORAGE REQUIREMENTS

1. Chapter 10 of reference (d) must be reviewed prior to storing classified material.

2. Each security container, Secure Room (SR) and vault will have a Security Container Records Form, Optional Form 89 (Figure 10-1). Security containers will be inspected periodically. The Optional Form (OF) 89, will be kept inside the control drawer or door of the container. SRs will have OF 89 attached to the inside of each door with a Federal Specification FF-L-2740 combination lock.

3. Only General Services Administration (GSA) approved security containers and secure rooms will be used for storage of classified material and classified COMSEC items.

4. Field safes, special purpose one and two drawer lightweight (*Short Depth usually under 200lbs*) Containers/Cabinets, GSA-approved under Federal Spec AA-F-358 are used primarily for storage of classified material in the field and in transportable assemblages. Such containers not located in a secure room/vault, must be rendered non-portable (*i.e., chained to a permanent fixture*), or guarded to prevent theft.

5. Authorization to store classified material will be requested from the Command Security Manager (B 054). A Physical Security Evaluation (PSE) will be conducted by the Command Security Manager's Office to determine the degree of security afforded within the existing area, and to recommend additional security requirements when necessary. Once the specifics of the PSE have been met, a certification will be issued authorizing the Secondary Control Point (SCP) to hold classified material and equipment at the classification level indicated in the PSE.No classified storage is authorized without this evaluation and certification. Additional security containers will not be procured until:

a. A PSE of existing equipment and a review of classified records on-hand has been made.

b. It has been determined that it would not be feasible to use available equipment or to retire, return, declassify, or destroy a sufficient volume of records currently on hand to make the needed security storage space available.

6. "Locked/Open" sign will be displayed on each container that contains classified material to indicate whether the container is locked or open.

7. A SR is designated as a "Restricted Area" and requires a Physical Security Survey (PSS) conducted by the Provost Marshal's Office, Physical Security Branch. An SCP with a designated Restricted Area has open storage status. In accordance with MCO P5530.14, a Restricted Area that is surveyed for classified information and material must have a PSS conducted every 18 months. A copy of the completed PSS is forwarded to the Command Security Manager (B 054) and becomes an enclosure to the commands PSE and certification process.

8. SR open storage will not be authorized without an Intrusion Detection System (IDS) and an approved Access Control System (ACS). Exceptions to the IDS requirements are contained in Chapter 10 of reference (d).

9. Certification for a Controlled Access Area (CAA) and Restricted Access Area (RAA) is by the Command Security Manager only, and are **never** authorized open storage status and will not in any way be referred to as a Restricted Area. Associated Protected Distribution Systems (PDS) terminating within an SR, CAA, or RAA is certified by the Designated Approving Authority and not by the Command Security Manager. Point of contact for a PDS is the Assistant, Chief of Staff G-6.

10002. COMBINATIONS, LOCKS, AND KEYS

1. Guidance pertaining to combinations, locks, and keys is contained in Chapter 10 of reference (d).

2. Combination changes, neutralization of lockouts and repairs, or maintenance of security containers will be requested through the Base Locksmith by submission of a Work Request (*Maintenance Management*), NAVFAC Form 9-11014/20. Only trained personnel with the appropriate security clearance will make combination changes. Depending on the availability of trained security personnel the Command Security Manager (B 054) can provide assistance for changing combinations upon request.

3. Records of combinations will be sealed in a Security Container Information Envelope, Standard Form (SF) 700 (*Figure 6-1*), and kept on file at the Classified Material Control Center (CMCC) by the Command Security Manager, multiple envelopes will be maintained at the SCP in a designated master container. The combination envelope to the master container and or a vault/secure room lending access to the master container will be turned in to the CMCC for safekeeping. The SCP Custodian will inspect the SF 700 envelopes maintained in the master container monthly for signs of tampering. Part one of the SF 700 will be attached to the inside of the control drawer or door of each container, visible to anyone who might find the container left open. All security containers will have the serial number recorded in Block 5 of the SF 700. In addition, you may also further identify security containers simply as, “Safe 1, 2, etc.”

4. When securing security containers, vaults, and secure rooms rotate the dial at least four complete turns in the same direction.

5. When a container with a built in lock or a padlock is taken out of service, the built-in lock will be reset to the standard combination 50-25-50, and combination padlocks will be reset to the standard combination 10-20-30.

10003. PROCUREMENT AND TURN-IN OF SECURITY CONTAINERS

1. New security containers will not be requested or requisitioned by activity heads if similar equipment is available from the Director, Facilities Division.

2. When GSA approved security containers are no longer required or are not being used for storage of classified material, the using activity will turn in the container to the Director, Facilities Division.

3. Command Security Manager will maintain listings of all security containers used for the storage of classified material. The Command Security Manager will be kept informed of all movements, change of possessions, and/or turn-ins of all approved security containers between and among users.

10004. DESTRUCTION OF CLASSIFIED INFORMATION

1. Prior to the destruction of classified information, review paragraph 10-17 of reference (d).

2. Destroy classified information no longer required for operational purposes in accordance with SECNAV M-5210.1. Destruction of classified information shall be accomplished by means that eliminate risk of recognition or reconstruction of the information.

3. Commanding Officers will establish at least 1 day each year as “clean-out” day, when specific attention and effort are focused on disposition of unneeded classified and unclassified information. It is recommended that it be done during April while conducting the SCP annual inventory.

4. Refer to EKMS 1 for the destruction of Communications Security information. Refer to DoD 5105.21-M-1 for destroying SCI and OPNAVINST C5510.101D for destroying NATO information. For the destruction of all AIS media use NAVSO P-5239-26.

5. The Directorate for Information Systems Security, National Security Agency, provides technical guidance concerning appropriate methods, equipment and standards for the destruction of classified electronic media and processing equipment components, e.g., floppy disks, zip disks, jazz drive disks, CD/DVD ROM disks, failed hard drives, and magnetic tape (audio, video and data). Once these medium types are associated with a classified source it is forever classified and the CMCC is the only authorized activity to implement their destruction. SCP's that have purchased or have access to approved destruction devices for CD and DVD mediums are authorized to conduct their own destruction for this type.

NOTE: *(An IT medium that is not always classified after a classified association is; an unclassified medium with a write protect capability may be used on a classified system as long as the write protect feature is activated prior to its association. Unclassified CD and DVD media may be used in a classified system and remain unclassified when removed as long as the device drive used is read only.)*

10005. DESTRUCTION METHODS AND STANDARDS

1. Various methods and equipment may be used to destroy classified information that include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition, or pulverizing.

2. A crosscut shredder shall reduce the information to shreds no greater than 1/32 inch wide by 3/16 inch long. Strip shredders will not be used for the destruction of classified information. Strip shredders and other shredders in use that do not meet the minimum standards for the destruction of classified material will have the following statement visibly attached, "NOT AUTHORIZED FOR THE DESTRUCTION OF CLASSIFIED INFORMATION."

3. Pulverize machines and disintegrators must have a 3/32-inch or smaller security screen.

4. Pulping (wet process) devices with a 1/4 inch or smaller security screen may be used to destroy classified water-soluble material.

5. The CMCC has an industrial shredder for the destruction of large amounts of classified information. However, the following restrictions apply:

a. Only top secret, secret and confidential information may be destroyed. Because of high maintenance costs the shredding of unclassified information described in paragraph 10007 will not be authorized.

b. Items must be free of all metal, (i.e., paperclips and all fasteners); no cardboard or hard back folders. No soft or rubber items of any kind and no magnetic tape will be placed in the shredder for destruction.

c. A representative from the CMCC must be present at all times to ensure that the equipment is operated properly. SCPs are required to provide their own transportation for material, personnel to conduct the destruction and for clean up.

d. Destructions will be scheduled by appointment only with the CMCC classified courier.

10006. DESTRUCTION PROCEDURES

1. Strict adherence to the procedures for the destruction of classified material and the methods of the destruction contained in Chapter 10 of reference (d) and this Order will be observed. The destruction of any classified material is always conducted by two cleared persons with clearance and access at the level of information being destroyed regardless of whether or not a destruction record is required.

2. A record of destruction is required for Top Secret information. The use of OPNAV 5511/12, “Classified Material Destruction Report,” may be used for this purpose or, by any means as long as the record includes complete identification of the information destroyed. See paragraph 10-19 of reference (d) for current methods of destruction, retention period for top secret destruction reports is 5 years.

3. In accordance with reference (d), a record of destruction is not required for Secret and Confidential information however, at Marine Corps Base, Quantico, there is a requirement for reporting the destruction of controlled information. All information being controlled in the Automated Security Control Program (ASCP) will be destroyed as follows:

a. Organizations owning GSA approved equipment capable of destroying mass media storage devices will notify the Command Security Manager prior to the destruction of any ASCP controlled items. The notification can be in any written communiqué that describes the equipment manufacture, model number, and the mediums in which the equipment has been approved for. Once the notification has been acknowledged, the SCP custodian will print the effective pages from their ASCP inventory. The SCP custodian will highlight the control number(s) of the items to be destroyed. Two appropriately cleared persons must witness the destruction as the information is actually destroyed. The pages containing the items to be destroyed are taken to the CMCC. The CMCC will provide the SCP with an official destruction report for retention.

b. When controlled documents are to be destroyed by the CMCC, deliver the pages from the inventory containing the highlighted items to be destroyed along with the items/documents/material to the CMCC. The CMCC will provide the SCP with an official destruction report for retention.

c. The SCP and the CMCC will retain a signed copy of the destruction report for a period of 2 years.

4. Use OPNAV 5511/12 and retain locally for 2 years when hardcopy documents, classified message traffic, working papers and other classified documents that are <u>not</u> controlled in the ASCP are destroyed. Confidential material and classified waste products do not require a record of destruction however, it is highly recommended that a record of destruction be made and retained by the SCP custodian as a precautionary for the individuals involved in the destruction. Top Secret working papers <u>are not</u> considered waste products, as they require a destruction report.

5. North Atlantic Treaty Organization (NATO) secret and confidential destruction must be conducted and recorded in the

same manner as in paragraph 3 above. Destruction Records for classified NATO documents will be retained for 5 years.

10007. DESTRUCTION OF UNCLASSIFIED MATERIAL

1. Destroy record copies of For Official Use Only (FOUO), Sensitive But Unclassified, Department of Defense, Unclassified Controlled Nuclear Information, Department of Energy Outside Continental United States, Sensitive (Computer Security Act of 1987), and unclassified technical documents assigned distribution statements B through X, in accordance with Navy and Marine Corps Records Disposition Manual (SECNAV M-5210.1) on-record copies may be shredded or torn into small pieces and placed into several trash containers to be discarded on different days. Records of destruction are not required.

2. Destroy Unclassified Drug Enforcement Administration Sensitive Information and Naval Nuclear Propulsion Information (NNPI) in the same manner approved for classified information.

3. Unclassified material, including formerly classified material that has been declassified, FOUO material, and unclassified messages do not require the assurance of complete destruction.

4. Contrary to widespread opinion, there is no security policy requiring destruction of unclassified messages (except NNPI). Tearing messages into pieces (as is done with FOUO material), defacing them before discarding, or using classified destruction methods are among the choices left to commanding officers and activity heads.

MAINTENANCE RECORD FOR SECURITY CONTAINERS/VAULT DOORS

NOTE: Store this form in the Secu"'ity · · or on the vault door.

TYPE			
	OvAULTOOOR	dra- vaua Doors and Map and Plan Container&: Located on lila Nlde face of the dOOr	123456

SECURITY CONTAINER: Mosler

o s01Wo OTHREE li)FOUR OsiX OsEVEN

TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	NAME	ACTIVITY	ORGANIZATION NAME
Neutralize	03/23/06	R. L. WHEATON	NCIS	NCIS

SIGNATURE OF RESPONSIBLE OFFICIAL | NAME OF RESPONSIBLE OFFICIAL | DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION

OPTIONAL FORM 89 (9-98)

OPERATIN() PR08LEMS	TYPE OF MAINTENANCE	DATE REPAIRED/ INSPECTED	TECHNICIAN NM1E	TECHNICIAN ACTIVITY	ORGANIZATION NAME

SIGNATURE OF RESPONSIBLE OFFICIAL | NAME OF RESPONSIBLE OFFICIAL | DATE SIGNED

AUTHORIZED FOR LOCAL REPRODUCTION

OPTIONAl FORM 89 (98) BACK

Figure 10-1.--Sample Security Container Records Form (Optional form 89)

Enclosure (1)

INFORMATION SECURITY

CHAPTER 11

INDUSTRIAL SECURITY PROGAM

11000. BASIC POLICY. The Commanding Officer is required to establish an industrial security program if the command engages in classified procurement with U.S. Industry, educational institutions or other cleared U.S. entities, hereafter referred to as contractors. This Order chapter supplements regulations to ensure that the Commanding Officer meets his requirements and to ensure that classified information released to industry is safeguarded.

11001. AUTHORITY

1. The Director of Defense Security Service (DSS) oversees Department of Defense (DoD) implementation of the National Industrial Security Program (NISP) through five regions comprised of field offices located throughout the U.S. Each region provides administrative assistance and policy guidance to local field offices charged with security oversight of contractors who perform on classified contracts. Consult the DSS home page at www.dss.mil for information pertaining to various DSS functions.

2. The Defense Industrial Security Clearance Office in Columbus, Ohio, processes and issues personnel and Facility Security Clearance (FCL) for contractors participating in the NISP; furnishes security assurances on U.S. contractor personnel and facilities to authorized foreign governments; reviews and processes visit requests for U.S. contractor employees to foreign government and contractor installations. It also responds to inquiries from defense contractors, military, government agencies; DSS field elements and headquarters personnel who require information or assistance with individual clearance or investigative processing, to include Freedom of Information or Privacy Act requests and Congressional inquiries.

11002. DSS AND COMMAND SECURITY OVERSIGHT OF CLEARED DOD CONTRACTOR OPERATIONS

1. On board ship, Quantico contractor employees under the purview of the Commander have visitor status and shall conform to the requirements of this and other appropriate security regulations.

2. U.S. Shore Installations. Contractors may perform work on and visit shore installation in one of the following ways:

a. When a determination is made that the contractor is a short or long-term visitor, the commanding officer shall require that the long-term visitor comply with command security regulations that included the command security education program.

b. Long-term contractors who have access to classified information and whose work is performed solely within the confines of the command in support of a classified contract, will participate in the commands security education and training program, *(See Paragraph 4 of Part I Personnel Security)*. Conversely, if duties are performed at both the command and contractor facilities, the contractor may participate in the contractor's security training program. However, evidence of annual training must be furnished to the command to verify participation. Additionally, the contractor may be required to participate in command specific training to address command specific and/or local security requirements. Failure to participate or failure to provide evidence of participation could be grounds for suspension of access to classified information.

c. When the contractor is a tenant aboard Quantico, i.e., has sole occupancy of a facility or space controlled and occupied by the contractor, the host command may assume responsibility for security oversight over classified work carried out by the cleared DoD contractor employees in these facilities. The Command is responsible for all security aspects of the contractor's operations in the facility. Oversight cannot be split between the commanding Officer and DSS. The contractor is considered a tenant and is obligated to comply with Department of Navy (DON) regulations and applicable portions of this and appropriate security regulations.

d. The commanding officer may request in writing that DSS grant the contractor a FCL and assume security oversight. If DSS accepts security oversight, DSS is responsible for all security aspects of the contractor operations. The commanding officer has no authority over the contractors' employees or its occupied spaces in this case. This process will normally be used when a contractor is the sole occupant of a building or controlled space that it is leasing and/or managing the operation of on a shore facility.

11003. OFF SITE LOCATIONS. When contractors perform work at DON locations other than the command awarding the contract, the awarding command shall inform the new host of the contractual arrangement and forward a copy of the notification of contract award, a copy of the DD 254 and other pertinent documents to the host command.

11004. OVERSEAS LOCATIONS. Activities under the purview of the Commander that award contracts requiring classified work at overseas locations shall ensure that this policy manual is enforced. Additionally, the contractor and his or her employees while at an overseas location are considered visitors and may be required to follow the security guidelines established by the overseas host command. The host command shall furnish their security requirements to the visiting contractor; the awarding activity shall provide the overseas host a copy of the contract, DD 254 and other pertinent documents.

11005. CONTRACTING OFFICER SECURITY REPRESENTATIVE (COSR) INDUSTRIAL SECURITY RESPONSIBILITIES. Part 1, paragraph 2001.2k of this Order identifies the appointment of a qualified security specialist as a Contracting Officer's Representative (COR). The following industrial security responsibilities are normally assigned to the COSR. Other responsibilities may be assigned as appropriate.

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

2. Validate security classification guidance, complete and sign Block 16.e of DD 254.

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

(b) Request a revised DD 254 if necessary.

(c) Resolve problems related to classified information provided by the contractor.

3. Provide in coordination with the program manager any additional security requirements beyond those required by this Order, in the DD 254, or in the contract document itself.

4. Initiate request for FCL action with the DSS when required.

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

6. Validate and endorse requests submitted by industry for Limited Access Authorizations for non-U.S. citizen employees. The endorsement must confirm that the appropriate foreign disclosure official has approved the release of the specified classified information. The request and its endorsement shall be forwarded to the Defense Security Service for processing the LAA investigation.

7. Coordinate, in conjunction with the appropriate transportation element, a suitable method of classified shipment when required.

8. Review requests by contractors for retention of classified information beyond a 2 year period, inform the contractor of disposition instructions or issue a final DD 254.

9. Ensure that timely notice of contract award is given to host commands when contractor performance is required at other locations and that Memoranda of Agreement or Memoranda of Understanding are in place to provide adequate security for the contractors.

11006. FCL. Refer to paragraph 11-6 of reference (d).

11007. PERSONNEL SECURITY CLEARANCE UNDER THE NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP). Refer to paragraph 11-7 of reference (d).

11008. DISCLOSURE OF CLASSIFIED INFORMATION TO A CONTRACTOR BY GOVERNMENT CONTRACTING AGENCIES

1. Disclose classified information only to contractors cleared under the NISP. Prior to disclosing classified information the custodian shall determine that the contractor requires access in connection with a legitimate U.S. Government requirement (e.g., contract solicitation, pre-contract negotiation, contractual relationship, or IR&D effort). The Command Security Manager can provide assistance in validating personnel/facility clearances.

2. Refer to paragraph 11-8 of reference (d) for guidance on determining contractor facility clearances/storage capabilities.

11009. DISCLOSURE OF CONTROLLED UNCLASSIFIED INFORMATION TO A CONTRACTOR BY GOVERNMENT CONTRACTING AGENCIES. Paragraph 11-9 of reference (d) provides guidance related to controlled unclassified information and the certification of individuals and enterprises qualified to receive unclassified technical data with military or space applications. These individuals and enterprises are referred to as Qualified Contractors. Certification is accomplished using a DD Form 2345, Military Critical Technical Data Agreement.

11010. CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD 254)

1. Commanding officers/directors and the Regional Contracting Officer share in the responsibility to ensure that a DD 254 is incorporated into each classified contract. The DD 254 with its attachments, supplements, and incorporated references is designed to provide a contractor with the security requirements and classification guidance needed for performance on 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.

2. DD 254s are prepared by the COR responsible for the classified contract. (*The Marine Corps Intelligence Activity (MCIA) Quantico will normally be responsible for DD 254s requiring release of intelligence to cleared DoD contractors.*) The DD 254 must be completed prior to submission to the Office of the Command Security Manager for review/signature by an appointed contracting officer security representative (COSR), Figure 11-1 provides a sample DD 254. Figure 11-2 provides the process for the flow of the DD 254 for MCBQ and its tenants.

11011. VISITS BY CLEARED DOD CONTRACTOR EMPLOYEES. Classified information may be disclosed during visits provided the visitor possess the appropriate clearance and access level and have a need-to-know. The responsibility for need-to-know lies with the individual who will disclose classified material during a visit. Quantico commands shall verify that visiting contractors have been granted access using Joint Personnel Adjudication System (JPAS). Once the access of a contractor is established, the clearance certification and access level for that contractor should be accepted. This certification normally will be by use of the visitor certification program in JPAS/ JCAVS unless the system is not available and then by visit authorization request (VAR) from the contractor. Quantico commands shall not accept a visit request hand carried by contractor personnel. Final approval of the visit is the prerogative of the Commander through the Command Security Manager of the command to be visited. DoD 5220.22R, Industrial Security Regulations addresses visit requirements for contractor employees.

11012. TRANSMISSION OR TRANSPORTATION

1. Appropriately cleared and designated DoD contractor personnel may act as couriers, escorts, or hand carriers for classified material. Paragraph 11-12 of reference (d) provides provisions and must be followed at all times.

2. Appropriately cleared contractors may use the GSA approved commercial contract carriers for overnight delivery of Secret and Confidential information to U.S. Government agencies within CONUS when procedures have been formerly approved by the DSS prior to starting such transmissions. GSA commercial carriers may not be used for Top Secret, COMSEC, NATO or foreign government information. See paragraph 11-12 of reference (d) for additional guidance.

11013. RELEASE OF INTELLIGENCE TO CLEARED DOD CONTRACTORS. See paragraph 11-13 of reference (d) for guidance. Release of intelligence information at Quantico will normally be through the MCIA, Marine Corps Base, Quantico.

11014. FOREIGN OWNERSHIP, CONTROL OR INFLUENCE. Refer to paragraph 11-15 of reference (d) for guidance pertaining to foreign ownership, control, or influence.

11015. FACILITY ACCESS DETERMINATION PROGRAM. Paragraph 11-16 provides guidance pertaining to facility access determinations on contracted employees. This program is designed to entrust commanding officers to protect persons and property against the actions of untrustworthy persons. It is further designed to assist commands in making trustworthiness determinations on contractor employees for access eligibility to controlled unclassified information or sensitive areas and equipment under DON control. Since this program is outside the provisions of the NISP, if a contracting command requires trustworthiness determinations that do not meet the requirement for access to classified information, i.e., requirement for a Common Access Card (CAC), the contracting officer shall include the requirement in the specifications of all contracts requiring trustworthiness determinations.

11016. CONTRACT SUPPORT PUBLIC TRUST DETERMINATIONS

1. Presidential Appointees or CAC eligible contract employees under the terms of applicable contracts will need to initiate a National Agency Check with Inquiries (NACI); National Agency Check (NAC), Law Checks and credit or an initiated national security investigation; and a favorable completion of a Federal Bureau of Investigation fingerprint check for credential issuance.The USD (P&R) and DoD lead for Homeland Security Presidential Directive-12 will work with the Office of Personnel Management to integrate the NACI status and fingerprint check information into the CAC issuance process.

2. Contract support entities that require the CAC to perform their government contract duties will submit a Standard Form (SF) 85 “Suitability for employment” or SF-85P “Questionnaire for Public Trust Positions,” and two copies of the DD Form 258 “Applicant Fingerprint Card” to the Office of the Command Security Manager.

3. All suitability/trustworthiness determinations are adjudicated by the Department of the Navy, Central Adjudication Facility (DON CAF) favorable suitability/trustworthy

determinations. The scope of suitability/trustworthiness investigations does not meet the standards for security clearance eligibility.

4. DON CAF will enter all determinations into the JPAS. Contract entities are responsible for determining when the DON CAF has completed adjudication by reviewing the notification status of their respective personnel in JPAS. When the determination is posted, the contract facility may request the issuance of the CAC using the Contract Verification System procedures.

5. When the DON CAF returns the NACI with a “No determination made”, it is the requesting organization that must make the adjudication determination to whether or not the contract employee is suitable for government service.

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 *(YYYYMMDD)*

3. THIS SPECIFICATIONS: *(X and complete as applicable)*
a. ORIGINAL *(Complete date in all cases)* — DATE *(YYYYMMDD)*
b. REVISED *(Supersedos all previous specs)* — REVISION NO. — DATE *(YYYYMMDD)*
c. FINAL *(Complete Item 5/n all cases)* — DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? j YES L._jNO. If *Yes,* complete the following:
Classified mater al received or generated under *(Preceding Contract Number)* Is transferred to this follow-on conttact.

5. IS THIS A FINAL DO FORM 254? L._jYES L._jNO. If *Yes,* complete the fOllowing:
In response to the contractor's request dated .retention of the classified mater al is authorized for the period of

6 CONTRACTOR *(Inclucle Commercial and Government EnUty (CAGE) Cocle)*
a. NAME, ADDRESS, AND ZIP CODE
Enter the Prime Contractor Here
b. CAGE CODE
c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Cocle)*
Enter DSS Field Office or cognizant command

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

8. ACTUAL PERFORMANCE
a. LOCATION
Enter location where work is to be performed. If multiple, use bldck 13 or addendendum sheet
b. CAGE CODE
c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Enter DSS Field Office or cognizant command

9. GENERAL IDENTIFICAT ON OF THIS PROCUREMENT

10. CONTRACTOR WILL REQU RE ACCESS TO:	YES	NO	11. IN PERFORMNG THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATON			a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RESTRICTED DATA			b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. CRITICA NUCLEAR WEAPON DES GN INFORMATION			c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FORMERLY RESTRICTED DATA			d. FABRICATE, MODIEY OR STORE CLASSIFIED HARDWARE		
e. INTELLIGENCE INFORMATION			e. PERFORM SERVCES ONeY		
(1) Sensitive Compartmented Information (SCI)			f. HAVE ACCESS TO U.S. 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 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)*					

DO FORM 254, DEC 1999 PREVIOUS EDITION IS OBSOLETE.

Figure 11-1.--Sample DD 254

Enclosure (1)

12. PUBLIC RELEASE. Any information *(classirled or unclassified)* pertaining to this cont-act shall not be released for public disseminatJon except as provided by the Industrial Security Manualor 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 Directt Through (Specify) to the Directorate ror Freedom of Information and Security Review, Office *of* the Assistant SccrctiJry *of* Defense (Public Affairs).. for review. •tn the case *of* non-OoD Usef Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classifiection guidance needed for this classified effort is Identified below. If any difficulty Is encountered in applying this guidance or if any othef 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 ofncialk:tentified below. Pending final decision. the information Involved shall be handled and protected at the highest levelof classifiCation assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or fOfWllrd under sepdrate correspondeQce, any documenrs/guides/extracrs referenced herein. Add additional pages as needed to provide complete guicknce.)*

Use this item to identify applicable guides, to provide na rAtive guidance which identifies the specific types of information to be classified, to provide down-"- grading or declassification instructions, to provide any special instructions, explanations, comments or statements required for information or to clarify any other items on the DD 254. Each contract is unique in its performance requirements. Write the guidance in plain english. It's not necessary to put all the g :l.dance in this space. Use additional pages as needed to expand or explain.

The DD 254, with its attachments, 1!3·the only authorized means for providing classification guidance to a contractor. It should be written as specifically as possible and include only that information that pertains to the contract for which it is issued. It s hould not contain reference to internal DON directives or instructions unless such documents Erovide instructions aE12licable to the contract. If so, the pertinent portions should be extracted and'provided as attachments. All documents referenced or cited in item 13 should be provided to the contractor, either as attachments or under separate cover if they are classified. Reguirements of the NISPOM should not be cited. . Security classifi- cation guidance provides detailed information regarding what information require! classification, at what level, and assigns downgrading or declassification instructions that apply to the information or material generated by the contract or in performance of the contract.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirement>.in addition to ISM requrements.are establ ished for this contract. ▪ Yes ▪▪No
(If Yesidentify the pcrtinenr contracwal clauses in the contract document itself, or provide dn appropriate statement which idenrifies the additional requirements. Provide a copy of the requirements to the cognizant security ofrice. Use Item 13 if IJdditional space is needed.)

YES in this item signifies that security requirements over and above those of the NISPOM will be imposed. Costs are normally reimbursed to the contractor.

15. INSPECTIONS. Elements of this contract are outside the <nspection responsibility of the cognizant security off1ce. _ _ Yes No
(If Yes. explain Ind identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional Sp4Ce Is needed.

YES in this item relieves DSS of oversight of the contract.

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 effon. All questions shallbe referred to the officialnamed below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area fAde)*
R. L. Wheaton	Contracting Officer's Reoresentative	COM (202) 433-4444 DSN 288-4444

d. ADORES$ *(Include lip Code)*
Chief of Naval Operations (N09N2)
Washington Navy Yard, Building 176
Washington D. C. 20388-5381

·.siG/7/U

c22: _REQUIRED DISTRIBUTION
___ a CONTRACTOR
___ b SUBCONTRACTOR
___ c COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
___ d U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY AOMINISTRATION
___ e. AOMINISTRATIIIE CONTRACTING OFFICER
___ f. OTHERS AS NECESSARY

DO FORM 254 (BACK), DEC 1999

Figure 11-1.--Sample DD 254 Continued

Enclosure (1)

PROCESS FOR THE FLOW OF DD 254

Requirements:	-A DD 254 is required when a procurement package (either pre or post award) requires access to, or generation of classified information by a contractor.
Activity (Customer-COR)	-Has a requirement that includes the contractor having access to classified material
Activity (Customer–COR)	-Generates draft Statement of Work (SOW) and DD 254 with attachments for solicitation process. -DD 254 will include purchase request number in Block 2c (Provided by RCO) and is forwarded to the Command Security Manager (B 054) with Attachment(s) and a copy to the SOW for review/signature and return to the activity.
Activity (Customer–COR)	-Forward completed DD 254 to Regional Contracting Officer (RCO) for processing. (DD 254 must be signed by a Security Specialist (080/COSR) prior to submission to RCO).
Regional Contracting Office	-Determines Awardees. -Generates contract. -Assigns Prime Contract Number, to include expiration date in (Block 2a) of DD 254 (**Note**: **expiration date shall include all option periods.)** -Completes block 6a, 6b and 6c of the DD 254. -Forwards DD 254 to Command Security Manager (B 054) for review/signature. -If an option is not exercised, notify the Security Manager at the conclusion of the contract.

Figure 11-1.--Sample DD 254 - Continued

Enclosure (1)

Command Security Manager	-Verifies/Corrects contractor information on DD 254. -Signs DD 254 (Retain copy/forward copy to CMCC). -Returns original DD 254 to activity for action as appropriate*.

*Process is the same once the bid is completed and **Original** Contract is generated.

* If a contractor has a requirement to hold classified material beyond the expiration of a contract, they must request authorization in writing. Activity COR will prepare **Final** DD 254 for signature by the Command Security Manager (Security Specialist/COSR). Final Signed copy of DD 254 is sent to RCO, CMCC, and interested parties.

Figure 11-1.--Sample DD 254 - Continued

INFORMATION SECURITY PROGRAM

CHAPTER 12

LOSS OR COMPROMISE OF CLASSIFIED INFORMATION

12000. BASIC POLICY. There are two types of security violations. One results in a compromise or a possible compromise of classified information. The other is when security regulations are violated but no compromise occurs. Compromise is the disclosure of classified information to a person who is not authorized access. Security violations of either type must be reported to the Command Security Manager, Marine Corps Base, Quantico (MCBQ) (B 054) where a vigorous inquiry/investigation will be initiated and the problems causing the violation corrected rather than covered up. Amplifying instructions are contained in Chapter 12 of reference (d).

12001. DISCOVERY OR SUBJECTION TO COMPROMISE

1. An individual who becomes aware of a compromise or subjection to compromise of classified information will immediately notify the activity security head, activity security manager, and the custodian. Once notified, all pertinent information will be reported to the command security manager, by telephone. Immediately follow up with a brief typed report or email. If the individual believes the commanding officer or Security Manager may be involved in the incident, the next higher echelon of command must be notified. If circumstances of discoveries make such notification impractical, the individual shall notify the commanding officer or Security Manager at the most readily available command, or contact the local National Criminal Investigative Service office.

2. Initial reports shall briefly address the circumstances causing the incident, pinpoint responsibility and attempt to determine the degree of compromise.

12002. PRELIMINARY INQUIRIES (PI)

1. Upon receiving a report of a security violation, the Command Security Manager will direct a PI in accordance with Chapter 12 of reference (d). Normally the inquiry will be conducted by the activity having custodial responsibility of the material.

When investigative support is required or circumstances warrant the use of trained investigators, the Commander, MCBQ may request that Naval Criminal Investigative Service personnel assist in or conduct the preliminary inquiry. When a PI is directed, the inquiry will be completed quickly, usually within 72 hours. The Commander, MCBQ will, upon receipt, comply with the guidance set forth in Chapter 12 of reference (d).

2. The overriding priority, upon receiving a report of a compromise or subjection to compromise is to regain custody of classified material or contain spillages where possible.

12003. JUDGE ADVOCATE GENERAL (JAG) PROCEDURES. In the event a PI indicates or recommends that a JAGMAN investigation is appropriate, the Command Security Manager will forward the PI and all known facts to the Chief of Staff, MCBQ for review and command action. Generally a JAGMAN is not warranted or required unless a PI indicates criminal activity, espionage or when punitive action
is anticipated. During the course of a JAGMAN, the Command Security Manager will provide expert interpretation of security regulations where classified material or other security-related incidents are involved.

12004. UNSECURED CONTAINERS

1. In the event that an open container is found, a 100 percent inventory of the containers contents will be made and a copy of said inventory forwarded to the Head, Classified material Control Center (CMCC) (B 054).

2. In the absence of assigned personnel, a security container or secure room in which classified material is stored is found unlocked; report the incident immediately to the duty officer. The container will be guarded until the duty officer arrives, the duty officer will contact the person or persons responsible by phone, starting with the first person indicated on the SF 700 form fixed to the inside of the control drawer. The first person contacted is required to report in person and conduct a complete inventory in the presence of the duty officer. A copy of the inventory will be forwarded to the Head, CMCC. If no contact is made, the duty officer will lock the container and record the event in the official log. The Command Security Manager will direct that a PI be conducted in all cases where a possible compromise of classified material is suspected.

12005. IMPROPER TRANSMISSION. When an individual aboard this Base receives classified material that shows improper handling, notify the Command Security Manager, MCBQ (B 054).

12006. INFORMATION SYSTEMS. In addition to the above, any security violations involving computers, computer systems, and networks (SIPRNet/NIPRNet) must be immediately reported, to the Command Security Manager, and the Information Assurance Manager G-6 MCBQ. Examples of such violations are lost or missing computers and hard drive, computers and hard drives that are found, and known or suspected spillages. Immediate spillage reporting cannot be overemphasized due to the nature of the violation and how quickly some spillages can spread if not immediately contained.

APPENDIX A

DEFINITIONS AND ABBREVIATIONS

Access - The ability and opportunity to obtain knowledge or possession of classified information.

Access Authorization - A formal determination that a person meets the personnel security requirements for access to classified information of a specified type or types.

Account Manager - The individual responsible for establishing local JPAS access and monitoring and controlling system access thereafter. The Security Manager is unusually the JPAS account manager.

Acquisition Systems Protection (ASP) - A program designed to identify and protect classified information or controlled unclassified information that has been identified as critical to the combat effectiveness of systems being developed within the DON acquisition programs.

ACES - The Automated Continuous Evaluation System is a Defense Security Service managed tool for querying automated national and local record sources for security significant information regarding DoD employees determined to be eligible for access to classified information or assignment to sensitive duties.

Adjudication - The process of an examination of a sufficient amount of information regarding an individual to determine whether the individual is an acceptable security risk. A determination that a person is an acceptable security risk equates to a determination of eligibility for access to classified information and/or sensitive duty assignment.

Adverse Action - A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less.

Adverse Information - Any information that adversely reflects on the integrity or character of an individual, which suggests that the individual's ability to safeguard classified information may be impaired or that the individual's access to classified information clearly may not be in the best interest of national security. See Issue Information.

Agency - Any "Executive agency," as defined in 5 U.S.C., 105; any "Military Department" as defined in 5 U.S.C. 102; and any other entity within the Executive Branch that comes into the possession of classified information. The DON is an agency but each DON command is not; rather, a command is part of an agency. Within the DoD, the Departments of the Army, Navy, and Air Force are agencies as well as the Defense Intelligence Agency, the National Security Agency and the National Reconnaissance Office.

Alternative Compensatory Control Measures (ACCM) – Used when an Original Classification Authority (OCA) determines that other security measures (as detailed in this instruction) are insufficient for establishing "need-to-know" for classified information, and where Special Access Program (SAP) controls are not warranted. The purpose of ACCM is to strictly enforce the "need-to-know" principle.

Appeal - A formal request, submitted by an employee or applicant under the provisions of EO 12968, sec. 5.2, for review of a denial or revocation of access eligibility.

Assist Visit - The informal assessment of the security posture of a command to be used as a self-help tool.

Associated Markings - The classification authority, office of origin, warning notices, intelligence markings, other special control markings, and declassification/downgrading instructions of a classified document.

Attestation - A verbal pronouncement by individuals prior to being granted initial Top Secret, Special Access Program (SAP) or Sensitive Compartmented Information (SCI) access.

Authorized Investigative Agency - An agency authorized by law or regulation to conduct a counterintelligence investigation or a personnel security investigation of persons who are nominated for access to classified information, to ascertain whether such persons satisfy the standards for obtaining and retaining access to classified information.

Authorized Person – A person who has a need-to-know for the specified classified information in the performance of official duties and who has been granted an eligibility determination and access at the required level.

Automatic Declassification - The declassification of information based upon the occurrence of a specific date or event as determined by the OCA or the expiration of a maximum time frame for duration of classification established under Executive Order 13526, as Amended.

Caution-Proprietary Information Involved (PROPIN) – Intelligence control marking used, with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value.

Classification - The determination by an authorized official that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure.

Classified Contract - Any contract that requires or will require access to classified information by a contractor or its employees in the performance of the contract.

Classified National Security Information (or "Classified Information") - Information that has been determined to require protection against unauthorized disclosure in the interest of national security and is classified for such purpose by appropriate classifying authority per the provisions of Executive Order 13526, as Amended, or any predecessor Order.

Classification Management - The management of the life cycle of classified information from its inception to its eventual declassification or destruction.

Classified Material - Any matter, document, product or substance on or in which classified information is recorded or embodied.

Classified Material Control Center (CMCC) - Is not defined in other policy documents though it is typically understood to mean a location through which a command controls classified documents and material. It may be as elaborate as a vault with multiple security specialists to a two drawer GSA approved security container in a corner of an office. Regardless of the size or scope of a command’s classified holdings, the term CMCC describes that place and/or which controls those classified holdings.

Classifier - An approved official who makes a classification determination and applies security classification to information. A classifier may be an approved OCA, designated in exhibit 4A, of reference (d) or a derivative classifier who assigns a security classification based on a properly classified source or classification guide.

Clearance - A formal determination that a person meets the personnel security eligibility standards and is thus afforded access to classified information. There are three types of clearances: Confidential, Secret, and Top Secret. A Top Secret clearance implies an individual has been determined by an authorized adjudicative authority to be eligible for access to Top Secret, and has access to the same; a Secret clearance implies an individual has been determined to be eligible for Secret, and has access to the same; and a Confidential clearance implies and individuals has been determined to be eligible for access to Confidential, and has access to the same.

Clearance Eligibility - A formal determination by an approved adjudicative authority that a person meets the EO 12968 personnel security eligibility standards for access to classified information. There are three levels of clearance eligibility: Confidential, Secret, and Top Secret. Eligibility is established at the highest levels supportable by the prerequisite personnel security investigation.

Cleared Contractor - Any industrial, educational, commercial, or other entity, grantee, or licensee, including an individual that has executed an agreement with the Federal Government and granted an FCL by the CSA for the purpose of performing on a classified contract, license, IR&D program, or other arrangement that requires access to classified information.

Cleared DoD Contractor Employee - As a general rule, this term encompasses all contractor employees granted a personnel security clearance under the NISP.

Cognizant Security Agency - Agencies of the Executive Branch that have been authorized by Executive Order 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry.

Cognizant Security Office (CSO) - An office functioning on behalf of the Cognizant Security Agency responsible for establishing an industrial security program for the purpose of

safeguarding classified information disclosed or released to U.S. industry. A CSO is designated for each contract issued by the Cognizant Security Agency.

Collateral Information - Information identified as NSI under the provisions of Executive Order 13526, as Amended, but which is not subject to enhanced security protection required for SAP or other compartmented information.

Command - For the purpose of this regulation, any organizational entity under one official authorized to exercise direction and control. The term includes, base, station, unit, laboratory, installation, facility, activity, detachment, squadron, and ship.

Commanding Officer - For the purpose of this Order, the Commanding Officer is the head of any DON organizational entity to include those in the position as “Acting”. The term includes commander, commanding officer, Commander, director, officer in charge, and any other title assigned to an official, military or civilian, who, through command status, position or administrative jurisdiction, has the authority to render a decision with regard to a specific issue under consideration.

Communications Security (COMSEC) - The protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications.

Compromise - An unauthorized disclosure of classified information to one or more persons who do not possess a current valid security clearance.

Continuous Evaluation - The process by which all individuals who have established security clearance eligibility are monitored to assure they continue to meet the loyalty, reliability and trustworthiness standards expected of individuals who have access to classified information. The monitoring process relies on all personnel within a command to report questionable or unfavorable security information that could place in question an individual's loyalty, reliability, or trustworthiness.

Continuous Service - Includes honorable active duty; attendance at the military academies; membership in ROTC scholarship program; Army and Air Force National Guard membership; service in the military Ready Reserve forces (including active status);

civilian employment in government service, employment with a cleared contractor or employment as a consultant with access to classified information under the National Industrial Security Program. For security clearance purposes continuous service is maintained despite changes from one of the above statuses to another as long as there is no single break in service greater than 24 months.

Confidential – A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security, that the OCA is able to identify or describe (Executive Order 12598, as Amended).

Confidential Source - Any individual or organization that has provided, or may provide, information to the U.S. on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

Constant Surveillance Service (CSS) - A transportation protective service provided by a commercial carrier qualified by the SDDC to transport classified shipments.

Continental United States (CONUS) - United States territory, including adjacent territorial waters, located within the North America continent between Canada and Mexico.

Contracting Command - A DON command with procurement authority to award contracts to industry.

Contracting Officer - A Government official, who, per the departmental or agency procedures, currently is designated as a contracting officer with the authority to enter into and administer contracts, make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representatives of the contracting officer, acting within the limits of their authority.

Contracting Officer's Security Representative (COSR) - A security specialist at a DON contracting command who has been appointed as a COSR and delegated authority on behalf of the command for the security administration of classified contracts. The COSR serves as the responsible official for any problems or questions related to security requirements and/or classification guidance for classified contracts.

Controlled Access Area (CAA) – IA Term – A physical area (e.g., building, room etc.), which is under physical control and to which only personnel cleared to the level of the information processed are authorized unrestricted access, open storage is not authorized in a true CAA.

Controlled Cryptographic Item - A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, that is unclassified when un-keyed (or when keyed with unclassified key) but controlled.

Controlled Unclassified Information (CUI) – Official information not classified or protected under Executive Order 13526, as Amended, or its predecessor Orders that requires the application of controls and protective measures for a variety of reasons.

Counterintelligence (CI) – Intelligence activity, with its resultant product, intended to detect, counteract, and/or prevent espionage and other clandestine activities, sabotage, international terrorist activities, or assassinations.

Critical Nuclear Weapons Design Information (CNWDI) – Top Secret or Secret RD revealing the theory of operation or design of the components of a thermonuclear or implosion type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable and high explosive material by type. Among these excluded items are the components that personnel set, maintain, operate, test, or replace.

Critical Technology – Technology that consists of: (1) Arrays of design and manufacturing know-how (including technical data); (2) Keystone manufacturing, inspection, and test equipment; (3) keystone materials; and (4) goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the U.S. (also referred to as militarily critical technology).

Cryptology – The branch of knowledge that treats the principles of cryptography and cryptanalysis; and the activities involved in SIGINT and maintaining COMSEC.

Custodian or Custodial Command – The individual or command who has possession of, or is otherwise charged with the responsibility for safeguarding classified information.

Damage to the National Security – Harm to the national defense or foreign relations of the U.S. resulting from the unauthorized disclosure of classified information.

Declassification – The determination by an authorized official that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure.

Declassification Authority – The official who authorizes original classification, if that official is still serving in the same position; the originator's current successor in function; a supervisory official of either; or officials delegated declassification authority, in writing, by the agency head or the senior agency official.

Deliberate Compromise – Any intentional act of conveying classified information to any person not officially authorized to receive it.

Derivative Classification – The incorporating, paraphrasing, restating, or generating, in new form, information that is already classified and ensuring that it continues to be classified by marking or similar means when included in newly created material.

Dissemination and Extraction of Information Controlled by the Originator (ORCON) – Most restrictive intelligence control marking used to enable the originator to maintain continuing knowledge and supervision of distribution of the intelligence beyond its original dissemination.

Disclosure – Conveying classified information to another person.

Distribution Controlled Information – Classified or unclassified information assigned distribution statements by the generating and/or responsible organizations to determine its distribution availability.

Document – Any physical medium such as any publication (bound or unbound printed material such as reports, studies, manuals), correspondence (such as military and business letters and

memoranda), electronic media, audio-visual material (slides, transparencies, films), or other printed or written products (such as charts, maps) on which information is recorded or stored.

DoD Component – The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, and the Defense agencies.

Downgrading – The determination by an approved authority that information classified at a specific level requires a lower degree of protection, therefore, reducing the classification to a lower level.

Due Process – Established procedures in presenting a preliminary unfavorable security clearance eligibility determination to the individual via their command, review of the individual's response, DoD CAF's final determination, and the appeals board decision.

Duration of Classification – A specific date or event, as established by the original classification authority, for automatic declassification of information based upon the duration of the national security sensitivity of that information as established by Executive Order 12598, as Amended.

Electronic Key Management System (EKMS) – Consists of four tiers designed to provide an integrated, end-to-end key management, and Communications Security (COMSEC) material generation, distribution, and accounting system for the Department of Defense (DoD) and civilian agencies.

Electronic Media – Used on Information Technology Systems to store or transfer information (i.e., Universal Serial Bus drives, flash drives, thumb drives, pen drives, compact disks, scanners, videotapes, floppy disks, recordings, etc.).

Eligibility – A determination made by a DoD Central Adjudication Facility, based upon favorable review of a standardized personnel security investigation, than an individual meets EO 12968 National Security Adjudicative Standards and is therefore eligible for access to classified national security information or assignment/retention in sensitive national security duties, or other designated duties requiring national security investigation and adjudication.

Employee – A person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

Entrance National Agency Check (ENTNAC) – An FBI fingerprint check conducted on first term military enlistees **e-Qip.** The Electronic Questionnaires for Investigations Processing is a software system developed by OPM which allows applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to their employing agency or security management office for review and approval of the personnel security investigation request.

Exception – An adjudication decision to grant or continue a security clearance or SCI access despite a failure to meet adjudicative or investigative standards. The head of the agency concerned or designee will make such decisions. An exception precludes reciprocity without review of the case by the gaining organization or program. Although they seldom occur, here are three types of exceptions granted by the DON CAF:

Condition: Clearance or SCI access granted or continued with the proviso that one or more additional measures will be required.

Deviation: Clearance or SCI access granted or continued despite either a significant gap in coverage or scope in the investigation or an out-of-date investigation.

Waiver: Clearance or SCI access granted or continued despite the presence of substantial issue information that would normally preclude access.

Event – An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification or downgrading of information.

Escort – To accompany, guide, usher, lead, attend, shepherd, or aid a person or group of people. In a classified environment escorts will not leave un-cleared persons unattended for any reason.

Exception – A written, CNO (N09N2)-approved long-term (12 months or longer) or permanent deviation from a specific safeguarding requirement of this regulation. Exceptions require compensatory security measures.

Facility Access Determination (FAD) – A process whereby Commanding Officers, in their responsibilities under the Internal Security Act of 1950 to protect persons and property under their command against the actions of untrustworthy persons, may request personnel security investigations and review the results to determine whether to allow the identified person(s) access to facilities under the commanding officer's control.

Facility Security Clearance (FCL) – An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

For Official Use Only (FOUO) – A marking applied to unclassified information that meets one or more exemptions of the Freedom of Information Act (FOIA) under Title 5 U.S.C., Section 522 (b) (2) through (9). Information must be unclassified to be designated FOUO. Declassified information may be designated FOUO, if it qualifies under exemptions 5 U.S.C. 522 (b) (2 through 9).

For Official Use Only Law Enforcement Sensitive (FOUO-LES) – A marking applied to unclassified information that meets one or more exemptions of the Freedom of Information Act (FOIA) under Title 5 U.S.C., Section 522 (b)(2) through (9). It is intended to denote that the information was compiled for law enforcement purposes.

Foreign Government - Any national governing body organized and existing under the laws of any country other than the U.S. and its possessions and trust territories and any agent or instrumentality of that government.

Foreign Government Information (FGI) - Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; information produced by the U.S. under or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

Information received and treated as FGI under the terms of a predecessor Order to Executive Order 13526, as Amended.

Foreign Intelligence - The product from collection, evaluation, analysis, integration, and interpretation of intelligence information about a foreign power and which is significant to the national security, foreign relations, or economic interests of the U.S. and which is provided by a Government agency that is assigned an intelligence mission.

Foreign National - Any person who is not a US citizen or US national, and/or representatives of foreign interests (see Non US Citizen). American citizens representing foreign governments, foreign private interests, or other foreign nationals are considered to be foreign nationals for purposes of this regulation, when acting in the capacity of a foreign representative.

Foreign Recipient - A foreign government or international organization to whom the U.S. is providing classified information.

Formerly Restricted Data (FRD) - Information removed from the DOE RD category upon a joint determination by the DOE (or antecedent agencies) and the DoD that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as RD.

Government-to-Government - Transfers by government officials through official channels or through other channels specified by the governments involved.

Head of DoD Component - The Secretary of Defense, the Secretary of the Navy, the Secretaries of the other military departments, the Chairman of the Joint Chiefs of Staff, the Commanders of Unified Combatant Commands, and the Directors of Defense Agencies.

Immediate Family - Any and all of the following are members of a person's immediate family: father, mother, brother, sister, spouse, son, and daughter. Each of these terms includes all of its variants; e.g., "sister" includes sister by blood, sister by adoption, half-sister, stepsister, and foster sister. For

purposes of determining security clearance and SCI access, cohabitants have a status identical to that of immediate family.

Immigrant Alien - Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

Incident Report - A report of developed issue information forwarded to the CAF through JPAS.

Industrial Security - That portion of information security that is concerned with the protection of classified information entrusted to U.S. industry.

Information - Any official knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Information Assurance - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance Manager (IAM) - Responsible for the information assurance program for a DON information system or organization. This individual is responsible for creating the site accreditation package. The IAM functions as the Command's focal point on behalf of and principal advisor for IA matters to the Designated Approving Authority (DAA). The IAM reports to the DAA and implements the overall IA program. Previously called the Information Systems Security Manager (ISSM) and ADP Systems Security Officer (ADPSSO).

Information Assurance Officer (IAO) - Implements and enforces system-level IA controls in accordance with program and policy guidance. Previously called the Information Systems Security Officer (ISSO).

Information Security - The system of policies, procedures, and requirements established under the authority of Executive Order 13526, as Amended, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

Information Technology (IT) - Any equipment or interconnected system or subsystem of IT equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Infraction - Any knowing, willful, or negligent action contrary to the requirements of Executive Order 13526, as Amended, or its implementing directives that does not comprise a "violation."

Inspection - An official examination of the security posture of a command to determine compliance with IPSP policy.

Intelligence - The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information that concerns one or more aspects of foreign nations or of areas of foreign operations, and that is immediately or potentially significant to military planning and operations.

Intelligence Activity - An activity that an agency within the intelligence community is authorized to conduct under Executive Order 12333.

Intelligence Community - U.S. organizations and activities identified by Executive Order 12333 as making up the Community. The following organizations currently comprise the Intelligence Community: CIA; NSA; DIA; special offices within the DoD for the collection of specialized foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the DOS; the intelligence elements of the military services, FBI, DEA, Departments of Treasury and Energy and the DEA; and staff elements of the Office of the DCI.

Inventory - The process of accounting for classified information.

Interagency Security Classification Appeals Panel (ISCAP) – A panel that will (1) decide on appeals by persons who have filed classification challenges; (2) approve, deny, or amend agency exemptions for automatic declassification; and (3) decide on appeals by persons or entities who have filed requests for mandatory declassification review.

Issue Information - Any information that could adversely affect a person's eligibility for access to classified information. See Adverse Information.

Minor Issue Information - Information that, by itself, is not of sufficient importance, or magnitude to justify an unfavorable administrative action in a personnel security determination.

Substantial Issue Information - Any information, or aggregate of information that raises a significant question about the prudence of granting a security clearance or SCI access. Normally, substantial issue information constitutes the basis for a determination made with waiver or condition, or for denying or revoking a security clearance or SCI access.

Judge Advocate General (JAG) Manual Investigation - A proceeding conducted per chapter II of the Manual of the Judge Advocate General. It is usually ordered by the command having custodial responsibility for the classified information that has been compromised or subjected to compromise.

Limited Access Area (LAA) – IA Term – A physical area (e.g., a military base in the U.S.) that is under direct U.S. physical control and to which only authorized personnel are admitted.

Limited Distribution – A caveat used only by the National Geospatial-Intelligence Agency (NGA) to identify a select group of sensitive but unclassified imagery or geospatial information and data created or distributed by NGA or information, data and products derived from such information.

Local Agency Checks (LACs) - A check of civilian law enforcement, criminal, civil courts, etc., where an individual has resided or been employed within the scope of an investigation. This check can only be accomplished by either the DSS or OPM.

Local Records Check (LRC) - A command review of available personnel, medical, legal, security, base/military police and other command records. A review of local civilian law enforcement records, the National Crime Information Center (NCIC), and the servicing NCIS office is prohibited.

Mandatory Declassification Review - Review for declassification of classified information in response to a request for declassification that meets the requirements under Section 3.5 of Executive Order 13526, as Amended.

Marking - The physical act of indicating on classified material the assigned classification, changes in classification, downgrading and declassification instructions, and any limitations on the use of the classified information.

Multiple Sources - Two or more source documents, classification guides, or a combination of both.

National Agency Check (NAC) - A review of records of certain national agencies, including a technical fingerprint search of the files of the Federal Bureau of Investigation.

National Agency Check Plus Written Inquiries and Credit Check (NACIC) - A review of documents and records conducted by the Office of Personnel Management (OPM), including a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references, schools and financial institutions.

National Agency Check with Local Agency Checks and Credit Check (NACLC) - The personnel security investigative requirement developed under EO 12968 for persons who will require access to Secret and Confidential classified information. A NACLC covers the past 5 years and consists of a NAC, a financial review, certification of date and place of birth, and LACs. The NACLC is the minimum investigative requirement for military service, and is the re-investigative requirement for continued access to Secret and Confidential classified information (sometimes previously referred to as a Secret PR (SPR) or Confidential PR (CPR).

National Industrial Security Program (NISP) - National program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the U.S. Government and serves as a single, integrated, cohesive industrial security program to protect classified information and preserve U.S. economic and technological interests.

National Security - The national defense or foreign relations of the U.S.

National Security Information (NSI) - Any official information that has been determined under Executive Order 13526, as Amended, or any predecessor order to require protection against unauthorized disclosure and is so designated. The designations Top Secret, Secret, and Confidential are used to identify such information and are usually referred to as "classified information."

Naval Nuclear Propulsion Information (NNPI) - All information, classified or unclassified, concerning the design, arrangement, development, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval

nuclear powered ships and prototypes, including the associated nuclear support facilities.

Need-to-know - A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized U.S. Governmental function.

Network - A system of two or more computers that can exchange data or information.

Nickname - A combination of two separate unclassified words, assigned an unclassified meaning that is employed for unclassified, administrative, morale, or public information purposes.

Nondisclosure Agreement (NdA) - An agreement between an individual who will be permitted access to classified national security information and the United States government, acknowledging and agreeing to obligations for protecting national security information. All personnel must execute the Standard Form 312 Nondisclosure Agreement as a condition of access to classified information.

Non-Privileged Access - IT Access that provides no capability to alter the properties, behavior or control of the information system/network. Also know as “User level access,” non-privileged access is typically controlled and limited to preclude intention or unintentional adverse impact to sensitive data or other resources within the IT environment.

Non US Citizen. - Any person who is not a US citizen or US national, usually used when referring to DON employees or affiliates who are not U.S. citizens (see United States Citizen).

Not Releasable to Foreign Nationals (NOFORN) – An intelligence control marking used to identify intelligence which an originator has determined falls under the criteria of DCID 6/7, and may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval.

North Atlantic Treaty Organization (NATO) – A military alliance of 26 countries from North America and Europe.

Official Information - Information that is owned by, produced for or by, or is subject to the control of the U.S. Government.

Original Classification - An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Original Classification Authority (OCA) - An official authorized in writing, either by the President, an agency head, or other official designated by the President "to classify information originally" or "to make an original classification decision."

Patent Secrecy Act – Protection of information in which the U.S. Government has a property interest that if published (i.e., an application or the granting of a patent) might be detrimental to the national security. It is governed by Title 35 U.S.C., Section 181.

Personnel Identifying Data - Personal information, e.g., date and place of birth, SSN, citizenship, used to identify an individual on personnel security questionnaire and in personnel security automated systems such as JPAS.

Personnel Security Investigation (PSI) - Any investigation conducted for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DoD, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties or access requiring such investigation. PSIs are conducted for the purpose of making initial personnel security determinations and to resolve allegations that may arise subsequent to a favorable personnel security determination to Ascertain an individual's continued eligibility for access to classified information or assignment or retention in a sensitive position.

Permanent Historical Value - Those records that have been identified in an agency's records schedule as being permanently valuable.

Possessions - U.S. possessions are the U.S. Virgin Islands, Guam, American Samoa (including Swain's Island), Howland Island, Baker Island, Jarvis Island, Midway Islands (this consists of Sand Island and Eastern Island), Kingman Reef, Johnston Atoll, Navassa Island, Northern Mariana Islands, Wake Island, and Palmyra Atoll.

Preliminary Inquiry (PI) - The "initial" process to determine the facts surrounding a possible loss or compromise. A

narrative of the PI findings is required when there is a loss or compromise of classified information. All preliminary inquiries must be documented for record purposes.

Privileged Access - Authorized access that provides capability to alter the properties, behavior or control of the information system/network. It includes, but is not limited to: “Super user,” “root,” or equivalent access, such as access to the control functions of the information system/network, administration of user accounts, etc; access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system/network equipment or software; ability and authority to control and change program files, and other users’ access to data; direct access to operating system level functions (also called unmediated access) which would permit system controls to be bypassed or changed; access and authority for installing, configuring, monitoring or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operation.

Program Protection Plan (PPP) - The PPP is the program manager's single source document used to coordinate and integrate all protection efforts designed to deny access to Critical Program Information to anyone not authorized or not having a need-to-know and prevent inadvertent disclosure of leading edge technology to foreign interests. If there is to be foreign involvement in any aspect of the program, or foreign access to the system or its related information, the PPP will contain provisions to deny inadvertent or unauthorized access.

Program Review - Formal assessment of the security posture of a command to be used in improving the management of the ISP.

Protected Distribution System (PDS) – Information Assurance term, used to transmit unencrypted NSI through common areas, continued physical security integrity after installation is critical.

Protective Security Service (PSS) - A transportation protective service provided by a cleared commercial carrier qualified by the SDDC to transport Secret material.

PSAB - The Personnel Security Appeals Board (PSAB) is the appellate authority for appeals of unfavorable DON CAF eligibility determinations.

Qualified Contractor - A private individual or enterprise located in the U.S. or Canada whose eligibility to obtain unclassified export controlled technical data has been established following certification of an Export-Controlled DoD and Canada Technical Data Agreement, DD 2345.

Reciprocity - Acceptance by one agency or program of a favorable security clearance eligibility determination, made by another. Reciprocity does not include agency access determinations or employment suitability determinations.

Record - All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by any command of the U.S. Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that command or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the U.S. Government or because of the information value of data in them.

Reinvestigation - An investigation conducted for the purpose of updating a previously completed investigation of persons occupying sensitive positions, afforded access to classified information or assigned other duties requiring reinvestigation. The intervals of reinvestigation are dependent upon the sensitivity of the position or access afforded. A periodic reinvestigation of an SSBI is conducted at five-year intervals; a reinvestigation of a NACLC for Secret or Confidential access is conducted respectfully at 10 year and 15 year intervals.

Report of Investigation (ROI) - Official report of investigation conducted by agents of the NCIS.

Restricted Access Area (RAA) – **IA Term -** A physical area (e.g., building, room, etc.) that is under physical control and to which only personnel cleared to the level of the information being processed are authorized unrestricted access. Does not have open storage of classified information status.

Restricted Data (RD) - All data concerning: (1) Design, manufacture, or utilization of atomic weapons; (2) The production of special nuclear material; or (3) The use of SECNAV special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category under Section 142 of the AEA, as amended.

Retrieval and Analysis of Navy K(C) *C*lassified *In*formation (RANKIN) Program – Provides for the standardization, centralized management, and issuance of all DON security classification guides (SCGs) and maintenance of historical files for all DON SCGs.

Risk Management - The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.

Safeguarding - Measures and controls prescribed to protect classified information.

Scope - The time period to be covered and the sources of information to be obtained during the prescribed course of a PSI.

Secret - A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security, that the OCA is able to identify or describe (Executive Order 12598, as Amended).

Secure Room (SR) – Cleared building/room/area for open storage of classified material at the level authorized/certified. (See Exhibit 10A of SECNAV M-5510.36).

Security - A protected condition that prevents unauthorized persons from obtaining classified information of direct or indirect military value. This condition results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influence.

Security Classification Guide (SCG) - The primary reference source for derivative classifiers to identify the level and duration of classification for specific informational elements. DON OCAs are required to prepare an SCG for each system, plan, program or project under their cognizance that creates classified information.

Security-In-Depth - A determination by the commanding officer that a command's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the command. Examples include perimeter fences, employee and visitor access controls, use of IDSs, random guard patrols during non-working hours, closed circuit video monitoring, and other safeguards that reduce the vulnerability of unalarmed storage areas and security storage cabinets.

Security Management Office (SMO) - For purposes of JPAS, a Security Management Office is a local entity that has personnel security management jurisdiction.

Security Violation - Any failure to comply with the regulations for the protection and security of classified material.

Self-Inspection - The internal review and evaluation of a command or the DON as a whole with respect to the implementation of the program established under Executive Order 13526, as Amended, and it’s implementing directives.

Senior Agency Official (SAO) - The official designated by the agency head under section 54(d) of Executive Order 13526, as Amended, to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

Sensitive But Unclassified (SBU) - Information that is originated within the DOS and warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the FOIA. (Previously "Limited Official Use" (LOU) in the DOS).

Sensitive Compartmented Information (SCI) - Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

Sensitive Duties - Duties in which an assigned military member or civilian employee could bring about, by virtue of the nature of the duties, a material adverse affect on the national security. Any duties requiring access to classified information are sensitive duties.

Sensitive Information - Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine DON payroll, finance, logistics, inventory, and personnel management systems. Examples include FOUO, Unclassified Technical Data, State Sensitive but Unclassified (SBU), or Foreign Government information.

Sensitive Position - Any position so designated, in which the occupant could bring about, by virtue of the nature of the position, a materially adverse affect on the national security. All civilian positions within the DoD are designated special-sensitive, critical sensitive, noncritical-sensitive, or non-sensitive.

Short Title - A brief, identifying combination of words, letters, or numbers applied to specific items of classified information.

Signals Intelligence (SIGINT) - Intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

Significant Derogatory Information - (See Issue Information) Information that could, in itself, justifies an unfavorable administrative action, an unfavorable security determination, or prompts an adjudicator to seek additional investigation or clarification.

Single Integrated Operational Plan (SIOP) - A general war plan of the Joint Chiefs of Staff distributed by the Joint Staff Director of Strategic Target Planning (CNO N5 GP2).

Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI) - Detailed Top Secret SIOP information that is extremely sensitive in nature.

Single Scope Background Investigation (SSBI) - A personnel security investigation which provides extensive information regarding an individual, gathered from people and places where the individual has lived or worked. The period of investigation for a SSBI is variable, ranging from 3 years for neighborhood checks to 10 years for local agency checks. No investigative information will be pursued regarding an individual's life prior to their 16th birthday.

Source Document - An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Special Access Program (SAP) - Any DoD program or activity (as authorized in Executive Order 13526, as Amended) employing enhanced security measures (e.g., safeguarding or personnel

adjudication requirements) exceeding those normally required for classified information at the same classification level which is established, approved, and managed as a DoD SAP.

Spillage – Occurs when data is placed on an IT system possessing insufficient information security controls to protect the data at the required classification. Electronic spillage resulting in the compromise of classified information is subject to the requirements of this instruction.

Systematic Declassification Review - The review for declassification of classified information contained in records that have been determined by the Archivist of the U.S. to have permanent historical value in accordance with Chapter 33 of Title 44, U.S.C.

Technical Data - Recorded information related to experimental or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material. The data may be graphic or pictorial delineations in media such as drawings or photographs, text in specifications or related performance or design type documents, or computer printouts. Examples of technical data include research and engineering data or drawings, associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information and computer software documentation.

Technical Documents - Documents containing technical data or information.

Technical Information - Information, including scientific information, which relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment.

Telecommunications - The preparation, transmission, or communication of information by electronic means.

Temporary Access - A local determination to allow temporary access to classified information based on the favorable minimum investigative requirements, pending the completion of the full investigative requirements. (Temporary access to Sensitive Compartmented Information cannot be approved locally and must be requested from the DON CAF).

Tentative Classification – Allows those individuals without original classification authority, who create information they believe to be classified or which they have significant doubt about the appropriate classification, to mark the information accordingly.

Top Secret - A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security, that the OCA is able to identify or describe (Executive Order 12598, as Amended).

Transmission - Any movement of classified information from one place to another.

Transportation - A means of transport; conveyance of classified equipment or bulky shipments.

Unauthorized Disclosure - A communication or physical transfer of classified information to an unauthorized recipient.

Unclassified Controlled Nuclear Information (UCNI) - DoD or DOE unclassified information on security measures (including security plans, procedures, and equipment) for the physical protection of DoD Special Nuclear Material, equipment or facilities.

Unclassified Technical Data - Sensitive data related to military or dual-use technology, which is subject to approval, licenses or authorization under the Arms Export Control Act.

Uncontrolled Access Area (UAA) – IA Term - A physical area (e.g., military base in a foreign country) that is not under direct U. S. physical control and to which unauthorized personnel may gain access.

Unfavorable Administrative Action - Action taken as the result of an unfavorable personnel security determination including a denial or revocation of security clearance eligibility; denial or revocation of access to classified information, denial or revocation of a SAP or SCI access authorization; non-appointment to or non-selection to a sensitive position.

Unfavorable Personnel Security Determination - A determination based on an assessment of available information that an individual does not meet the standards required for access to classified information or assignment to sensitive duties.

United States and its Territorial Areas - The 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and those possessions listed in the definition above.

United States Citizens (including U.S. Nationals) - A person born in the United States or any of its territories, a person born abroad but having one or both parents who are themselves United States citizens, and a person who has met the requirements for citizenship as determined by the Immigration and Naturalization Service and has taken the requisite oath of allegiance.

United States National - A United States citizen, or a person who, though not a citizen of the United States, owes permanent allegiance to the United States. NOTE: Consult 8 USC. 1401(a)(1-7) whenever there is doubt whether a person qualifies as a national of the United States.

Upgrade - To raise the classification of an item of information from one level to a higher one.

Visitor Group - Cleared DoD contractor employees assigned to a DON command, normally in support of a classified contract or program, who occupy or share government spaces for a predetermined period.

Waiver - A written temporary relief, normally for a period of 1 year, from specific requirements imposed by this regulation, pending completion of actions which will result in conformance with the requirements. Interim compensatory security measures are required.

Working Papers - Documents and material accumulated or created while preparing finished material (e.g., classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents).

ABBREVIATIONS

-A-

AA&E - Arms, Ammunition and Explosives
ACDUTRA - Active Duty for Training
ACCM – Alternative Compensatory Control Measures
ACS - Access Control System
AEA - Atomic Energy Act
AECS - Access Entry Control Systems
AIS - Automated Information Systems
ANACI/ANCI - Access National Agency Check with Inquiries
AJ - Administrative Judge
ASCP – Automated Security Control Program
ASP - Acquisition Systems Protection

-B-

BI - Background Investigation
BUPERS - Bureau of Naval Personnel

-C-

C – Confidential
CAA – Controlled Access Area
CAF – Central Adjudication Facility
CAGE - Commercial and Government Entity Code
CFR - Code of Federal Regulation
CHNAVPERS - Chief of Naval Personnel
CI - Counterintelligence
CIA - Central Intelligence Agency
CHINFO - Chief of Information
CMC - Commandant of the Marine Corps
CMCC – Classified Material Control Center
CMS - Communications Security Material System
CNO - Chief of Naval Operations
CNR - Chief of Naval Research
CNWDI - Critical Nuclear Weapons Design Information
CO - Commanding Officer
COMNAVSECOMMANDERRU - Commander, Naval Security Group Command
COMSEC - Communications Security
CONUS – Continental United States
COR - Contracting Officer's Representative (formerly Contracting Officer's Security Representative)
CPR - Confidential Periodic Reinvestigation
CS - Critical-Sensitive

CSA - Cognizant Security Agency
CSO - Cognizant Security Office
CSP - Cryptographic Security Publication
CSS - Constant Surveillance Service
CUI – Controlled Unclassified Information
CUSR - Central U.S. Registry (NATO)
CVA - Central Verification Activity

-D-

DAA - Designated Approval Authority
DCI - Director, Central Intelligence
DCID - Director, Central Intelligence Directive
DCII - Defense Central Investigations Index
DCPDS - Defense Civilian Personnel Data System
NCMS - Navy, Communications Security Material System
DCS - Defense Courier Service
DEA - Drug Enforcement Agency
DEERS – Defense Enrollment Eligibility Reporting System
DFAS – Defense Finance & Accounting Service
DIA - Defense Intelligence Agency
DIRNCIS – Director, Naval Criminal Investigative Service
DISCO – Defense Industrial Security Clearance Office
DHS – Department of Homeland Security
DLSC - Defense Logistics Services Center
DNI - Director of Naval Intelligence
DOB – Date of birth
DoD - Department of Defense
DOE - Department of Energy
DOHA - Defense Office of Hearings and Appeals
DON CAF - Department of the Navy Central Adjudication Facility
DON CIO – Department of the Navy Chief Information Officer
DON - Department of the Navy
DOS - Department of State
DSS – Defense Security Service (formerly Defense Investigative Service)
DTS – Defense Transportation System
DUSD(PS) – Deputy Under Secretary of Defense for Policy Support
DUSD(CI&S) – Deputy Under Secretary of Defense for Counterintelligence and Security)
DUSD(TSP&NDP) – Deputy Undersecretary of Defense for Technology Security Policy and National Disclosure Policy)

-E-

EDVR – Enlisted Distribution Verification Report
EKMS – Electronic Key Management System

ENAC – Expanded National Agency Check
ENTNAC – Entrance National Agency Check
E.O. – Executive Order
EOD – Explosive Ordnance Disposal
EPSQ – Electronic Personnel Security Questionnaire
E-QIP – Electronic Questionnaires for Investigations Processing
ESS – Electronic Security System

-F-

FAA – Federal Aviation Administration
FAD – Facility Access Determination
FBI – Federal Bureau of Investigation
FCL – Facility (Security) Clearance
FFI – Full Field Investigation
FGI – Foreign Government Information
FI – Foreign Intelligence
FIPS – Federal Information Processing Standard
FMS – Foreign Military Sales
FRD – Formerly Restricted Data
FOIA – Freedom of Information Act
FOUO – For Official Use Only
FOUO LES – For Official Use Only Law Enforcement Sensitive
FRD – Formerly Restricted Data

-G-

GAO – General Accounting Office
GCA – Government Contracting Activity
GSA – General Services Administration

-H-

HQMC – Headquarters Marine Corps
HRO – Human Resource Office

-I-

IA – Information Assurance
IAM – Information Assurance Manager
IAO - Information Assurance Officer
IBI - Interview oriented Background Investigation
IC - Intelligence Community
IDE - Intrusion Detection Equipment
IDS - Intrusion Detection Systems
INFOSEC - Information Security
INS – Immigration and Naturalization Service

IR&D - Independent Research and Development
IRR - Inactive Ready Reserves
ISIC – Immediate Superior in Chain of Command
ISP - Information Security Program
ISSM - Information Systems Security Manager
ISCAP – Interagency Security Classification Appeals Panel
ISOO - Information Security Oversight Office
IT – Information Technology

-J-

JAG - Judge Advocate General of the Navy
JAGMAN – Judge Advocate General Manual
JAMS – Joint Adjudication Management System
JANAP - Joint Army, Navy, Air Force Publication
JCAVS – Joint Clearance and Access Verification System
JCS - Joint Chiefs of Staff
JPAS – Joint Personnel Adjudication System

-L-

LAA - Limited Access Authorization/Limited Access Area
LBI - Limited Background Investigation
LIMDIS – Limited Distribution
LOI - Letter of Intent
LOD - Letter of Decision
LRC - Local Records Check

-M-

MBI - Minimum Background Investigation
MCTFS - Marine Corps Total Force System
MOS - Military Operations Specialty
MSRB - Master Service Record Book
MTT - Mobile Training Team

-N-

NARA - National Archives and Records Administration
NAC - National Agency Check
NACI - National Agency Check plus Inquiries
NACIC - National Agency Check plus Inquiry with Credit Check
NACLC/NCL- National Agency Check with Local Agency Checks and Credit Check
NAF - Non-appropriated Fund
NAFI - Non-appropriated Fund Instrumentalities
NASA - National Aeronautics and Space Administration

NATO - North Atlantic Treaty Organization
NAVY IPO - Navy International Programs Office
NCIC - National Crime Information Center
NCIS - Naval Criminal Investigative Service (Formerly NSIC, NISCOM and NIS)
NCISFO - Naval Criminal Investigative Service Field Office
NCISRA - Naval Criminal Investigative Service Resident Agency
NCS - Noncritical-Sensitive
NdA – Nondisclosure Agreement
NETWARCOM SD – Naval Network Warfare Command Security Directorate
NGA – National Geospatial-Intelligence Agency
NISP - National Industrial Security Program
NISPOM - National Industrial Security Program Operating Manual
NJAG - Navy Judge Advocate General
NMCI – Navy and Marine Corps Intranet
NNPI - Naval Nuclear Propulsion Information
NRC - Nuclear Regulatory Commission
NSA - National Security Agency
NSC - National Security Counsel
NSDD - National Security Decision Directive
NSG - Naval Security Group
NSI – National Security Information
NSN - National Stock Number
NWP - Naval Warfare Publication

-O-

OASD(PA) - Office of the Assistant Secretary of Defense (Public Affairs)
OASDOCB - Operations Center, Columbus (Formerly Defense Investigative Service Clearance Office (DISCO))
OCA - Original Classification Authority
OCC - Operations Center Columbus (formerly Defense Investigative Service Clearance Office (DISCO))
ODCR - Officer Distribution Control Report
OGC - Office of the General Counsel
OMB - Office of Management and Budget
OMT - Office of Mission Training (Formerly Department of Defense Security Institute (DoDSI)
ONI - Office of Naval Intelligence
OPLOC - Operating Locations (formerly Cognizant Security Office)
OPF - Official Personnel Folder (civilians)
OPM - Office of Personnel Management
OPM-FISD - Office of Personnel Management - Federal Investigative Services Division
OPNAV - Staff Offices of the Chief of Naval Operations

OSD - Office of the Secretary of Defense
OSR – Office of Security Reviews (DoD)

-P-

PA - Privacy Act
PAO - Public Affairs Officer
PCC – Policy Coordinating Committee
PDS – Protected Distribution System
PIN - Personal Identification Number
PCL - Personnel Clearance Level
PEP - Personnel Exchange Program
PID – Personnel Identification Data
PSAB - Personnel Security Appeals Board
PSI - Personnel Security Investigation
PSM Net – Personnel Security Management Network
PSP - Personnel Security Program
PSQ - Personnel Security Questionnaire
PCS – Permanent Change of Station
PCU - Premise Control Unit
PI - Preliminary Inquiry
PM - Program Manager
POB – Place of Birth
POC – Point of Contact
POE - Port of Embarkation
PPP - Program Protection Plan
PR - Periodic Reinvestigation
PRP - Nuclear Weapon Personnel Reliability Program
PSA - Presidential Support Activities
PSS - Protective Security Service

-R-

RANKIN - Retrieval and Analysis of Navy Classified Information
RD - Restricted Data
RAA – Restricted Access Area
ROI - Report of Investigation
RRU – Request to Research/Recertify/Upgrade Eligibility
RSI – Reimbursable Suitability Investigation
RUC - Reporting Unit Code

-S-

S - Secret
SAC - Special Agent in Charge
SAO - Senior Agency Official
SAP - Special Access Programs

SAPOC - Special Access Program Oversight Committee
SBU - Sensitive But Unclassified
SCG - Security Classification Guide
SCI - Sensitive Compartmented Information
SCIF - Sensitive Compartmented Information Facility
SDDC - Surface Deployment Distribution Command
SECDEF - Secretary of Defense
SECNAV - Secretary of the Navy
SF - Standard Form
SI - Sensitive Information
SIOP - Single Integrated Operational Plan
SIOP-ESI - Single Integrated Operational Plan-Extremely
SJA - Staff Judge Advocate
SMO - Security Management Office
SOIC - Senior Official of the Intelligence Community
SOP - Standard Operating Procedures
SOR - Statement of Reason
SPB - Security Policy Board
SPECAT - Special Category Communications caveat
SPR - Secret Periodic Reinvestigation
SS - Special-Sensitive
SSBI- Single Scope Background Investigation
SSN - Social Security Number
SSO - Special Security Officer
SSSO - Subordinate Special Security Officer
STAAT - Security Training, Assistance, Assessment Team

-T-

TIS - Transfer in Status
TNAC - Trustworthiness National Agency Check
TS - Top Secret
TSCA - Top Secret Control Assistant
TSCO - Top Secret Control Officer

-U-

UAA – Uncontrolled Access Area
UCMJ - Uniform Code of Military Justice
UCNI - Unclassified Controlled Nuclear Information
UIC - Unit Identification Code
USMTF - U.S. Message Text Format
U.S.C. - United States Code
USD(I) – Under Secretary of Defense for Intelligence
USD(CI&S) – Under Secretary of Defense (Counterintelligence & Security)
USD(P) – Under Secretary of Defense for Policy

USIS - U.S. Investigative Service
USO - United Service Organization
USSAN - United States Security Authority, NATO

-W-

WHS – Washington Headquarters Service

APPENDIX B

FORMS

The forms listed below are used in conjunction with the ISP. These forms are procured through the Navy Supply System.

Form Number/Name Stock Number

DD 254 (12-99) 0102-LF-011-5800
Contract Security Classification Specification

DD 2501 (3-88) 0102-LF-000-6900
Courier Authorization Card

OPNAV 5511/10 (12-89) 0107-LF-008-8000
Record of Receipt

OPNAV 5511/51 (5-80) 0107-LF-055-5355
Security Discrepancy Notice

These forms are available only through GSA.

SF 700 (4-01) 7540-01-214-5372
Security Container Information

SF 701 (8-85) 7540-01-213-7899
Activity Security Checklist

SF 702 (8-85) 7540-01-213-7900
Security container Check Sheet

SF 703 (8-85) 7540-01-213-7901
Top Secret Cover Sheet

SF 704 (8-85) 7540-01-213-7902
Secret Cover Sheet

SF 705 (8-85) 7540-01-213-7903
Confidential Cover Sheet

SF 706 (1-87) 7540-01-207-5536
Top Secret Label

SF 707 (1-87) 7540-01-207-5537
Secret Label

SF 708 (1-87) 7540-01-207-5538
Confidential Label
SF 709 (1-87) 7540-01-207-5540
Classified Label

SF 710 (1-87) 7540-01-207-5539
Unclassified Label

SF 711 (1-87) 7540-01-207-5541
Data Descriptor Label

SF 712 (10-87) 7540-01-267-1158
Classified SCI

OF 89 (9-98) Local reproduction
Maintenance Record for authorized
Security Containers/Vaults

Note: The OF 89 may be found on the GSA website at **www.gsa.gov/forms**

APPENDIX C

REFERENCES

Executive Order 13526, *Classified National Security Information, Memorandum of December 29, 2009*

32 CFR Parts 2001 and 2004, *Classified National Security Information (ISOO Directive No. 1), 22 Sep 03*

DoD Manual 5200.01, Vol 1 *DoD Information Security Program, 24 Feb 12 (Overview, Classification, and Declassification*

DoD Manual 5200.01, Vol 2 *DoD Information Security Program, 24 Feb 12 (Marking of Classified Information)*

DoD Manual 5200.01, Vol 3 *DoD Information Security Program, 24 Feb 12 (Protection of Classified Information)*

DoD Manual 5200.01, Vol 4 *DoD Information Security Program, 24 Feb 12 (Controlled Unclassified Information/CUI)*

Executive Order 12829, *National Industrial Security Program, 6 Jan 93*

DCID 1/7, *Security Controls on the Dissemination of Intelligence Information, 30 Jun 98*

DOE Final Rule on Nuclear Classification and Declassification, 10 CFR Part 1045, 22 Dec 97

SECNAVINST 5510.30B, *DON Personnel Security Program Regulation*

DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual, 3 Aug 98*

DoD Directive 5205.7, *Special Access Program (SAP) Policy*, 5 Jan 06

DoD Instruction 0-5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs), 1 Jul 97*

SECNAVINST S5460.3C, *Management, Administrative Support and Oversight of Special Access Programs Within the Department of the Navy (U), 5 Aug 99*

DoD Directive 8500.1, *Information Assurance (IA), 24 Oct 02*

DoD Instruction 8500.2, *Information Assurance (IA) Implementation, 6 Feb 03*

SECNAV M-5239.1, *Department of the Navy Information Assurance (IA) Program, Nov 05*

EKMS 1A, CMS Policy and Procedures for Navy Electronic Key Management Systems (U), 5 Oct 04

OPNAVINST S5511.35K, *Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U), 1 Jul 98*

NAVSEAINST 5511.32C, *Safeguarding of Naval Nuclear Propulsion Information (NNPI), 26 Jul 05*

Title 42, U.S.C., Sections 2011-2284, *Atomic Energy Act of 30 Aug 54, as amended*

DoD Directive 5210.2, *Access to and Dissemination of Restricted Data, 12 Jan 78*

SECNAVINST 5212.1D, *Navy and Marine Corps Records Disposition Manual, 22 April 1998*

USSAN 1-07, *United States Implementation of NATO Security Procedures, 5 April 2007*

Title 5, U.S.C., Section 552, *Freedom of Information Act of 4 Jul 66, as amended*

OPNAVINST 5570.2, *DoD Unclassified Controlled Nuclear Information (DoD UCNI), 11 Feb 93*

DoD Directive 5230.24, *Distribution Statements on Technical Documents, 18 Mar 87*

DoD Directive 5030.59, *National Imagery and Mapping Agency (NIMA) Limited Distribution Imagery or Geospatial Information and Data, 13 May 03*

MCO P5530.14A, *Marine Corps Physical Security Program Manual, 05 June 2009*

DON Policy updates may be found on the CNO (N09N2) website at www.navysecurity.navy.mil

Local policy updates and changes for Information and Personnel Security can be found on the Command Security Manager's web site. http://www.quantico.usmc.mil/activities/?Section=CSM