DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20350

SECNAVINST 5510.30A
09N
10 March 1999

SECNAV INSTRUCTION 5510.30A

From: Secretary of the Navy
To: All Ships and Stations

Subj: DEPARTMENT OF THE NAVY PERSONNEL SECURITY PROGRAM

Ref: (a) Executive Order 12968, Access to Classified Information, 2 Aug 95
(b) DoD 5200.2-R of Jan 87, Department of Defense Personnel Security Program Regulation (NOTAL)
(c) Navy Department Supplement to DoD S5105.21.M-1 of 18 Mar 97 (NOTAL)
(d) SECNAVINST 5510.36, Department of the Navy Information Security Program (ISP) Regulation

Encl: (1) Department of the Navy Personnel Security Program (PSP) Regulation

1. **Purpose**. To provide all Department of the Navy (DON) commands, activities and personnel with regulations and guidance governing the Department of the Navy Personnel Security Program (PSP). This regulation is a complete revision of chapters 20-24 of OPNAVINST 5510.1H and should be read in its entirety.

2. **Cancellation**. SECNAVINST 5510.30, Chapters 20-24 of OPNAVINST 5510.1H and Report Symbols DD-C3I(A)1749, OPNAV 5510-6K and OPNAV 5510-6P.

3. **Objective**. To ensure maximum uniformity and effectiveness in the application of PSP policies within the DON.

4. **Scope**. This regulation is the basic DON regulation governing the PSP. The provisions of this regulation apply to all military and civilian personnel.

5. **Summary of Changes**. Substantive changes have been made to this regulation to implement new national and Department of Defense (DoD) PSP policies. Changes include:

a. Integration of Automated Information Systems positions with national security position sensitivity designations, chapter 5.

b. Revision of the Personnel Security Investigations standards and command request procedures, chapter 6.

c. Revision of the Personnel Security Determinations process, including the unfavorable determination appeal process, chapter 7.

d. Revision of procedures for granting and accepting security clearance determinations, chapter 8.

e. Revision to procedures for certifying and validating clearance determinations, chapter 8.

f. Revision of procedures for granting and recording access, chapter 9.

g. Inclusion of summary guidance regarding Sensitive Compartmented Information access, chapter 9.

h. Revision of procedures for administration of Non-disclosure Agreements, chapter 9.

i. Inclusion of guidance regarding access to Restricted Data and Critical Nuclear Weapon Design Information, chapter 9.

j. Expansion of guidance regarding Continuous Evaluation, chapter 10.

k. Revision of guidance regarding visitor access to classified information, chapter 11.

l. Revision of definitions and terms used in the PSP, appendix A.

m. Expansion of guidance regarding the Defense Clearance and Investigations Index, appendix E.

n. Inclusion of national adjudication guidelines, appendix G.

6. **Action**. Commanding officers will ensure compliance with the provisions of this instruction.

7. **Reports and Forms**. The reporting requirements levied by this regulation are assigned the report symbols identified in exhibit 6B. Information regarding procurement of the forms mentioned in this regulation is contained in exhibit 6C.

Richard Danzig

Distribution:
SNDL Parts 1 and 2
MARCORPS PCN 710000000000 and 71000000100

TABLE OF CONTENTS

Paragraph Page

Chapter 1: Basic Program Policy and Authorities

1-1 Basic Policy 1-1
1-2 Authority 1-1
1-3 National Authorities for Security Matters 1-1
1-4 Department of Defense Security Program Authorities 1-3
1-5 Department of the Navy Security Program Management 1-4
1-6 Special Programs 1-6
1-7 Special Access Programs 1-6
1-8 Applicability 1-7
1-9 Combat Operations 1-7
1-10 Waivers 1-7
1-11 Commanding Officer 1-8
1-12 Guidance 1-8

Chapter 2: Command Security Program Management

2-1 Basic Policy 2-1
2-2 Commanding Officer 2-1
2-3 Security Manager 2-2
2-4 Duties of the Security Manager 2-2
2-5 Top Secret Control Officer 2-4
2-6 Other Security Assistants 2-4
2-7 Contracting Officer's Representative 2-5
2-8 Information Systems Security Manager 2-5
2-9 Special Security Officer 2-5
2-10 Inspections, Assist Visits, and Review 2-6
2-11 Security Servicing Agreements 2-6
2-12 Standard Program Requirements 2-7
2-13 Planning For Emergencies 2-7

Chapter 3: Counterintelligence Matters

3-1 Basic Policy 3-1
3-2 Sabotage, Espionage, International Terrorism or Deliberate Compromise 3-1
3-3 Contact Reporting 3-2
3-4 Suicide or Attempted Suicide 3-2
3-5 Unauthorized Absentees 3-2
3-6 Death or Desertion 3-3
3-7 Foreign Travel 3-3
3-8 Foreign Connections 3-3

Chapter 4: Security Education

4-1 Basic Policy 4-1
4-2 Responsibility 4-1
4-3 Scope 4-1
4-4 Minimum Requirements 4-3
4-5 Indoctrination 4-4
4-6 Orientation 4-5
4-7 On-The-Job Training 4-5

4-8 Refresher Briefings 4-6
4-9 Counterintelligence Briefings 4-6
4-10 Special Briefings 4-6
4-11 Command Debriefing 4-7
4-12 Security Termination Statements 4-8
4-13 Training For Security Personnel 4-9
4-14 Security Awareness 4-10
Exhibit 4A - Security Termination Statement 4A-1

Chapter 5: National Security Positions

5-1 Basic Policy 5-1
5-2 Designation of Sensitive Positions 5-1
5-3 Criteria for Designating Sensitive Positions 5-2
5-4 Suitability Determination Authority 5-4
5-5 Suitability Determinations 5-4
5-6 Determining Eligibility to Occupy a Sensitive Position 5-5
5-7 Non-US Citizens in Sensitive Positions 5-6
Exhibit 5A - Sample Designation of Position Sensitivity 5A-1

Chapter 6: Personnel Security Investigations

6-1 Basic Policy 6-1
6-2 Types of Personnel Security Investigations 6-2
6-3 Restrictions During Subject Interviews 6-6
6-4 Investigative Requirements for Personnel Security Clearance 6-5
6-5 Investigative Requirements for Military Appointment or Enlistment . 6-7
6-6 Investigative Requirements for Civilian Employment in Sensitive Positions 6-8
6-7 Investigative Requirements for DON Contractor Personnel 6-10
6-8 Other Investigative Requirements for Specific Performance of Duty . 6-10
6-9 Programs with Special Investigative Requirement 6-13
6-10 Reciprocity 6-15
6-11 Limitations on Requesting Personnel Security Investigations 6-16
6-12 Command Responsibilities Regarding Personnel Security Investigation Requests 6-17
6-13 Electronic Personnel Security Questionnaire 6-19
6-14 Preparation and Submission of Investigative Requests 6-19
6-15 Maintaining Questionnaire Information 6-21
6-16 Follow-up Actions on Investigative Requests 6-22
6-17 Processing Completed Reports of Investigation 6-23
6-18 Safeguarding Reports of Investigation 6-24
Exhibit 6A - Personnel Security Investigations 6A-1
Exhibit 6B - Report Symbols 6B-1
Exhibit 6C - Procurement of Forms 6C-1

Chapter 7: Personnel Security Determinations

7-1 Basic Policy 7-1
7-2 Personnel Security Program Authorities and Responsibilities 7-2
7-3 Adjudicative Officials 7-6
7-4 Personnel Security Determinations 7-7
7-5 Trustworthiness Determinations 7-8
7-6 Facility Access Determination (FAD) Program 7-9
7-7 Unfavorable Determinations Process 7-10

7-8 Appealing Unfavorable Determinations 7-12
7-9 Unfavorable Personnel Security Actions 7-15

Chapter 8: Clearance

8-1 Basic Policy 8-1
8-2 Reciprocal Acceptance of Security Clearances 8-1
8-3 Clearance Prohibitions 8-3
8-4 Recording Determinations 8-4
8-5 Interim Security Clearance 8-5
8-6 Granting a Security Clearance 8-7
8-7 Unique Security Clearance Requirements 8-7
8-8 Clearance Under the National Industrial Security Program (NISP) . . 8-9
8-9 Clearance Withdrawal or Adjustment 8-10
8-10 Denial or Revocation of Security Clearance 8-11
8-11 Reestablishing Security Clearance Eligibility After a Denial or Revocation 8-11
Exhibit 8A - Personnel Security Data Codes 8A-1

Chapter 9: Access to Classified Information

9-1 Basic Policy 9-1
9-2 Granting Access to Classified Information 9-1
9-3 Sensitive Compartmented Information (SCI) Access 9-2
9-4 Classified Information Nondisclosure Agreement (SF 312) 9-4
9-5 Recording Access 9-6
9-6 One-Time Access 9-7
9-7 Temporary Access 9-9
9-8 Temporary Access Pending Receipt of Clearance Certification 9-9
9-9 Access by Retired Personnel 9-10
9-10 Access by Reserve Personnel 9-11
9-11 Access by Investigative and Law Enforcement Agent 9-11
9-12 Access Authorizations for Attorneys 9-11
9-13 Contractor Access 9-12
9-14 Access Authorization (AA) for Persons Outside of the Executive Branch of the Government 9-12
9-15 Historical Researchers 9-13
9-16 Limited Access Authorization (LAA) for Non-U.S. Citizens 9-14
9-17 Terminating, Withdrawing or Adjusting Access 9-17
9-18 Suspension of Access for Cause 9-17
9-19 Access to and Dissemination of Restricted Data (RD) Including Critical Nuclear Weapon Design Information (CNWDI) . . . 9-19
Exhibit 9A - Classified Information Nondisclosure Agreement Form (SF 312) 9A-1

Chapter 10: Continuous Evaluation

10-1 Basic Policy 10-1
10-2 Security Education 10-2
10-3 Employees Education and Assistance Program 10-2
10-4 Performance Evaluation System 10-2
10-5 Command Reports of Locally Developed Unfavorable Information . . . 10-3
Exhibit 10A - Continuous Evaluation Check Sheet 10A-1

Chapter 11: Visitor Access to Classified Information

11-1 Basic Policy 11-1
11-2 Classified Visit Request Procedures 11-2
11-3 Visits by Foreign Nationals and Representatives of Foreign Entities. 11-5
11-4 Classified Visits by Members of Congress 11-5
11-5 Classified Visits by Representatives of the General Accounting Office 11-5

Appendices

A Definitions A-1
B Acronyms B-1
C Guidelines for Command Security Inspection C-1
D Security Inspection Checklist D-1
E Defense Clearance and Investigations Index (DCII) E-1
F Personnel Security Standards F-1
G Adjudication Guidelines G-1
H Structure and Functions of the Personnel Security Appeals Board (PSAB) H-1
I Citizenship I-1

CHAPTER 1

BASIC PROGRAM POLICY AND AUTHORITIES

1-1 BASIC POLICY

1. This regulation establishes the Department of the Navy (DON) Personnel Security Program (PSP) under the authority of Executive Order (E.O.) 12968, Access to Classified Information, reference (a) and E.O. 10450, Security Requirements for Government Employees, and in compliance with Department of Defense (DoD) 5200.2-R, DoD Personnel Security Program Regulation, January 1987 (NOTAL) reference (b).

2. The objective of the PSP is to authorize initial and continued access to classified information and/or initial and continued assignment to sensitive duties to those persons whose loyalty, reliability and trustworthiness are such that entrusting the persons with classified information or assigning the persons to sensitive duties is clearly consistent with the interests of national security. Additionally, the PSP ensures that no final unfavorable personnel security determination will be made without compliance with all procedural requirements.

1-2 AUTHORITY

1. The Secretary of the Navy (SECNAV) is responsible for establishing and maintaining a Personnel Security Program in compliance with the provisions of E.O.s, public laws, National Security Council guidance, DoD regulation and other security directives regarding trustworthiness standards and the protection of classified information.

2. The SECNAV has designated the Chief of Naval Operations, Special Assistant for Naval Investigative Matters and Security, (CNO (N09N)), who functions primarily as the Director, Naval Criminal Investigative Service (NCIS), as the senior security official of the DON. CNO (N09N) is responsible for ensuring that the DON has an effective PSP and for complying with all directives issued by higher authority.

1-3 NATIONAL AUTHORITIES FOR SECURITY MATTERS

1. The President of the United States (U.S.), bears executive responsibility for the security of the Nation which includes the authority to classify information and limit access thereto for the protection of the national defense and foreign relations of the United States. Standards for the classification and

safeguarding of national security information are detailed in E.O. 12958 and standards for personnel receiving access thereto are detailed in E.O. 12968.

2. **The National Security Council (NSC)** provides overall policy guidance on information and personnel security matters.

3. **The Director of the Information Security Oversight Office (ISOO)**, has the responsibility for issuing directives as necessary to implement E.O. 12958 and provides guidance regarding the Classified Information Nondisclosure Agreement, Standard Form (SF) 312.

4. **The Security Policy Board (SPB)** is an interagency organization co-chaired by the Deputy Secretary of Defense and the Director of Central Intelligence created by the President to consider, coordinate, and recommend to the President, through the NSC, uniform standards, policies and procedures governing classified information and personnel security, to be implemented and applicable throughout the Federal Government.

5. **The Attorney General of the United States** upon request from the head of an agency or the Director, ISOO, interprets E.O. provisions in response to questions arising from implementation.

6. **The Office of Personnel Management (OPM)** is responsible for oversight and implementation of E.O. 10450, which prescribes security requirements (including investigations) for federal government employment.

7. **The Director of Central Intelligence (DCI)**, as the chairman of the National Foreign Intelligence Board (NFIB), issues instructions in the form of DCI directives or policy statements affecting intelligence policies and activities. The DCI is charged by 50 U.S.C. Section 403(g), National Security Act of 1947, with protecting intelligence sources and methods.

8. **The Federal Bureau of Investigation (FBI)** is the primary internal security agency of the Government with jurisdiction over investigative matters which include espionage, sabotage, treason and other subversive activities.

9. **The Secretary of the Navy (SECNAV)** is the Department of the Navy agency head responsible under E.O. 12968 for establishing and maintaining an effective program to ensure that access to classified information by each DON employee is clearly consistent with the interests of national security.

1-4 DEPARTMENT OF DEFENSE SECURITY PROGRAM AUTHORITIES

1. **The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I))** is the senior DoD official charged by the Secretary of Defense with responsibility for development of policies and procedures governing information and personnel security policy programs. The Deputy Assistant Secretary of Defense, Security and Information Operations (DASD(S&IO)) issues DoD 5200.1-R, Information Security Program Regulation (NOTAL), and DoD 5200.2-R, Personnel Security Program Regulation, reference (b) (NOTAL).

2. **The Deputy Under Secretary of Defense for Policy Support DUSD(PS)** administers international security policy and performs administrative support to the Secretary of Defense who is designated the United States Security Authority for NATO (USSAN). The USSAN implements security directives issued by the North Atlantic Treaty Organization (NATO) and oversees the Central U.S. Registry (CUSR), with the Department of the Army as executive agency.

3. **The National Security Agency (NSA)** provides centralized coordination and direction for signals intelligence and communications security for the Federal Government. The DON contributes to these efforts primarily through the Commander, Naval Security Group Command (COMNAVSECGRU). The Director, NSA is authorized by the Secretary of Defense to prescribe procedures or requirements, in addition to those in DoD regulations, for Sensitive Compartmented Information (SCI) and communications security (COMSEC). The authority to lower any COMSEC security standard within the DoD rests with the Secretary of Defense.

4. **The Defense Intelligence Agency (DIA)** coordinates the intelligence efforts of the Army, Navy and Air Force and is responsible for implementation of standards and operational management of SCI for the DoD. The Director, DIA is the Senior Official of the Intelligence Community (SOIC) for DoD and is a member of the NFIB.

5. **The Defense Security Service (DSS)** conducts personnel security investigations for the DoD (with the exception of those investigations conducted by OPM and investigations conducted overseas). DSS additionally administers the National Industrial Security Program (NISP) as the executive agency and provides security training for employees of defense contractors and for DoD military and civilian personnel. DSS components include:

a. **The National Computer Center (NCC)**, created to support the DSS Strategic Implementation Plan, is involved with automation projects such as the Electronic Personnel Security Questionnaire (EPSQ) and Defense Clearance and Investigations Index (DCII) enhancements.

b. **The DSS Operations Center - Baltimore**, is the operations center controlling personnel security investigations conducted by DSS.

c. **The Deputy Director, Industrial Security** manages the DoD implementation of the NISP through regional Cognizant Security Offices throughout the operating centers in the Continental United States (CONUS) and the Offices of Industrial Security International in locations overseas.

d. **The DSS Operations Center - Columbus**, grants personnel security clearances to individuals in private industry (contractors) who need access to classified information in order to perform their jobs and responds to requests for information regarding contractor personnel security clearance applications.

e. **The Security Research Center** performs research and analysis to improve security programs.

f. **The Office of Mission Training (OMT)** provides job training to DSS investigative agents and other security training previously provided by the Department of Defense Security Institute (DoDSI) to DoD contractors and DoD employees.

1-5 DEPARTMENT OF THE NAVY SECURITY PROGRAM MANAGEMENT

1. **The Secretary of the Navy (SECNAV)**. SECNAV is responsible for implementing a PSP in compliance with the provisions of E.O.'s, public laws, and directives issued by the NRC, DOE, DoD, DCI, and other agencies.

2. **The Special Assistant for Naval Investigative Matters and Security, Office of the Chief of Naval Operations (CNO (N09N))/Director, Naval Criminal Investigative Service (DIRNCIS)**. The SECNAV has designated CNO (N09N)/DIRNCIS as the **DON senior agency security official** under reference (a). The Assistant for Information and Personnel Security (CNO (N09N2))/Deputy Assistant Director, Information and Personnel Security Programs (NCIS-21) provides staff support for these functions and responsibilities.

a. CNO (N09N) is responsible to the SECNAV for establishing, directing, and overseeing an effective DON PSP and for

implementing and complying with all directives issued by higher authority. This responsibility includes:

(1) Formulating policies and procedures, issuing directives, monitoring, inspecting, and reporting on the status of administration of the PSP in the Navy and Marine Corps.

(2) Establishing and maintaining continuing security awareness, training, and education programs to ensure effective implementation of reference (a).

(3) Cooperating with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines.

(4) Establishing procedures to prevent unnecessary access to classified information, including procedures to establish need to know before access is authorized and to limit the number of persons granted access to classified information to the minimum consistent with operational needs and security requirements.

b. CNO (N09N) is also responsible for establishing, administering, and overseeing the DON Information Security Program (ISP) and issuing information security policy and procedures through reference (d).

3. **The Director, Department of the Navy Central Adjudication Facility (DON CAF)** reports directly to DIRNCIS and is the personnel security adjudicative determination authority for all DON personnel.

4. **The Director of Naval Intelligence (CNO (N2))**, as the Senior Official of the Intelligence Community (SOIC) for the DON, is responsible for administering the Navy's SCI program. **The Office of Naval Intelligence (ONI)**, is responsible for the security management and implementation of SCI programs. **The Director, Security Directorate (ONI-5)**, as Special Security Officer/Special Activities Officer for the DON (SSO Navy), is responsible for guidance and instruction on matters concerning the security, control and use of SCI.

5. **The Commander, Naval Security Group Command (COMNAVSECGRU)**, is responsible for the security and administration of SCI programs within the Department's cryptologic community.

6. **The Deputy Chief of Naval Operations (CNO (N89)), Special Programs Division**, is responsible for security policy and procedures for SAPs established under Special Access Program Oversight Committee (SAPOC) authority.

7. **The Director, Navy International Programs Office (Navy IPO),** is assigned the authority to approve or disapprove routine requests for access to or transfer of DON technical data or disclosure of DON classified or sensitive unclassified information to other nations in accordance with national disclosure policy.

1-6 SPECIAL PROGRAMS

1. The security requirements for access to information classified as Confidential, Secret or Top Secret normally provide sufficient protection. Any program requiring additional security protection, handling measures, reporting procedures or formal access lists is considered a special program.

2. Most special programs requiring additional security measures have been established by authorities outside the DON. Although the requirements for these programs are included in this regulation, these programs are implemented and governed in the DON by the following instructions: OPNAVINST C5510.101D, NATO Security Procedures (U) (NOTAL); OPNAVINST S5511.35K, Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U) (NOTAL); SECNAVINST 5510.35, Nuclear Weapon Personnel Reliability Program (PRP); SECNAVINST 5312.12B, Selection of Department of the Navy Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities; OPNAVINST C8126.1A, Navy Nuclear Weapon Security (U) (NOTAL); DoD Directive 5210.2 of 12 January 1978, Access to and Dissemination of Restricted Data (NOTAL), and the Navy Department Supplement to DoD S-5105.21-M-1 of 8 Mar 95 (NOTAL) for the protection of SCI.

1-7 SPECIAL ACCESS PROGRAMS (SAP)

Programs requiring security measures in addition to those requirements for the protection of Top Secret, Secret or Confidential classified information which are established by and within the Department of Defense are referred to as DoD SAPs. A DoD SAP must be authorized by the Secretary of Defense or by the Deputy Secretary of Defense and is governed by DoD Directive 0-5205.7, Special Access Program (SAP) Policy of 13 Jan 1997 (NOTAL), DoD Instruction 0-5205.11, Management, Administration, and Oversight of DoD Special Access Programs (SAPs) of 1 Jul 97 (NOTAL); DoD 5220.22-M, National Industrial Security Program Operating Manual of January 1995 (NOTAL); and SECNAVINST S5460.3B, Control of Special Access Programs within the Department of the Navy (U) (NOTAL). The Deputy Chief of Naval Operations (CNO (N89)) receives and reviews requests for SAPs from DON requesters and the Under Secretary of the Navy must

formally approve the establishment of each SAP in coordination with the Deputy Secretary of Defense.

1-8 APPLICABILITY

1. This regulation applies to all regular and reserve military members of the Navy and Marine Corps; civilian personnel employed by, hired on a contractual basis by, or serving in an advisory/consultant capacity to the DON whether on a permanent, temporary or part-time basis, and whether or not compensated from appropriated or non-appropriated funds; and applicants selected for sensitive positions, or persons accepted for consideration for enlistment or appointment (military), or other persons covered by contract or other legal agreement.

2. This regulation establishes coordinated policies for personnel security matters. It incorporates policies provided in references (a) through (c) and other directives bearing on personnel security. This is the controlling regulation for implementation and maintenance of the DON PSP. Personnel security provisions incorporated in other departmental directives must comply with these policies and procedures.

3. This regulation provides minimum requirements. Commanding officers may choose to impose more stringent requirements on their command or on their subordinate commands; however, they may not establish requirements that impact on commands that are not their subordinate commands. Commanding officers may not establish requirements that are contradictory to this regulation.

4. Commanding officers are responsible for compliance with and implementation of this regulation within their commands. Personnel are individually responsible for compliance with this regulation.

1-9 COMBAT OPERATIONS

Security requirements may be modified as necessary to meet local conditions in combat or combat-related operations. In these circumstances, follow the provisions of this regulation as closely as possible. Exercises are not combat-related operations. This exception does not apply to regularly scheduled training exercises or operations.

1-10 WAIVERS

1. When a commanding officer finds that fulfilling the requirements of this regulation will result in an untenable

sacrifice of operating efficiency, or when there are other good and sufficient reasons, a waiver of a specific requirement may be requested from the Chief of Naval Operations (N09N2) via the administrative chain of command.

2. Each request for waiver must give the reason why the requirement cannot be met and describe the alternative procedures or protection to be provided.

1-11 COMMANDING OFFICER

"Commanding officer" is used throughout this regulation as a generic term for the head of an organizational entity and includes commander, commanding general, director, officer in charge, etc. Responsibilities assigned to the commanding officer by this regulation may be delegated unless specifically prohibited. "Command" is used as a generic term for the organizational entity and includes ship, laboratory, facility, activity, unit, squadron, etc.

1-12 GUIDANCE

1. Requests for guidance or clarification of this regulation may be addressed formally or informally to the Chief of Naval Operations (N09N2), 716 Sicard Street, SE, Washington, DC 20388-5381. For telephone inquiries, the Security Action Line (with a recorder for after-hours calls) may be reached at DSN 288-8856, commercial (202) 433-8856. Send facsimile requests to (202) 433-8849. The CNO homepage at www.navysecurity.navy.mil provides policy updates, security awareness items and other instructional materials.

2. Definitions of terms used in this regulation are listed in appendix A.

3. Acronyms used throughout this regulation are listed in appendix B.

CHAPTER 2

COMMAND SECURITY MANAGEMENT

2-1 BASIC POLICY

Commanding officers are responsible for compliance with and implementation of the DON Information and Personnel Security Program within their command. The effectiveness of the command's security program depends on the importance the commanding officer gives it.

2-2 COMMANDING OFFICER

1. An effective security program relies on a team of professionals working together to fulfill the commanding officer's responsibilities.

2. Command security management responsibilities include:

a. Designate a security manager.

b. Designate a Top Secret control officer (TSCO) if the command handles Top Secret information.

c. Designate an information systems security manager (ISSM) if the command processes data in an automated system.

d. Designate a security officer to manage facilities security.

e. Designate a Special Security Officer (SSO) to administer the command SCI security program.

f. Issue a written command security instruction. See appendix C and exhibit 2A of reference (d).

g. Establish an industrial security program when the command engages in classified procurement or when cleared contractors operate within areas under the commanding officer's control.

h. Ensure that the security manager and other command security professionals are appropriately trained, that all personnel receive required security education and that the command has a robust security awareness program.

i. Prepare an emergency plan for the protection of classified material.

j. Ensure that command security inspections, program reviews, and assist visits to subordinate commands are conducted, as determined necessary.

k. Ensure that the performance rating systems of all DON military and civilian personnel, whose duties significantly involve the creation, handling, or management of national security information (NSI), include a security element on which to be evaluated.

2-3 SECURITY MANAGER

1. Every command in the Navy and Marine Corps eligible to receive classified information is required to designate a security manager **in writing**.

2. The security manager will be afforded direct access to the commanding officer to ensure effective management of the command's security program.

3. The command security manager may be assigned full-time, part-time or as a collateral duty and must be an officer or a civilian employee, GS-11 or above, with sufficient authority and staff to manage the program for the command. The security manager must be a U.S. citizen and have been the subject of a favorably adjudicated SSBI completed within the previous 5 years.

4. The command security manager must be designated by name and identified to all members of the command on organization charts, telephone listings, rosters, etc. OPNAVINST 3120.32C, Standard Organization and Regulations of the U.S. Navy (NOTAL), recommends the security manager report to the commanding officer for functional security matters and to the executive officer for administrative matters.

5. Commanding officers are strongly encouraged to obtain formal training for their security managers. The Navy Security Managers Course offered by the Naval Criminal Investigative Service (NCIS) Mobile Training Team (MTT), is highly recommended.

2-4 DUTIES OF THE SECURITY MANAGER

1. The security manager is the principal advisor on information and personnel security in the command except issues specific to SCI and other special access program information and is responsible to the commanding officer for the management of the program. The duties described here and in chapter 2 of reference (d) may be assigned to a number of personnel and may even be

assigned to individuals senior to the security manager. However, the security manager remains ultimately responsible for all program requirements. The security manager must be cognizant of the command security functions and ensure the security program is coordinated and inclusive of all requirements. The security manager must ensure that those in the command who have security duties are kept abreast of changes in policies and procedures, and must provide assistance in solving security problems. The job may involve direct supervision, oversight, coordination, or a combination thereof. The security manager is the key in developing and administering the command's Information and Personnel Security Program.

2. The below listed duties and those provided in chapter 2 of reference (d), apply to every security manager:

a. Serves as the commanding officer's advisor and direct representative in matters pertaining to the security of classified information held at the command.

b. Serves as the commanding officer's advisor and direct representative in matters regarding the eligibility of personnel to access classified information and to be assigned to sensitive duties.

c. Develops written command information and personnel security procedures, including an emergency plan which integrates emergency destruction bills where required.

d. Formulates and coordinates the command's security awareness and education program.

e. Ensures security control of visits to and from the command when the visitor requires, and is authorized, access to classified information.

f. Ensures that all personnel who will handle classified information or will be assigned to sensitive duties are appropriately cleared through coordination with the DON CAF and that requests for personnel security investigations are properly prepared, submitted and monitored.

g. Ensures that access to classified information is limited to those who are eligible and have the need to know.

h. Ensures that personnel security investigations, clearances and accesses are properly recorded.

i. Coordinates the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

j. Maintains liaison with the command SSO concerning information and personnel security policies and procedures.

k. Coordinates with the command information systems security manager on matters of common concern.

l. Ensures that all personnel who have had access to classified information who are separating or retiring have completed a Security Termination Statement. The original statement is filed in the individual's field service record or official personnel file and a copy in the command files.

m. Ensures all personnel execute a Classified Information Nondisclosure Agreement (SF 312) prior to granting initial access to classified information.

2-5 TOP SECRET CONTROL OFFICER (TSCO)

Commands that handle Top Secret material will designate a TSCO **in writing**. The TSCO must be an officer, senior non-commissioned officer E-7 or above, or a civilian employee, GS-7 or above. The TSCO must be a U.S. citizen and have been the subject of a SSBI completed within the previous 5 years. Duties of a TSCO are listed in chapter 2 of reference (d).

2-6 OTHER SECURITY ASSISTANTS

1. **Assistant Security Manager**. Persons designated as assistant security managers must be U.S. citizens, and either officers, enlisted persons E-6 or above, or civilians GS-6 or above. The designation must be **in writing**. Assistant security managers must have an SSBI if they are designated to issue interim security clearances; otherwise, the investigative and clearance requirements will be determined by the level of access to classified information required.

2. **Security Assistant**. Civilian and military member employees performing administrative functions under the direction of the security manager may be assigned without regard to rate or grade as long as they have the clearance needed for the access required to perform their assigned duties and taskings.

3. **Top Secret Control Assistant (TSCA)**. Individuals may be assigned to assist the TSCO as needed. The designation will be

in writing. A person designated as a TSCA must be a U.S. citizen and either an officer, enlisted person E-5 or above, or civilian employee GS-5 or above. An established Top Secret security clearance eligibility is required. Top Secret couriers are not considered to be Top Secret control assistants. Duties of a TSCA are listed in chapter 2 of reference (d).

2-7 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

Commands that award classified contracts to industry will appoint, **in writing**, one or more qualified security specialists as the Contracting Officer's Representative (COR). The COR is responsible to the security manager for coordinating with program managers and technical and procurement officials. The COR will ensure that the industrial security functions are accomplished when classified information is provided to industry for performance on a classified contract.

2-8 INFORMATION SYSTEMS SECURITY MANAGER (ISSM)

1. Each command involved in processing data in an automated system, including access to local area networks and/or INTRANET/INTERNET, must designate a civilian or military member as an ISSM.

2. The ISSM is responsible to the commanding officer who develops, maintains, and directs the implementation of the INFOSEC program within the activity. The ISSM advises the commanding officer on all INFOSEC matters, including identifying the need for additional INFOSEC staff. The ISSM serves as the command's point of contact for all INFOSEC matters and implements the command's INFOSEC program.

2-9 SPECIAL SECURITY OFFICER (SSO)

1. Commands in the DON accredited for and authorized to receive, process and store SCI will designate an SSO. The SSO is the principal advisor on the SCI security program in the command and is responsible to the commanding officer for the management and administration of the program. SCI security program responsibilities are detailed in reference (c). The SSO will be afforded direct access to the commanding officer to ensure effective management of the command's SCI security program. The SSO will be responsible for the operation of the Sensitive Compartmented Information Facility (SCIF) and the security control and use of the SCIF. All SCI matters are referred to the SSO.

2. The SSO and the subordinate SSO will be appointed in writing and each will be a U.S. citizen and either a commissioned officer or a civilian employee GS-9 or above, and must meet Director, Central Intelligence Directive (DCID) 1/14, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)" (NOTAL) standards. The same grade limitations apply to assistant SSOs. The security manager cannot function as the SSO unless authorized by the Director, ONI or COMNAVSECGRU. The SSO will be responsible for the operation of the SCIF and the security control and use of the SCIF. All SCI matters are referred to the SSO.

3. Although the SSO administers the SCI program independent of the security manager, the security manager must account for all clearance and access determinations made on members of the command. There is great need for cooperation and coordination between the SSO and security manager, especially for personnel security matters. For individuals who are SCI eligible, the security manager and the SSO must keep one another advised of any changes in status regarding clearance and access and of information developed that may affect eligibility. The security manager and SSO must also advise each other of changes in SCI and command security program policies and procedures as they may impact on the overall command security posture.

2-10 INSPECTIONS, ASSIST VISITS, AND REVIEWS

1. Commanding officers are responsible for evaluating the security posture of their subordinate commands.

2. Senior commanders may, as determined necessary, conduct inspections, assist visits, and reviews to examine overall security posture of subordinate commands. Unless otherwise required, it is not necessary to conduct separate inspections for security. They may be conducted during other scheduled inspections and results identified as such.

3. A command personnel security program self-inspection guide is provided as appendix D.

4. Refer to exhibit 2C of reference (d) for the ISP self-inspection guide.

2-11 SECURITY SERVICING AGREEMENTS

1. Commands may perform specified security functions for other commands via security servicing agreements. 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 of one or more subordinate commands;

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

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

f. When either a cleared contractor facility or a long term visitor group is physically located on a Navy or Marine Corps installation.

2. A security servicing agreement will be specific and must clearly define where the security responsibilities of each participant begin and end. The agreement will include requirements for advising commanding officers of any matters which may directly affect the security posture of the command. Append security servicing agreements to the command security instruction.

2-12 STANDARD PROGRAM REQUIREMENTS

Each command which handles classified information is required to prepare and keep current a written command security instruction, specifying how security procedures and requirements will be accomplished in the command. Appendix C and exhibit 2A of reference (d) pertain.

2-13 PLANNING FOR EMERGENCIES

Commands will establish a plan for the protection and removal of classified NSI under its control during emergencies. Depending upon the location of the command, the plan may direct destruction of classified NSI in an emergency. The plan should be made part of the overall disaster preparedness plan of the command security program instruction. See reference (d), exhibit 2B.

CHAPTER 3

COUNTERINTELLIGENCE MATTERS

3-1 BASIC POLICY

Certain matters affecting national security must be reported to the Director, Naval Criminal Investigative Service (DIRNCIS) so appropriate counterintelligence action can be taken. All military and civilian personnel of the DON, whether they have access to classified information or not, will report to their security managers, commanding officers or to the nearest command, any activities described in this chapter involving themselves, their dependents, co-workers, or others. Commanding officers will immediately notify the nearest NCIS office.

3-2 SABOTAGE, ESPIONAGE, INTERNATIONAL TERRORISM OR DELIBERATE COMPROMISE

1. Individuals becoming aware of sabotage, international terrorism, espionage, deliberate compromise or other subversive activities will report all available information concerning such activities immediately to the security manager or commanding officer at their command or at the most readily available command. The command receiving the report must notify the servicing NCIS office. If the servicing NCIS office cannot be contacted immediately and the report concerns sabotage, international terrorism, espionage, or imminent flight or defection of an individual, the command will immediately contact the Director, NCIS (DIRNAVCRIMINVSERV WASHINGTON DC) by classified IMMEDIATE message, with CNO (N09N) as an information addressee.

2. The servicing NCIS office will be notified immediately of any requests, through other than official channels, for classified or national defense information from anyone without an official need to know, regardless of nationality. The NCIS office will also be notified of any requests for unclassified information from any individual believed to be in contact with a foreign intelligence service. Examples of requests to be reported include attempts to obtain: names, duties, personal data or characterizations of DON personnel; technical orders, manuals, regulations, base directories, personnel rosters or unit manning tables; and information about the designation, strength, mission, combat posture, and development of ships, aircraft and weapons systems.

3. The NCIS will then advise what additional action is to be taken and will effect liaison and coordination with appropriate

members of the U.S. intelligence community.

3-3 CONTACT REPORTING

1. All personnel who possess a security clearance are to report to their commanding officer, activity head, or designee, contacts with any individual, regardless of nationality, whether within or outside the scope of the individual's official activities in which illegal or unauthorized access is sought to classified or otherwise sensitive information.

2. Personnel must report to the command if they are concerned that they may be the target of exploitation. The commanding officer will review and evaluate the information and promptly report it to the local NCIS office.

3-4 SUICIDE OR ATTEMPTED SUICIDE

1. When personnel who have access to classified information commit or attempt to commit suicide, the individual's commanding officer will immediately forward all available information to the nearest NCIS office for action, with an information copy to the DON CAF. The report will, as a minimum, describe the nature and extent of the classified information to which the individual had access, and the circumstances surrounding the suicide or attempted suicide.

2. The NCIS office receiving the report will coordinate investigative action with the commanding officer. If NCIS assumes immediate investigative cognizance, command investigative efforts will be subordinate to those of NCIS. No independent questioning of witnesses should be conducted without prior approval of NCIS.

3-5 UNAUTHORIZED ABSENTEES

1. When personnel who have access to classified information are determined to be in an unauthorized absentee status, the individual's commanding officer will conduct an inquiry to determine if there are any indications from the individual's activities, behavior, or associations that the absence may be contrary to the interests of national security. If the inquiry develops such concerns, the command will report, by quickest means available, all pertinent information to the nearest NCIS office for action, with an information copy to the DON CAF.

2. NCIS will promptly advise whether or not they will conduct an investigation.

3-6 DEATH OR DESERTION

When a member of the DON who has access to classified information dies or deserts, the member's commanding officer must identify any unusual indicators or circumstances that may be contrary to the interests of national security. If such conditions exist, the command will report by the most expedient means available, all pertinent information to the nearest NCIS office.

3-7 FOREIGN TRAVEL

1. Commands will advise personnel of the particular vulnerabilities associated with foreign travel during orientation and annual refresher briefs. See paragraph 4-10, Special Briefings, for additional information regarding the foreign travel briefing.

2. All personnel possessing security clearance eligibility are required to list all personal foreign travel as part of the required Periodic Reinvestigation (PR). The Defense Security Service (DSS) will explore the foreign travel issue during the PR and may refer the investigation to NCIS if the travel patterns or failure to list travel create concerns that would make referral appropriate.

3-8 FOREIGN CONNECTIONS

1. A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom the individual is bound by affection or obligation, are not citizens of the United States. Having a financial interest in a foreign country may also present a security risk.

2. The personnel security adjudicative process requires an examination of a sufficient amount of information regarding an individual to determine whether the individual is an acceptable security risk. The assessment of risk due to the individual's relationship with foreign nationals and foreign entities is a part of the personnel security adjudicative process. Issues regarding foreign connections should be reported to the DON CAF.

CHAPTER 4

SECURITY EDUCATION

4-1 BASIC POLICY

1. Each command handling 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.

2. The purpose of the security education program is to ensure that all personnel understand the need and procedures for protecting classified information. The goal is to develop fundamental security habits as a natural element of each task.

4-2 RESPONSIBILITY

1. CNO (N09N) is responsible for policy guidance, education requirements and support for the DON security education program. Development of security education materials for use throughout the DON must be coordinated with CNO (N09N2) for consistency with current policies and procedures. This requirement does not apply to materials which are prepared for use in command programs.

2. Recruit training commands are responsible for indoctrinating military personnel entering the Navy and Marine Corps, with a basic understanding of what "classified information" is and why and how it is protected. Civilians being employed by the DON for the first time (who will handle classified material) must also be given a basic security indoctrination by the employing activity.

3. Commanding officers are responsible for security education in their commands, ensuring time is dedicated for training and awareness. Supervisors, in coordination with the command security manager, are responsible for determining security requirements for their functions and ensuring personnel under their supervision understand the security requirements for their particular assignment. On-the-job training is an essential part of command security education and supervisors must ensure that such training is provided.

4-3 SCOPE

1. Security education must be provided to all personnel. The education effort must be tailored to meet the needs of the command, as well as those of different groups within the command.

2. In formulating a command security education program, the security manager must provide for the minimum briefing requirements of this regulation. Security managers must guard against allowing the program to become stagnant or simply comply with requirements without achieving the real goals.

3. The security education program should be developed based on the command mission and function and should:

a. Advise personnel of the adverse effects to the national security which could result from unauthorized disclosure of classified information and of their personal, moral and legal responsibility to protect classified information within their knowledge, possession or control;

b. Advise personnel of their responsibility to adhere to the standards of conduct required of persons holding positions of trust and to avoid personal behavior which could render them ineligible for access to classified information or assignment to sensitive duties;

c. Advise personnel of their obligation to notify their supervisor or command security manager when they become aware of information with potentially serious security significance regarding someone with access to classified information or assigned to sensitive duties;

d. Advise supervisors of the requirement for continuous evaluation of personnel for eligibility for access to classified information or assignment to sensitive duties;

e. Familiarize personnel with the principles, criteria and procedures for the classification, downgrading, declassification, marking, control and accountability, storage, destruction, and transmission of classified information and material and alert them to the strict prohibitions against improper use and abuse of the classification system;

f. Familiarize personnel with procedures for challenging classification decisions believed to be improper;

g. Familiarize personnel with the security requirements for their particular assignments and identify restrictions;

h. Instruct personnel having knowledge, possession or control of classified information how to determine, before disseminating the information, that the prospective recipient has been authorized access, needs the information to perform his/her

official duties, and can properly protect (store) the information;

i. Advise personnel of the strict prohibition against discussing classified information over an unsecured telephone or in any other manner that may permit interception by unauthorized persons;

j. Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information;

k. Inform personnel of their particular vulnerability to compromise during foreign travel;

l. Advise personnel that they are to report to their commanding officer, activity head or designee, contacts with any individual regardless of nationality, whether within or outside the scope of the individuals official activities, in which:

(1) illegal or unauthorized access is sought to classified or otherwise sensitive information; or

(2) the employee is concerned that he or she may be the target of exploitation by a foreign entity.

m. Advise personnel of the penalties for engaging in espionage activities and for mishandling classified information or material.

4-4 MINIMUM REQUIREMENTS

1. The following are the minimum requirements for security education:

a. Indoctrination of personnel upon employment by the DON in the basic principles of security (paragraph 4-5 applies).

b. Orientation of personnel who will have access to classified information at the time of assignment, regarding command security requirements (paragraph 4-6 applies).

c. On-the-job training in specific security requirements for the duties assigned (paragraph 4-7 applies).

d. Annual refresher briefings for personnel who have access to classified information (paragraph 4-8 applies).

e. Counterintelligence briefings once every 2 years for personnel who have access to information classified Secret or above (paragraph 4-9 applies).

f. Special briefings as circumstances dictate (paragraph 4-10 applies).

g. Debriefing upon termination of access (paragraph 4-11 applies).

4-5 INDOCTRINATION

1. Personnel entering employment with DON need to have a basic understanding of what classified information is, and the reasons(s) for its protection, as well as how to protect it.

2. A basic indoctrination for military members is done during training at the time of accession. Civilians will be indoctrinated by the employing command.

3. Through indoctrination, all personnel should know that:

a. Certain information, essential to the national security, requires protection from disclosure to unauthorized persons;

b. Classified material will be marked to show the level of classification;

c. Only those who have been officially and specifically authorized may have access to classified information;

d. Personnel will be continually evaluated regarding their eligibility to access classified information and to be assigned to a sensitive position.

e. Classified material must be stored and used in secure areas, must be protected during transfer from one area to another (including electronic transfer), and must be destroyed by authorized means;

f. Any compromise or other security violation must be reported;

g. Any attempt by an unauthorized person, regardless of nationality, to solicit classified information must be reported.

4-6 ORIENTATION

1. Personnel who will have access to classified information will be given a command security orientation briefing as soon as possible after reporting aboard or being assigned to duties involving access to classified information.

2. A review of written command security manuals or material is not normally considered to provide an adequate orientation.

3. The timing and format for orientation will vary, depending on the size of the command. At large commands with a high turnover rate, briefings may be scheduled on a regular basis. At smaller commands, with irregular changes of personnel, individual instruction may be necessary.

4. Through orientation, all personnel should know:

a. The command security structure (i.e., who the security manager is, who the TSCO is, SSO, etc.);

b. Any special security precautions within the command, (e.g. restrictions on access);

c. Command security procedures for badging, security check-points, destruction, visitors, etc.;

d. Their responsibility to protect classified information;

e. Their obligation to report suspected security violations;

f. Their obligation to report information which could impact on the security clearance eligibility of an individual who has access to classified information;

5. The security orientation should be tailored to the command and to the individual receiving it. More emphasis on security procedures will be needed when the individual has not had previous experience handling classified information.

4-7 ON-THE-JOB TRAINING

1. 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.

2. Supervision of the on-the-job training process is critical. Supervisors are ultimately responsible for procedural violations or for compromises which result from improperly trained personnel. Expecting subordinates to learn proper security procedures by trial-and-error is not acceptable.

4-8 REFRESHER BRIEFINGS

1. Once a year, all personnel who have access to classified information will receive a refresher briefing designed to enhance security awareness.

2. The refresher briefing may be addressed to the entire command or it could be tailored for particular groups in the command. It should cover general security matters but need not cover the whole subject of security.

3. Refresher briefings should cover:

a. New security policies and procedures,

b. Counterintelligence reminders regarding reporting contacts and exploitation attempts and foreign travel issues;

c. Continuous evaluation;

d. Command specific security concerns or problem areas. Results of self-inspections, inspector general reports, or security violation investigations provide valuable information for use in identifying command weaknesses.

4-9 COUNTERINTELLIGENCE BRIEFINGS

Once every 2 years in accordance with SECNAVINST 5520.3B, Criminal and Security Investigations and Related Activities Within the Department of the Navy, 4 Jan 93, those who have access to material classified Secret or above must be given a counterintelligence briefing by an NCIS agent. The security manager is responsible for arranging for the briefing with the local NCIS office.

4-10 SPECIAL BRIEFINGS

Briefings not required as a matter of routine, but which may be governed by circumstances or other program requirements are considered special briefings and may include the following:

1. Foreign Travel Briefing

a. Although foreign travel (personal or business) may be briefly discussed during annual refresher briefings, it may also be appropriate to require separate foreign travel briefings for personnel, especially for those who travel frequently. It is in the best interest of the command and the traveler to ensure travelers are fully prepared for any particular security or safety concerns that the foreign travel may introduce.

b. A foreign travel briefing is usually only offered to those individuals who have access to classified information. However upon request, an unclassified version may be given to dependents, or others who do not have access, separately. (Individuals with SCI access should be referred to their SSO for foreign travel briefing requirements).

c. Upon return of the traveler, they should be provided the opportunity to report any incident - no matter how insignificant it might have seemed - that could have security implications.

d. Audiovisual material for a formal foreign travel briefing is stocked at servicing NCIS offices.

2. New Requirement Briefings. Whenever security policies or procedures change, personnel whose duties would be impacted by these changes must be briefed as soon as possible.

3. Program Briefings. Briefings that are specified or required by other program regulations (e.g. NATO, SIOP-ESI, SCI, etc.)

4-11 COMMAND DEBRIEFING

1. A debriefing will be given to individuals who no longer require access to classified information as a result of:

a. Transfers from one command to another;

b. Terminating active military service or civilian employment;

c. Temporarily separating for a period of 60 days or more, including sabbaticals, leave without pay status, or transferred to the Inactive Ready Reserves (IRR);

d. Expiration of a Limited Access Authorization (LAA);

e. Inadvertent substantive access to information which the individual is not eligible to receive;

f. Security clearance eligibility revocation; or

g. Administrative withdrawal or suspension of security clearance and SCI access eligibility for cause. Refer to reference (c) for additional information.

2. Debriefings must include the following:

a. All classified material in individuals' possession must be returned;

b. Individuals are no longer eligible for access to classified information;

c. Reminder of provisions of the Classified Nondisclosure Agreement (SF 312) to never divulge classified information, verbally or in writing, to any unauthorized person or in judicial, quasi-judicial, or in administrative proceedings without first receiving written permission of CNO (N09N);

d. There are severe penalties for disclosure; and

e. The individual must report to the NCIS (or to the FBI or nearest DoD component if no longer affiliated with the DON), without delay, any attempt by an unauthorized person to solicit classified information.

3. As part of a debriefing, individuals will be required to read the provisions of the Espionage Act and other criminal statutes. If individuals are retiring from active service and will be entitled to receive retirement pay, they must be advised that they remain subject to the Uniform Code of Military Justice (UCMJ).

4. As part of every debriefing (except when individuals transfer from one command to another command) a Security Termination Statement is required (paragraph 4-12 applies).

4-12 SECURITY TERMINATION STATEMENTS

1. Individuals must read and execute a Security Termination Statement (OPNAV 5511/14), exhibit 4A, at the time of debriefing, unless the debriefing is done simply because the individual is transferring from one command to another and will continue to require access to classified information.

2. A witness to the individual's signature must sign the Security Termination Statement.

3. The command, agency, or activity's name and mailing address will be annotated on the three lines at the top of the form.

4. The original signed and witnessed Security Termination Statement will be placed in the individual's official service record or the official personnel folder for permanent retention except:

a. When the security clearance eligibility of a Marine is revoked for cause, the original Security Termination Statement will be forwarded by the command to the Commandant of the Marine Corps (CMC) along with a copy of the revocation letter, for placement in the Master Service Record Book (MSRB).

b. When the Security Termination Statement is executed at the conclusion of a Limited Access Authorization, the original will be retained in command files for 2 years.

5. If an individual refuses to execute the Security Termination Statement, the individual will be debriefed, before a witness if possible, stressing the fact that refusal to sign the Security Termination Statement does not change the individual's obligation to protect classified information from unauthorized disclosure as stated on the Classified Information Nondisclosure Agreement (SF 312). The Security Termination Statement will be annotated to show the identity and signature of the witness, if one was present, and that the individual was debriefed, but refused to sign the Security Termination Statement. Send a copy of refusals only, to CNO (N09N2).

6. The Secretary of Defense has specifically directed that Security Termination Statements will be executed by senior officials (flag and general officers, ES-1 and above, Senior Executive Service and equivalent positions). The immediate senior officials will ensure that the statement is executed and that failure to execute the statement is reported immediately to the Deputy Assistant Secretary of Defense for Security and Information Operations (DASD(S&IO) via CNO (N09N2).

4-13 TRAINING FOR SECURITY PERSONNEL

1. The NCIS Mobile Training Team (MTT) offers the Naval Security Manager's Course, DON unique core training developed to train security managers, but also available to security specialists and assistants as quotas allow. For more information on this course,

contact the Atlantic MTT at NAB Little Creek, (804) 464-8925 or DSN 680-8925 or the Pacific MTT at NAS North Island, (619) 545-8934 or DSN 735-8934.

2. A Navy correspondence course entitled "Department of the Navy Introduction to the Information and Personnel Security Program," NAVEDTRA #13080, is available through the command education service officer (ESO).

3. For other security training available for DON personnel contact the CNO (N09N2) security education specialist at (202) 433-8858 or DSN 288-8858. Security training opportunities are also posted on the CNO (N09N2) Internet homepage at www.navysecurity.navy.mil.

4. CNO (N09N2) publishes the "Information and Personnel Security Newsletter" on a quarterly basis. This newsletter is also posted on the CNO homepage. The newsletter is not a directive, but states interpretations of security policies and procedures and provides advance notification of changes to the program. A roster of personnel assigned to CNO (N09N2), showing each area of responsibility is published aperiodically and posted on the homepage to assist you in routing your telephonic requests.

4-14 SECURITY AWARENESS

To enhance security, a security education program must include continuous and frequent exposure to current information and other awareness materials. Signs, posters, bulletin board notices, and Plan of the Day reminders are some of the media which should be used to promote security awareness.

EXHIBIT 4A

SECURITY TERMINATION STATEMENT

OPNAV 5511/14 (REV. 7-78)
S/N 0107-LF-055-1171

Enter name and address of appropriate Naval or Marine Corps activity obtaining statement.

NCIS MTT PAC

BOX 357141

SAN DIEGO CA 92135-7141

1. I HEREBY CERTIFY that I have conformed to the directives contained in the Information Security Program Regulation (OPNAV Instruction 5510.1), and the Communications Security Material System Manual (CMS-4) in that I have returned to the Department of the Navy all classified material which I have in my possession.

2. I FURTHER CERTIFY that I no longer have any material containing classified information in my possession.

3. I shall not hereafter communicate or transmit classified information orally or in writing to any unauthorized person or agency. I understand that the burden is upon me to ascertain whether or not information is classified and agree to obtain the decision of the Chief of Naval Operations or his authorized representative on such matters prior to disclosing information which is or may be classified.

4. I will report to the Federal Bureau of Investigation or to competent naval authorities without delay any incident wherein an attempt is made by an unauthorized person to solicit classified information.

5. I, JOHN RAY TAYLOR, have been informed and am aware that Title 18 U.S.C. Sections 793-799, as amended and the Internal Security Act of 1950 prescribe severe penalties for unlawfully divulging information affecting the National Defense. I certify that I have read and understand appendix F of the Information Security Program Regulation OPNAV Instruction 5510.1. I have been informed and am aware that certain categories of Reserve and Retired personnel on inactive duty can be recalled to duty, under the pertinent provisions of law relating to each class for trial by court-martial for unlawful disclosure of information. I have been informed and am aware that the making of a willfully false statement herein renders me subject to trial therefor, as provided by Title 18 U.S.C. 1001.

6. I have/have not received an oral debriefing.

SIGNATURE OF WITNESS	SIGNATURE OF EMPLOYEE OR MEMBER OF NAVAL OR MARINE CORPS SERVICE *(Fill in first, middle, and last name If military, indicate rank or rate. If civilian indicate grade.)*
Laine S. Marquet	John Ray Taylor LT USN
TYPE OR PRINT NAME OF WITNESS LAINE S. MARQUET, LT USN	DATE 1 OCT 1998

R-14794

CHAPTER 5

NATIONAL SECURITY POSITIONS

5-1 BASIC POLICY

1. National Security Positions include (1) those positions that involve activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and (2) positions that require regular use of, or access to, classified information.

2. Title 5 Code of Federal Regulations (CFR) 732.201 requires that positions identified as National Security Positions be assigned a position sensitivity level.

5-2 DESIGNATION OF SENSITIVE POSITIONS

1. A sensitive national security position is any position whose occupant could bring about, by virtue of the nature of the position, a material adverse effect on the national security. There are three sensitivity levels that apply to national security positions:

a.	Special-Sensitive (SS)*	Potential for inestimable impact and/or damage
b.	Critical-Sensitive (CS)	Potential for exceptionally grave impact and/or damage
c.	Noncritical-Sensitive (NCS)	Potential for serious impact and/or damage

*** Special Security Officer (SSO) Cognizance. Director of Central Intelligence Directive No. 1/14 (DCID 1/14), Personnel Security Standards and Procedures Government Eligibility for Access to Sensitive Compartmented Information (NOTAL) applies.**

2. Commanding officers will designate each National Security Position in their command, henceforth referred to as "sensitive" positions, as either special-sensitive, critical-sensitive, or noncritical-sensitive.

CHAPTER 5

NATIONAL SECURITY POSITIONS

5-1 BASIC POLICY

1. National Security Positions include (1) those positions that involve activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and (2) positions that require regular use of, or access to, classified information.

2. Title 5 Code of Federal Regulations (CFR) 732.201 requires that positions identified as National Security Positions be assigned a position sensitivity level.

5-2 DESIGNATION OF SENSITIVE POSITIONS

1. A sensitive national security position is any position whose occupant could bring about, by virtue of the nature of the position, a material adverse effect on the national security. There are three sensitivity levels that apply to national security positions:

a.	Special-Sensitive (SS)*	Potential for inestimable impact and/or damage
b.	Critical-Sensitive (CS)	Potential for exceptionally grave impact and/or damage
c.	Noncritical-Sensitive (NCS)	Potential for serious impact and/or damage

*** Special Security Officer (SSO) Cognizance. Director of Central Intelligence Directive No. 1/14 (DCID 1/14), Personnel Security Standards and Procedures Government Eligibility for Access to Sensitive Compartmented Information (NOTAL) applies.**

2. Commanding officers will designate each National Security Position in their command, henceforth referred to as "sensitive" positions, as either special-sensitive, critical-sensitive, or noncritical-sensitive.

5-3 *CRITERIA FOR DESIGNATING SENSITIVE POSITIONS*

1. Office of Management and Budget (OMB) Circular A-130, December 12, 1985 (NOTAL) provides the criteria for determining Automated Information Systems (AIS) risk levels, and 5 CFR 732 contains the criteria for designating position sensitivity for federal civilian employees.

2. It is vital to the national security that great care be exercised in the selection of individuals to fill sensitive positions. Similarly, it is important that only positions which meet one or more of the criteria set forth below be designated as sensitive:

a. Special-Sensitive (SS): Any position which the head of the agency determines to be at a level higher than Critical Sensitive because of (1) the greater degree of damage to the national security that an individual could effect by virtue of his/her position, or (2) or special requirements concerning the position under authority other than E.O. 10450 (e.g., DCID 1/14).

b. Critical-Sensitive (CS): Any position which includes:

(1) Access to Top Secret national security information.

(2) Development or approval of plans, policies, or programs which affect the overall operations of the Department of the Navy (e.g., policy making or policy determining positions).

(3) Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

(4) Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.

(5) Fiduciary, public contact, or other duties demanding the highest degree of public trust.

(6) Category I AIS (High Risk) positions in which the incumbent is responsible for the planning, direction and implementation of a computer security program; has a major responsibility for direction, planning, and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance in such a way, and with relatively high risk for causing grave damage or realizing

5-3 CRITERIA FOR DESIGNATING SENSITIVE POSITIONS

1. Office of Management and Budget (OMB) Circular A-130, December 12, 1985 (NOTAL) provides the criteria for determining Automated Information Systems (AIS) risk levels, and 5 CFR 732 contains the criteria for designating position sensitivity for federal civilian employees.

2. It is vital to the national security that great care be exercised in the selection of individuals to fill sensitive positions. Similarly, it is important that only positions which meet one or more of the criteria set forth below be designated as sensitive:

a. Special-Sensitive (SS): Any position which the head of the agency determines to be at a level higher than Critical Sensitive because of (1) the greater degree of damage to the national security that an individual could effect by virtue of his/her position, or (2) or special requirements concerning the position under authority other than E.O. 10450 (e.g., DCID 1/14).

b. Critical-Sensitive (CS): Any position which includes:

(1) Access to Top Secret national security information.

(2) Development or approval of plans, policies, or programs which affect the overall operations of the Department of the Navy (e.g., policy making or policy determining positions).

(3) Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

(4) Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.

(5) Fiduciary, public contact, or other duties demanding the highest degree of public trust.

(6) Category I AIS (High Risk) positions in which the incumbent is responsible for the planning, direction and implementation of a computer security program; has a major responsibility for direction, planning, and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance in such a way, and with relatively high risk for causing grave damage or realizing

significant personal gain.

(7) Any other position so designated by the Secretary of the Navy and/or his designee.

c. Noncritical-Sensitive (NCS): Any position which involves:

(1) Access to Secret or Confidential national security information.

(2) Assignment to duties involving the protection and safeguarding of DON personnel and property (e.g., security police, provost marshall).

(3) Duties involving education and orientation of DoD personnel.

(4) Duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DON personnel and property.

(5) Category II AIS (Moderate Risk) positions in which the incumbent is responsible for the direction, planning, design, operation or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the Critical-Sensitive level to insure the integrity of the system.

(6) Any other position so designated by the Secretary of the Navy and/or his designee.

d. All other civilian positions in the DON are to be designated as non-sensitive, including category III AIS positions.

4. Commanding officers are responsible for ensuring that only those positions that meet the above criteria are designated as sensitive; and that the number of positions designated as sensitive is held to the minimum consistent with mission requirements.

5. The process of designating sensitive positions is best accomplished in coordination with the personnel program manager, the position supervisor or program manager, the security manager and the AIS manager for AIS risk determinations, as appropriate. The commanding officer may establish standard operating procedures (SOP) to discharge this responsibility.

6. The command security manager will maintain a record of position designation decisions. The record will identify sensitivity level, the required investigation, and indicate as appropriate the level of access to classified information required and/or whether the position involves an AIS risk. The record will also list the criteria most predominately responsible for the sensitivity determination assigned. Access to classified information will normally be predominate. A recommended format is provided in exhibit 5A, or the command may develop their own unique record.

5-4 SUITABILITY DETERMINATION AUTHORITY

The Office of Personnel Management (OPM) is charged with establishing the program for investigating and adjudicating the suitability of Federal Government applicants for and appointees to the Federal civil service. OPM uses the US Investigative Service (USIS) to carry out its investigative mission. OPM has further delegated the authority to adjudicate suitability to heads of agencies.

5-5 SUITABILITY DETERMINATIONS

1. Suitability means "fitness" or eligibility for employment. Potentially disqualifying suitability factors may be found in Title 5 CFR 731. The focus of a suitability adjudication is whether the employment of an individual can reasonably be expected to promote the efficiency of the Federal Service. The focus of a security adjudication is whether the assignment or continued assignment of the individual in a sensitive position can reasonably be expected to be clearly consistent with the nation's security interests.

2. Personnel security investigations are conducted to gather information for two purposes; to meet OPM requirements for accomplishing employment suitability determinations and to satisfy requirements for security determinations.

3. The standards and requirements for personnel security investigations are contained in paragraph 6-4. Security determinations are made subsequent to favorable suitability adjudications. Suitability adjudications are based on standards and criteria established by OPM and contained in Title 5 CFR 731 and are a command responsibility. Security determinations are based on criteria found in this regulation and are in most cases the DON CAF responsibility.

4. OPM forwards all completed investigations to the DON CAF. The DON CAF has been delegated the authority in the DON to make de facto suitability determinations only on investigations closed without actionable issues. In cases without issue, a favorable security determination equates to a favorable suitability determination. All other investigations must be adjudicated by the command for suitability before the DON CAF security determination can be made. The following procedures have been established to accomplish this requirement:

a. Investigations for non-sensitive positions are forwarded by the DON CAF to the command for the suitability determination. There is no adjudication action by the DON CAF.

b. Investigations for sensitive positions:

(1) When the OFI Form 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations, indicates "No Actionable Issue," the investigation will not normally be returned to the requesting command. The DON CAF will favorably adjudicate the investigation, as appropriate, enter the favorable determination in the Navy Joint Adjudication and Clearance System (NJACS), and notify the command of the determination. The DON CAF will complete the OFI 79A and forward it to OPM-FIPC. A favorable security determination on a "No Actionable Issue" case will result in an automatic favorable suitability determination.

(2) When the OFI 79A indicates "Actionable Issues," the completed investigation, with the OPM Certification of Investigation and OFI 79A, will be forwarded to the requesting command for a suitability determination. If the requesting command makes a favorable suitability determination, it will be indicated in the applicable blocks on the OFI 79A and the entire package will be returned to the DON CAF to make a security determination. If the <u>suitability</u> determination made by the command is <u>unfavorable</u>, it remains a personnel action and no DON CAF action is required.

5-6 DETERMINING ELIGIBILITY TO OCCUPY A SENSITIVE POSITION

1. The determination of eligibility to occupy a sensitive position is made by the DON CAF based on the appropriate investigation using the criteria and procedures provided in paragraph 7-1. The same criteria and procedures are applied to both security clearance and sensitive position eligibility determinations. A determination by the DON CAF that an individual is not eligible for assignment to sensitive duties will also result in the removal of clearance eligibility whether

or not the individual requires a clearance to perform sensitive duties. Conversely, a determination by the DON CAF that an individual is not eligible for access to classified information will also result in a determination of ineligibility to occupy a sensitive position.

2. Emergency Appointments. In cases where a command must hire an individual prior to completion of an investigation for suitability or security determination, emergency appointment procedures contained in paragraph 6-6.7 apply.

5-7 NON-US CITIZENS IN SENSITIVE POSITIONS

1. Under E.O. 11935, "Citizenship Requirements for Federal Employment", September 2, 1976, a non-U.S. citizen cannot be appointed to a civilian position in the Federal civil service without approval from the Office of Personnel Management (OPM). OPM's approval of employment is not to be construed as a personnel security determination, authorizing assignment to sensitive duties or access to classified information. If the position for which OPM's approval is sought is a sensitive position, CNO (N09N2) must first approve it to insure that assignment or access would not be prohibited or restricted. (For example, there would be no point in asking for OPM's approval of an immigrant alien for a position requiring a security clearance.)

2. Requests for CNO (N09N2) approval will include:

a. The full identity of the individual;

b. All compelling reasons for approving assignment to include special expertise;

c. The type of duties to be performed, the type of sensitive information to be accessed, the date and type of investigation conducted when available, and if there is no completed investigation, the date the investigation was requested and a copy of the request forms; and the security measures in place to preclude the individual from having access to classified information.

3. All completed investigations conducted on non-U.S. citizens occupying sensitive positions will be forwarded to CNO (N09N2) to make the required sensitive position security adjudication.

EXHIBIT 5A

DATE

MEMORANDUM FOR RECORD

SUBJ: DESIGNATION OF POSITION SENSITIVITY, SECURITY CLEARANCE AND PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS

Ref: (a) SECNAVINST 5510.30A

1. Per reference (a), position sensitivity, security clearance level and personnel security investigative requirements are certified, as indicated, for the following position:

a. Position Description Number: AC123

b. Position Title: SUPERVISORY COMPUTER SPECIALIST

c. Grade/series: GS-0334-15

d. Position Sensitivity: Critical-sensitive

e. Security Clearance Level: Top Secret

f. Required Investigation: SSBI

g. AIS Risk: AIS Category II, Moderate Risk

2. Position sensitivity is based on the criteria found in reference (a), paragraph (5-3).

XXXXXXXX
(Signature Block will include the internal code of the individual signing this document)

CHAPTER 6

PERSONNEL SECURITY INVESTIGATIONS

6-1 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 following officials are authorized to request PSIs on individuals under their jurisdiction:

a. Commanding officers of organizations and activities listed on the Standard Navy Distribution List (SNDL); and Marine Corps List of Activities - MARCORPS 2766;

b. Director, Department of the Navy Central Adjudication Facility (DON CAF); and

c. Chiefs of recruiting stations.

3. The scope of the investigation conducted will be commensurate with the level of sensitivity of the access required or position occupied. Only the minimum investigation to satisfy a requirement may be requested. CNO (N09N2) must give prior approval to establish investigative requirements in addition to, or at variance with, those established here.

4. The Defense Security Service (DSS) or, where specified, the US Investigative Service (USIS), conducts (or controls the conduct of) all PSIs for the DON. DON elements are prohibited from conducting PSIs, including local public agency inquiries, unless specifically requested to do so by an authorized investigative agency (e.g., DSS or USIS). An exception to this restriction is made for DON overseas commands employing foreign nationals for duties not requiring access to classified material. Paragraph 6-8, subparagraph 1.n. provides further details.

5. PSIs will not normally be requested for any civilian or military personnel who will be retired, resigned, or separated with less than 1 year service remaining.

6-2 TYPES OF PERSONNEL SECURITY INVESTIGATIONS

1. The term **Personnel Security Investigation** describes an inquiry by an investigative agency to determine 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 requiring such investigation. Investigations conducted for other basic purposes may have an impact on security clearance determinations but are not PSIs. (Examples of other types are investigations of compromise, criminal activity, sabotage, espionage or subversion.)

2. PSIs are as follows:

a. **National Agency Check (NAC)**. A NAC was historically conducted for officer commissioning and provided the basis for access up to and including Secret classified information. The NAC was replaced by the National Agency Check with Local Agency and Credit Checks (NACLC) in accordance with reference (a) for access requirements, but remains the standard for trustworthiness determinations. The NAC includes a search of the Defense Clearance and Investigations Index (DCII), Federal Bureau of Investigation (FBI) files and files of other appropriate federal government agencies (Immigration and Naturalization Service (INS), Office of Personnel Management (OPM), Central Intelligence Agency (CIA), etc.) for information relevant to suitability and personnel security determinations. A NAC is an integral part of each Single Scope Background Investigation (SSBI), Periodic Reinvestigation (PR) and Secret Periodic Reinvestigation (SPR). A technical fingerprint search of the FBI files is conducted as part of a NAC, except during a PR.

b. **Entrance National Agency Check (ENTNAC)**. An ENTNAC is a NAC usually conducted to determine suitability of first-term enlistees in the Navy and Marine Corps. It includes the basic elements of the NAC but it does not include a technical fingerprint search of FBI files. For an ENTNAC, the FBI files are checked by name only. If a service member re-enlists after a break in active service greater than 24 months, a NAC (not an ENTNAC) is requested.

c. **National Agency Check with Written Inquiries (NACI)**. A NACI is required by the Office of Personnel Management (OPM) for

civilian employees for Federal Government suitability determinations. NACIs are directed by E.O. 10450 and are conducted by the USIS to meet the investigative requirements for appointment to a nonsensitive or noncritical-sensitive positions.

d. **Access NACI (ANACI).** An ANACI is conducted by USIS and includes a NACI and meets the investigative requirements for appointment to nonsensitive and non-critical sensitive positions. An ANACI also meets the reference (a) investigative requirements for Confidential and Secret security clearance eligibility. The ANACI includes a NAC, a credit check, and written inquiries covering the last 5 years to law enforcement agencies, to former employers and supervisors, to references, and to schools. USIS also conducts a Minimum Background Investigation (MBI), a Limited BI (LBI) and a Single Scope BI (which they refer to as an SBI) for agencies other than DoD. For the purposes of this regulation, an MBI or LBI is an acceptable equivalent to an ANACI.

e. **National Agency Check with Local Agency and Credit Checks (NACLC).** A NACLC is conducted by DSS and is required to support suitability determinations on military officers and Secret and Confidential security clearance determinations. The NACLC includes a NAC, inquiries of law enforcement agencies and a credit check.

f. **SSBI.** An SSBI is usually conducted by DSS, as the investigative basis for Top Secret and SCI access eligibility determinations. It includes extended coverage of the subject's background to provide a complete picture of character, loyalty, trustworthiness, and reliability.

(1) Elements of an SSBI include a NAC, verification of the subject's date and place of birth, citizenship, education and employment, neighborhood interviews, developed character reference interviews, credit checks, local agency checks, public record checks (i.e., verification of divorce, bankruptcy, etc.), foreign travel, foreign connections and organizational affiliations, with other inquiries as appropriate. A subject interview is conducted, as well as a NAC of the subject's spouse or cohabitant. The scope of an SSBI covers the most recent 10 years of the subject's life or from the 18th birthday, whichever is the shorter period; however, at least the last 2 years will be covered. No investigation is conducted prior to the subject's 16th birthday. Additional investigative requirements exist for individuals requiring SCI access eligibility who have foreign national immediate family members (reference (c) applies).

(2) SSBIs are required for assignment to Special Sensitive positions; access to Top Secret information, access to Single Integrated Operational Plan - Extremely Sensitive Information (SIOP-ESI) and access to Sensitive Compartmented Information (SCI); assignment to critical-sensitive positions, assignment to critical positions in the Nuclear Weapon Personnel Reliability Program (PRP); assignment to certain Presidential Support activities; granting non-U.S. citizens Limited Access Authorizations (LAA); assignment as a security manager, assignment as a security clearance adjudicator, or for assignment to an investigative agency as a special agent or investigative support personnel requiring continuous access to investigative files and material.

(3) Any investigation conducted by a Federal agency in accordance with National Security Decision Directive 63 (NSDD-63), meets SSBI investigative requirements. A Full Field Investigation (FFI) conducted by the FBI, State Department or U.S. Secret Service is usually equivalent to an SSBI. The FFI will be reviewed by the DON CAF to ensure that all the investigative elements have been covered.

g. **Reinvestigation**. A reinvestigation updates a previous investigation and is authorized only for specific duties and access. The extent of the investigative coverage for reinvestigations is proportional to the sensitivity level of the duties and/or access. There are two scopes for reinvestigations, the Periodic Reinvestigation (PR) completed to update an SSBI and the Secret or Confidential Periodic Reinvestigation (SPR) or (CPR) completed to update a NAC, ENTNAC, NACI or NACLC.

(1) **PR:** PRs are conducted on personnel whose clearance/access to SCI or Top Secret information is based on an investigation that is 5 years old or more. The PR is also required to support personnel security determinations on personnel assigned to NATO billets requiring Top Secret (COSMIC) access, assignment to Nuclear Weapons Personnel Reliability Program (PRP) critical positions, assignment to Presidential Support Activities, access to SIOP-ESI, assignment to critical-sensitive and special-sensitive positions and for Limited Access Authorizations (LAAs) for non-U.S. citizens. The PR investigative elements include: a NAC (except that a technical fingerprint check of FBI files is not conducted); a subject interview, a credit check, an employment check, neighborhood interviews, local agency checks, interviews of employers and developed character references, an ex-spouse interview, and additional investigation when warranted by the facts of the case.

(2) **SPR or CPR:** SPRs are required by reference (a) for persons with a Secret clearance at 10-year intervals. CPRs are required by reference (a) for persons with a Confidential clearance at 15-year intervals. As an exception, SPRs are conducted at 5-year intervals for personnel in Special Access Programs (SAPs) with access to Secret classified information and those performing Explosive Ordnance Disposal (EOD) or Personnel Reliability Program (PRP) duties. The SPR and CPR include the elements of the NACLC.

h. **Special Investigative Inquiry (SII).** An SII is an investigation conducted to resolve personnel security issues which arise after a PSI is conducted, evaluated or adjudicated. SII's are scoped as necessary to address the specific matters to be resolved. They usually consist of record checks and interviews with potentially knowledgeable persons. The subject of the investigation may be interviewed to resolve conflicting information and/or to provide an opportunity to refute or mitigate adverse information. The term "SII" applies to limited inquiries, post-adjudication investigations or other additional inquiries conducted by DSS. SIIs do not cover investigations of criminal activity, sabotage, espionage, or subversion. Those are matters under the investigative jurisdiction of the NCIS. SII's are usually requested by the DON CAF.

3. When adverse or questionable information is developed during a PSI, regardless of type, the investigation is expanded to the extent necessary to substantiate or disprove the information. A personal interview of the subject will be conducted by DSS when necessary to resolve or clarify any information which may impute the subject's moral character, threaten the subject's future Federal employment, raise the question of the subject's eligibility for security clearance, or be otherwise incriminating.

4. **Hostage/Foreign Connection Investigation Interview.** For PSI purposes, a hostage situation may exist when members of an individual's immediate family, or any other person to whom the individual is bound by obligation or affection, lives in a country whose interests are contrary to the interests of the United States. In the absence of indications that the individual is being subjected to coercion, influence, blackmail, or pressure, a personal interview will be conducted by a DSS agent or, when authorized, by investigative personnel of other DoD investigative organizations. If the hostage relationship is known at the time an SSBI or PR is being conducted, DSS will include hostage situation coverage as a part of the investigation. If the hostage relationship is known at the time of

submission of a NACI request to OPM, the commanding officer will concurrently request an SII from DSS. The request form to OPM should be annotated to indicate that an SII has been requested from DSS. The request form to DSS should be annotated to indicate that a NACI has been submitted to OPM. When there are indications that any action is being specifically directed against the individual or if there is evidence that the individual is being coerced, influenced or pressured, the case becomes a counter-intelligence matter to be referred to the NCIS.

5. **Prenomination Interview**. A prenomination interview is conducted for applicants/potential nominees for SCI access. Guidance for the conduct of the prenomination interview is provided in the Navy Supplement (NAVSUPP) to DoD Dir S-5105.21. M-1. A designee of the command to which the applicant or potential nominee is assigned will conduct the interview.

6-3 RESTRICTIONS DURING SUBJECT INTERVIEWS

Questions pertaining to an individual's sexual orientation are not permitted on personnel security questionnaires, supplemental questionnaires or screening forms, and will not be asked during subject interviews. However, an individual's sexual conduct whether heterosexual or homosexual, may be developed by investigative agencies as an issue of legitimate security concern if the individual is susceptible to exploitation or coercion, or if the conduct is indicative of a lack of the trustworthiness, reliability or good judgment required of all personnel with access to classified information.

6-4 INVESTIGATIVE REQUIREMENTS FOR PERSONNEL SECURITY CLEARANCE

1. Only United States citizens are eligible for security clearance. Guidance for validating citizenship status is found in appendix I.

2. Security clearance eligibility for access to classified information will be based on a PSI prescribed for the level of classification.

a. Top Secret. The investigative basis for Top Secret clearance eligibility is a favorably completed SSBI or PR. For those who have continuous assignment or access to Top Secret, critical sensitive positions, SCI, Presidential Support Activities, COSMIC Top Secret, LAA, PRP or SIOP-ESI, the SSBI must be updated every 5 years by a PR.

b. Secret/Confidential. The investigative basis for Secret or Confidential clearance eligibility is a favorably completed NACLC or ANACI. Clearances granted based on ENTNAC's NAC's or NACI's prior to NACLC or ANACI implementation remain valid. For PRP and Secret SAP's, the NACLC must be updated every 5-years by a SPR. For Secret and Confidential clearance, the investigation is updated every 10 and 15-years, respectively.

6-5 INVESTIGATIVE REQUIREMENTS FOR MILITARY APPOINTMENT OR ENLISTMENT

1. An ENTNAC is required for each enlisted member of the Navy and Marine Corps, including Reserve components, at the time of initial entry into the service.

2. A NACLC is required for each commissioned officer, warrant officer, midshipman and Reserve Officer Training Corps candidate before appointment. Exceptions may be made to this general rule to allow the commissioning of Navy Reserve health professionals, chaplains, and attorneys before completion of the NAC when a need exists, if the NACLC has been initiated and the applicant has acknowledged in writing that, if the NACLC develops information that disqualifies the applicant as an officer candidate, he/she will be subject to discharge.

3. All derogatory information revealed during the enlistment or appointment process that results in a waiver of accession standards will be fully explained in a written summary attached to the SF 86 and submitted with the request for the required ENTNAC/NACLC.

4. The authority to take action to deny acceptance or retention in the Navy and Marine Corps, except for loyalty reasons, is vested in the Chief of Naval Personnel and the Commandant of the Marine Corps. Cases involving loyalty issues will be forwarded to CNO (N09N2) for referral to the Secretary of the Navy for action. The procedures prescribed in SECNAVINST 1910.4B, Enlisted Administrative Separation, 29 May 96 (NOTAL), govern loyalty determinations for enlisted personnel and SECNAVINST 1920.6A, Administrative Separation of Officers, 21 Nov 83 (NOTAL) govern loyalty determinations for officer personnel.

5. A previously conducted PSI which is still valid for security clearance purposes may suffice for appointment or commissioning purposes. A new investigation is required upon reentry of officers and enlisted members if there has been a break in active service greater than 24 months.

6. Requests for investigation for Navy and Marine Corps reserve members will be submitted by the active duty command holding the service record or exercising administrative jurisdiction.

7. Mobilization. For the purposes of partial or full mobilization under provisions of 10, U.S.C. (Title 14 pertaining to the U.S. Coast Guard as an element of the DON), the requirement for a NAC upon reentry may be waived.

6-6 INVESTIGATIVE REQUIREMENTS FOR CIVILIAN EMPLOYMENT IN SENSITIVE POSITIONS

1. A NACI is required for each civilian employee of the DON appointed to a nonsensitive position. (Note: If access to classified information is required in performance of those duties, an ANACI will always be required.)

2. An SSBI is required for each civilian employee of the DON appointed to a critical-sensitive or special-sensitive position.

3. A previously conducted NACI or SSBI may satisfy federal civilian employment suitability requirements; however, a previously conducted ENTNAC or NAC will not. A new NACI or SSBI is required for reappointment to a Federal Government position if there has been a break in service greater than 24 months.

4. The authority to deny appointment or terminate employment of civilian personnel for loyalty reasons is vested solely in the Secretary of the Navy, under procedures established in compliance with Title 5 CFR 732. Any civilian whose employment has been terminated under the provisions of Title 5 CFR 732 will not be reinstated, restored to duty or reemployed unless the Secretary of the Navy finds that such reinstatement, restoration or reemployment is clearly consistent with the interests of national security.

5. Each civilian employee appointed under civil service procedures, including consultants and Intergovernmental Personnel Act (IPA) employees, is subject to investigation to determine suitability for federal employment. Employees being reappointed are exempt from this requirement only if their break in employment is less than 24 months.

6. Temporary Employment. A NACI is the minimum requirement for civilian summer hires in noncritical-sensitive positions and nonsensitive positions of 180 days or more. For appointment to a nonsensitive position for 180 days or less an investigation is not required (e.g., summer hires, intermittent and seasonal

appointees, or work/study and cooperative education program employees).

7. Emergency Appointments. If the appointee does not have the necessary investigative basis for appointment, he/she may be placed in a noncritical-sensitive position only as an emergency measure after: the commanding officer determines that delay in appointment would be harmful to the national security, the NACI has been requested, and a check of locally available records is favorable. The commanding officer's justification for the emergency appointment will be recorded in writing. Commands must maintain a central file of all emergency appointments for review during security and personnel management evaluations. The record of emergency appointments will include:

a. Identifying data on the appointee to include full name, social security number, date and place of birth, position or job title;

b. Organizational location of the position;

c. Position sensitivity and designation criterion;

d. Certification and justification by the commanding officer that emergency appointment is necessary. (In determining whether emergency appointment is justified; a delay in appointment may be considered harmful to the national security if regulatory requirements and mission-essential functions or responsibilities cannot be met and no other cleared or otherwise qualified personnel are available on a temporary basis to do the work.)

e. A statement that a check of locally available records was favorable; and

f. The date that the required PSI was requested. For a critical-sensitive position, the record will also include the date of the ENTNAC, NAC, NACI, NACLC or ANACI which formed the basis for emergency appointment.

8. To keep emergency appointments to the absolute minimum, activities must anticipate the need to fill a sensitive position and request the required investigation sufficiently in advance of the desired date of appointment.

9. Mobilization. For the purpose of mobilizing selected civilian annuitants under Title 5 U.S.C., with a break in active service greater than 24 months, investigative requirements will be expedited or waived, depending on the sensitivity of the

position. Priority will be afforded to mobilized reemployed annuitants being assigned to intelligence and security activities with respect to granting security clearances.

6-7 INVESTIGATIVE REQUIREMENTS FOR DON CONTRACTOR PERSONNEL

1. Investigative requirements for DON contractor personnel are managed under the National Industrial Security Program (NISP). Requests for investigation of contractor personnel for security clearance eligibility are processed by the DSS Operations Center, Columbus. When Sensitive Compartmented Information (SCI) access is at issue, reference (c) applies.

2. Contractor employees who require access to DON controlled/restricted areas, sensitive information or equipment not involving access to classified information will be processed under the DON Facility Access Determination (FAD) Program. FAD program procedures are found in paragraphs 7-6 and 7-7.

3. Consultants Hired by a DON Government Contracting Activity (GCA). A consultant who is hired by a DON command or activity who will work strictly at the command/activity and requires access to classified information only at the command/activity or in connection with authorized visits, will have security clearance eligibility established under this regulation. The consultant is considered for security clearance purposes as an employee of the DON command/activity and is investigated by DSS and adjudicated by the DON CAF, as appropriate.

6-8 OTHER INVESTIGATIVE REQUIREMENTS FOR SPECIFIC PERFORMANCE OF DUTY

1. The following specific duties have assigned minimum investigative or clearance requirements:

a. Security Manager. The designated security manager of a command must have a favorably adjudicated SSBI or PR completed within the past 5 years.

b. Clearance Granting Authorities. Persons authorized to adjudicate PSIs and/or grant, deny or revoke security clearances must have a favorably adjudicated SSBI or PR completed within the past 5 years.

c. Appellate Authorities. Persons selected to serve with a board, committee, or other group responsible for adjudicating appeals of personnel security determinations must have a

favorably adjudicated SSBI or PR completed within the past 5 years.

d. Educational and Training Programs. Persons selected for duties in connection with formal programs involving the education and training of military or civilian personnel must have a favorably adjudicated NAC/NACI prior to assignment. This requirement applies to those assigned to formal programs and does not include those incidentally involved in training. It does not apply to teachers or administrators associated with university extension courses conducted on DON installations in the United States.

e. Cryptographic Duties. Personnel assigned to cryptographic duties must have security clearance eligibility established prior to authorizing access at a level commensurate with the level of classified U. S. cryptographic information they will require. Interim security clearances are not valid for access to U.S. cryptographic information.

f. Investigative Duties. Investigative agents and other personnel assigned to investigative agencies whose official duties require continuous access to investigative files and material require a favorably adjudicated SSBI or PR completed within the past 5 years.

g. Non-Appropriated Fund (NAF). NAF employees are not Federal employees; therefore, submitting a NACI request to the OPM is not appropriate. NAF employees assigned to positions of trust within DoD require completion of a favorable NAC by DSS. A favorably completed prior investigation for Federal service will satisfy this requirement if there has not been a break in service greater than 24 months between the Federal service and employment by Non-Appropriated Fund Instrumentalities. When the individual employed in a position of trust requires access to classified information, the individual will be processed for a security clearance as directed by chapter 8.

h. American Red Cross/United Service Organization (USO). A favorably adjudicated NAC is required on American Red Cross or USO personnel as a prerequisite for assignment to activities overseas. If Red Cross or USO personnel assigned to duties with U.S. Navy or U.S. Marine Corps activities overseas will require access to classified information, they will be nominated for access as specified in paragraph 9-14.

i. Chemical Agents. Personnel whose duties involve access to or security of chemical agents require a favorably adjudicated

NAC completed within the past 5 years before assignment, in accordance with SECNAVINST 5510.29A, Chemical Agent Security Program, 13 Mar 87 (NOTAL).

j. Customs Inspectors. DON personnel, appointed as custom inspectors under waiver require a favorably adjudicated NAC completed within the past 5 years in accordance with SECNAVINST 5840.6, Custom Inspections, 13 Apr 72 (NOTAL).

k. AIS. Personnel whose duties meet the criteria for an AIS-I designation require a favorably adjudicated SSBI or PR. The SSBI or PR will be updated every 5 years. (NOTE: AIS-I equates to a designation for civilian critical-sensitive positions. This AIS requirement also applies to military members whose duties meet the AIS-I criteria and for whom an SSBI or PR would not otherwise be justified.) A favorably adjudicated NACI for civilian personnel and a favorably adjudicated NAC for military members is required for AIS-II and AIS-III positions. Paragraph 5-3 provides a description of the AIS position designations.

l. Arms, Ammunition and Explosives (AA&E). Personnel operating a vehicle or providing security to a vehicle transporting Category I, II or Confidential AA&E require a favorably adjudicated NAC, ENTNAC or NACI.

m. Contract Guards. Contract guards require a favorably adjudicated NAC.

n. Foreign Nationals Employed Overseas. Certain record checks are required before a DON overseas command can employ a foreign national for duties not requiring access to classified information. The hiring command will request the servicing NCIS office or the military organization having investigative jurisdiction to conduct a record check of the host government law enforcement and security agencies at the city, state (province) and national level, wherever it is legally possible to do so. At the same time, the command will request the NCIS to check the DCII and, if the foreign national resided in the U.S. for 1 year or more after age 18, the Federal Bureau of Investigation-Headquarters/Identification Division (FBI-HQ/ID).

o. Nuclear Weapon Personnel Reliability Program (PRP). SECNAVINST 5510.35, Nuclear Weapon Personnel Reliability Program (PRP), 11 Oct 94, provides the standards of individual reliability required for personnel performing duties involving nuclear weapons and components. PRP requires commands to screen personnel before transferring them to training leading to PRP

assignment. The investigative requirements for PRP assignment are based on the position designation. PRP positions are designated as either **critical** or **controlled**.

(a) **Critical PRP position**. The investigative requirement for initial assignment to a critical PRP position is a favorably adjudicated SSBI completed within the past 5 years. This requirement may also be satisfied by a favorable PR. If there is no investigation to satisfy the requirement for initial assignment, the command must request an SSBI. A PR is required every 5 years.

(b) **Controlled PRP position**. The investigative requirement for initial assignment to a controlled PRP position is a favorably adjudicated NAC completed within the past 5 years. The requirement may be satisfied by a favorably adjudicated ENTNAC, NAC, NACI, SPR, SSBI, or PR completed within the past 5 years. If there is no investigation to satisfy the requirements for initial assignment, the command must request a NACLC. A SPR is required every 5 years.

2. If an individual requires different levels of investigations to accomplish differing assignments, request the greater investigation to satisfy all requirements.

6-9 PROGRAMS WITH SPECIAL INVESTIGATIVE REQUIREMENTS

1. Executive Order 12968 establishes, to the extent possible, uniform and consistent personnel security investigative requirements. Accordingly, investigations exceeding established requirements are authorized only when mandated by statute, national regulations or international agreement. In this regard, there are certain programs originating at the national or international level that require specific investigation and unique procedures. These programs are as follows:

a. **Special Access Programs (SAPs)**. Special Access Programs are discussed in paragraph 1-7 and are established in DoD under SAP Oversight Committee (SAPOC) authority. SAP requirements may include, but are not limited to, special clearance eligibility, additional adjudication, unique investigative requirements, material dissemination restrictions, and formal identification of personnel with need to know. These requirements are individually dictated by the SAP manager.

b. **Sensitive Compartmented Information (SCI)**. The investigative requirement for access to SCI is a favorably adjudicated SSBI. A PR is required every 5 years. The

requirements for SCI access are established under Director of Central Intelligence (DCI) authority (reference (c) applies). When military personnel are ordered to billets requiring SCI access, the transfer orders will identify the requirement. The losing command's security manager/SSO must ensure the required investigative requests are submitted promptly prior to transfer. If an individual is indoctrinated for SCI access, the commanding officer may not administratively lower the individual's security clearance below the Top Secret level without approval of the DON CAF.

c. **Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI).** Investigative requirements for access to Single Integrated Operational Plan (SIOP) information vary depending on whether the information to be accessed is SIOP or SIOP-ESI. OPNAVINST S5511.35K, Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U), 1 Jul 98 (NOTAL), provides administrative requirements:

(1) Access to SIOP is based on need to know and requires security clearance eligibility commensurate with the classification of the information to be accessed.

(2) Access to SIOP-ESI requires a Top Secret security clearance eligibility based on a favorably adjudicated SSBI. The SSBI need not have been completed within the past 5 years to grant access to SIOP-ESI, providing a new SSBI or PR is initiated within 30 days.

d. **Presidential Support Activities (PSA).** SECNAVINST 5312.12B, Selection of Department of the Navy Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities, 22 Sep 83, prescribes the policies and procedures for the nomination, screening, selection, and continued evaluation of DON military and civilian personnel and contractor employees assigned to or used in PSA. There are two categories of PSA assignments, Category One and Category Two.

(1) Personnel nominated for Category One and Category Two duties must have been the subject of a favorably adjudicated SSBI completed within the 12 months preceding selection into Presidential Support duties.

(2) The U.S. citizenship of foreign-born immediate family members of all Presidential Support nominees must be verified by investigation. If the individual marries or cohabitates after completion of the SSBI, a NAC for the spouse or cohabitant must be requested.

e. **North Atlantic Treaty Organization (NATO).** An equivalent level United States security clearance is the basis for access to NATO classified information. OPNAVINST C5510.101D, NATO Security Procedures (U), 17 Aug 82 (NOTAL), prescribes the policies and procedures for this program.

(1) The investigative basis for assignment to a NATO billet is a favorably adjudicated SSBI, PR, NACI, NAC, ENTNAC, or NACLC, depending on the level of clearance and access the billet requires. The investigation must have been completed within the 5 years preceding the assignment. Continued assignment to a NATO COSMIC billet requires a PR every 5 years. For access to NATO Secret information, an SPR is required every 5 years.

(2) For Navy military members under permanent change of station (PCS) orders to NATO billets, detailers will coordinate with the Chief of Naval Personnel (CHNAVPERS) (Pers-831) to ensure that investigations are properly completed. Pers-831 provides instructions to ensure that proper investigative requests are submitted for NATO billet candidates. Instructions will specify that the command may not execute the PCS orders until specifically released to do so by Pers-831, after verification of investigation and coordination with the DON CAF.

(3) Personnel who have access to NATO information but are not assigned to NATO billets will have a security clearance eligibility commensurate with the level of access required.

2. This regulation is <u>not</u> the governing instruction for the programs listed in this paragraph. Consult the governing instructions for a full description of program requirements.

6-10 RECIPROCITY

1. Investigations will not be duplicated when a previously conducted investigation meets the scope and standards for the level required. Previously conducted investigations by Federal Government agencies will be mutually and reciprocally accepted.

2. Whenever security clearance eligibility is established, agencies will not request DSS or other investigative organizations to forward prior investigative files for review unless:

a. Potentially disqualifying information is developed since the last favorable adjudication;

b. The individual is being considered for a higher level clearance eligibility; and

c. The most recent clearance or access authorization was conditional or based on a waiver.

3. When DON personnel are assigned or detailed to other Federal agencies (i.e., DOE and NRC, etc.), the DON command that maintains the individual's service record, or official personnel file, will be responsible for initiating the required personnel security investigation. The completed investigation will be forwarded to the DON CAF for a security clearance eligibility determination.

4. When it becomes necessary for a commanding officer to grant access to personnel from another military department or DoD agency who do not have the required security clearance eligibility, the command granting access will submit the request for investigation to DSS indicating that the results are to be forwarded to the person's parent Central Adjudication Facility (CAF). The parent CAF will be responsible for expeditiously transmitting results of the security clearance determination to the requestor.

6-11 LIMITATIONS ON REQUESTING PERSONNEL SECURITY INVESTIGATIONS

1. PSIs for purposes other than allowed by this regulation are not authorized unless detailed justification has been submitted to CNO (N09N2) and approved by ASD(C3I).

2. Before requesting an investigation, activities must determine that the individual does not have an investigation which satisfies the requirements.

3. Requests for PSIs will not normally be submitted on any civilian or military personnel who will be retired, resigned, or separated with less than 1 year service remaining.

4. Review of Prior Investigations. Prior personnel security investigations may only be requested for review in support of an official requirement. Official requirements include determining eligibility for special access, critical PRP positions, or assignment to special-sensitive duties; acceptance or retention in the Armed Forces; or appointment or retention in civilian employment. All requests must be fully justified and forwarded to Director, Naval Criminal Investigative Service (NCIS), Code 27D, Building 111, Washington Navy Yard, 716 Sicard St., S.E., Washington, D.C. 20388-5380. Requests should fully identify the

subject and include the social security number, and the date and place of birth. The justification for the request will acknowledge that there is no connection to a clearance adjudication.

6-12 COMMAND RESPONSIBILITIES REGARDING PERSONNEL SECURITY INVESTIGATION REQUESTS

1. There are certain functions necessary to support an efficient PSI process that are performed by the requesting command prior to submission of a PSI request. The functions are as follows:

a. **Verification of Prior Investigation.** Determine if the required investigation already exists. If available check the DCII. (Guidelines for accessing the DCII are found in appendix E). If DCII access is not available for Navy and Marine Corps civilians, check in the Official Personnel Folder (OPF). For Navy military members check the service record and/or the Officer Distribution Control Report (ODCR), or Enlisted Distribution Verification Report (EDVR). For Marine Corps military members check the Marine Corps Total Force System (MCTFS). Finally, if unable to determine if a current investigation exists at the local command, contact the DON CAF. If the DON CAF confirms no investigative basis is present or if there has been a break in service greater than 24 months since the date of the individual's last investigation, submit a request for the required PSI.

b. **Local Records Check (LRC).** A local records check (LRC) consists of a review of available personnel, medical, legal, security, base/military police and other command records to determine if locally available disqualifying information exists. A review of local civilian law enforcement records, the National Crime Information Center (NCIC), and the servicing (NCIS) office is prohibited because the information gleaned from these sources may not, in fact, pertain to the individual which in turn may cause the command not to hire, resulting in the lack of due process rights.

c. **Validate Citizenship.** Commands are required to validate citizenship of individuals subjected to a PSI. (Remember only U.S. citizens are eligible for security clearance.) Procedures for validating citizenship are contained in appendix I.

d. **Verify Date and Place of Birth and Education.** When requesting an SSBI, commands will attempt to validate subject's date and place of birth and most recent or most significant claimed education. Date and place of birth may be validated through review of available personnel records. The subject may

provide a diploma or transcript to validate education. If verification is not accomplished, advise DSS in the "Remarks" section of the request form. Verification of date and place of birth and education are required elements of an SSBI and will be conducted by DSS if the request form indicates the requestor was unable to accomplish the verification.

e. Ensure the request is completed according to instruction and prepared using the EPSQ or current forms to preclude rejection by DSS.

2. Document your efforts to validate and verify the required information where appropriate.

3. **Catch 'Em In Conus.** The Catch 'Em in CONUS program was adopted by DSS to reduce completion times for SSBIs and PRs on subjects ordered to overseas assignments (to include Adak, Alaska) or extended deployment. DSS has established the "Catch 'Em in CONUS" Program, aimed at completing as much of an SSBI or PR as possible prior to the subject's departure. Commands will:

a. Identify individuals requiring SSBIs or PRs to support scheduled overseas PCS assignment or deployment with sufficient time for DSS to complete necessary local leads.

b. Submit the SSBI or PR to DSS. Annotate in the "Remarks" section of the DD 1879, "Catch Em in CONUS" and send the request package to the attention of "DSS, Operations Center, Baltimore, Team F."

c. Contact the local DSS office as soon as possible, no later than 90 days prior to the individual's departure, allowing DSS to accomplish the case opening and subject interview leads. The local DSS office will accept a copy of the request package; conduct the subject interview and the local leads.

4. **Pre-Nomination Interview.** Before a request for an SSBI for SCI access is submitted to DSS, the nominee must undergo a pre-nomination interview. Unfavorable information developed during the pre-nomination interview that is not fully explained in the applicable remarks sections of the SF 86, will be explained in a written report which identifies the interviewer and is attached to the DD 1879 requesting the SSBI (refer to reference (c)). Note: Individuals who are in or selected for command status (CO/XO) do not require a pre-nomination interview.

6-13 ELECTRONIC PERSONNEL SECURITY QUESTIONNAIRE

1. DSS requires all requestors to use the Electronic Personnel Security Questionnaire (EPSQ) when requesting a personnel security investigation from DSS. The EPSQ is a complete software package used to request all DSS investigations, designed to gather and validate personnel security information and send that information to DSS for investigation. It speeds the investigative process by ensuring questionnaire information is accurately and completely provided and delivering questionnaire information in a format that allows DSS to instantly open the investigation without processing delays.

2. The EPSQ software and customer instruction manuals are available free of charge if downloaded from the DSS Web site at: www.dis.mil.

3. Customers who cannot download the EPSQ from the Web site may request the EPSQ software on diskette at a cost from the Defense Technical Information Center (1-800-225-3842) at 8725 John J. Kingman Rd, Suite 0940 (Code BRR), Ft. Belvoir, VA 22060. The DSS Customer Service Center (1-800-542-0237) is available to answer questions and provide technical assistance on EPSQ matters.

4. The EPSQ information can be forwarded to DSS electronically, it can be copied on a 3-1/2" diskette and mailed to DSS "ATTN: EPSQ DISKETTE PROCESSING," or the questionnaire information may be printed and mailed to DSS in printout format. When electronically submitting an EPSQ, commands must separately mail the fingerprint cards to DSS when they are required.

5. Commands requesting investigations using the EPSQ are also required to forward the signed authority for release of information to DSS. EPSQ requests forwarded to DSS on diskettes must be accompanied by the signed release form. Users of EPSQ 2.x may scan and electronically transmit the signed release with the EPSQ. Signed release forms for all other electronically transmitted EPSQ's will be forwarded to:

DSS-OCB
P. O. Box 28989
Baltimore, MD 21240-8989

6-14 PREPARATION AND SUBMISSION OF INVESTIGATIVE REQUESTS

1. The US Investigative Service (USIS) is not equipped to use the EPSQ and requires submission of standard investigative

request forms. For investigative requests submitted to USIS, or when logistical or technical problems prohibit EPSQ submission to DSS, commands will use the following approved Standard Forms: Standard Form (SF) 86, Questionnaire for National Security Positions, SF 85P, Questionnaire for Public Trust Positions, SF 85, Questionnaire for Nonsensitive Positions and the SF 86A, Continuation Sheet for Questionnaires SF 86, SF 85P and SF 85 when additional space for documentation is required. Additionally, the DD Form 1879, DoD Request for Investigation and SF 87, OPM fingerprint card, DD 2280, Armed Forces Fingerprint Card and FD 258, Applicant Fingerprint Card are also used.

2. Requests for investigation using standard forms will be submitted as follows:

a. **ENTNAC** - required to support suitability determinations for military enlisted accessions. The PSI request package will be submitted to DSS using the SF 86 and one DD 2280.

b. **NAC** - required to support trustworthiness determinations, e.g., for child care providers, etc. The PSI request package will be submitted to DSS using the SF 85P and a FD 258, Applicant fingerprint card.

c. **NACI** - required to support suitability determinations for civilian employees assigned to non sensitive duties without access to classified information. The PSI request package will be submitted to USIS using the SF 86, the SF 87, a resume or equivalent and an OF 306, Declaration for Federal Employment.

d. **ANACI** - required for civilian employees in noncritical sensitive positions and those who will require access to Confidential and Secret classified information. The ANACI request will be submitted using the NACI request forms and procedures, indicating "ANACI - 09B", under item A "Type of Investigation."

e. **NACLC** - required to support suitability determinations on military officer accessions and Secret and Confidential security clearance determinations for military members. The PSI request package will be submitted to DSS using the SF 86 and FD 258.

f. **SPR and CPR** - required to support the continuous evaluation of civilian employees and military members with access to Secret and Confidential classified information and other programs requiring an SPR. The SPR request will be submitted to DSS using the SF 86.

g. **SSBI** - required to support security and suitability determinations for civilian employees and military members requiring access to Top Secret information and/or SCI, assignment to critical-sensitive positions and other identified programs. The SSBI request will be submitted to DSS using a DD 1879, SF 86 and two FD 258 fingerprint cards. (The DD 1879 is submitted instead of filling out Part 1, items A - P of the SF 86.)

h. **PR** - required to support the continuous evaluation of civilian employees and military members with access to Top Secret information and/or SCI and other identified programs requiring a PR. The PR request will be submitted to DSS using a DD 1879 and an SF 86. **Fingerprint cards are not required.**

i. **SII** - required to prove or disprove allegations concerning an individual on whom a PSI has been conducted. The SII request package will be submitted to the DON CAF using the DD 1879 and an SF 86 under cover of an OPNAV 5510/413. The DON CAF will coordinate the investigative effort with DSS and the command and take necessary follow-up action.

6-15 MAINTAINING QUESTIONNAIRE INFORMATION

1. A tickler copy of the above requests may be locally retained to enable future tracer actions. Additionally, commands may maintain copies of completed questionnaires as a service to personnel, to aid personnel with future reinvestigation questionnaire requirements. Commands must ensure appropriate protection of completed questionnaires and will ensure copies are destroyed when no longer required.

2. Requesting an individual to prepare a questionnaire using the EPSQ or paper form for PSI purposes constitutes solicitation of personal information which is protected by the Privacy Act of 1974. Commanding officers have a responsibility to ensure that the information provided by the individual receives the appropriate protection.

3. If an individual refuses to provide or permit access to relevant information for investigative purposes, after being advised of the effect of refusal, commands will terminate the PSI request process. The individual will not be eligible for access to classified information or assignment to sensitive duties unless the information is made available. If the individual is currently cleared for access to classified information and/or is performing sensitive duties, the matter will be referred to the DON CAF for action. Personnel indoctrinated for SCI access will be debriefed for cause (refer to reference (c)).

6-16 FOLLOW-UP ACTIONS ON INVESTIGATIVE REQUESTS

1. Rejection of Investigation Requests. When the investigation request is rejected by the investigative agency because the forms were not completed and the investigation is still required, commands must take corrective action **immediately** and resubmit the request. All forms being resubmitted and the tickler copy of the request form will be annotated with the resubmission date. If a military subject has been transferred, the rejected PSI request must be forwarded immediately to the gaining command for correction and resubmission.

2. Cancellation of Investigation Requests. When an investigation is in a pending status and the subject is released from active duty, discharged, resigns, or circumstances change that negate the need for the investigation, the command that requested the investigation will notify the DON CAF. The DON CAF will direct the investigative agency, as appropriate, to cancel the investigation.

3. ENTNAC Follow-up. An ENTNAC must be completed on each first-term enlistee. If a first-term enlistee is received without evidence that the ENTNAC has been requested or completed, the receiving command must ensure an ENTNAC is conducted by submitting the request to DSS using the EPSQ, if available, the SF 86 and a FD 258, fingerprint card. The following directions will be used to ensure completion of the paper form ENTNAC request:

a. On the SF 86, Part 1, place an "E" in Item "H" and type or write "Applicant" in Item "I."

b. On the FD 258, type the term "military enlistee" in place of the word "applicant".

c. If more than 24 months has lapsed since enlistment, follow the procedures for requesting a NAC.

4. Transfer of a Military Subject of Investigation. When a military member is transferred after an SSBI has been requested, the losing command will notify DSS by submitting a corrected copy of the DD 1879. The address and Unit Identification Code/Reporting Unit Code (UIC/RUC) of the gaining command and the effective date of transfer must be entered in item 18, "Remarks."

5. Tracer Action. When it appears that it is taking an inordinate amount of time to receive investigation results, a tracer may be submitted to the DON CAF using a copy of an OPNAV

5510/413, Personnel Security Action Request. The word "TRACER" will be boldly printed or stamped in large letters. Exhibit 6A provides an OPNAV 5510/413 form example. **Tracers for USMC military members may be made through the MCTFS.** To obtain the status of a DSS investigation, call DSS customer service at 1-888-282-7682 or DSN 850-7682. The following time-lines should be used to determine if tracer action is appropriate:

TYPE OF INVESTIGATIVE BASIS REQUESTED	MINIMUM TIME FOR TRACER
ENTNAC/NAC	90 days
NACI/ANACI	75 days
NACLC	180 days
PR	180 days
SSBI/SII	180 days

6. Follow-up requirements and tracer actions when interim clearances have been granted are described in paragraph 8-5.4.

6-17 PROCESSING COMPLETED REPORTS OF INVESTIGATION

1. All PSIs conducted for DON activities are forwarded to the DON CAF upon completion. The DON CAF will make a personnel security determination based on the requirements identified on the PSI request.

2. When the PSI contains information that indicates further investigation is necessary, adjudication of the PSI will be held in abeyance pending completion of the additional investigative leads. Interim clearance and access will not be granted in these situations.

3. The DON CAF will formally notify commands of the completion of the investigation and the DON CAF determination. Additionally, investigations and the DON CAF determinations will be reflected as appropriate on PCS orders, in the ODCR, EDVR, MCTFS or Defense Civilian Personnel Data System (DCPDS) and the DCII.

4. Investigations requested to support trustworthiness determinations and non-sensitive positions are not adjudicated by the DON CAF. These investigations are forwarded by the DON CAF to commands for the appropriate trustworthiness and suitability determination. Investigations requested for sensitive positions that uncover suitability issues are forwarded to the command for the appropriate suitability determination before the DON CAF security determination is possible. After the command

suitability determination is made, the investigative results must be returned to the DON CAF for a security determination.

6-18 SAFEGUARDING REPORTS OF INVESTIGATION

1. In recognition of the sensitivity of personnel security reports and records, particularly with regard to personal privacy, results of investigations must be handled with the highest degree of discretion. Any investigative material, favorable or unfavorable, must be handled, stored, and transmitted using the following safeguards:

a. Investigative reports will be made available only to those authorities who require access in the performance of their official duties for the purposes of determining eligibility for access to classified information and/or assignment to sensitive duties; acceptance or retention in the Armed Forces; appointment or retention in civilian employment; or for law enforcement and counterintelligence purposes.

b. PSIs will not be made available for or communicated to selecting officials. For any other uses, specific written approval must be obtained from ASD(C3I) via CNO (N09N2).

c. Reproduction of investigative reports is restricted to the minimum required for the performance of official duties. All copies of PSIs will be destroyed as soon as final action is taken.

d. Retention of copies of PSIs longer than 120 days after final action has been completed must be specifically approved, in writing, by the investigating agency.

e. Investigative reports will be stored in a vault, safe, or steel filing cabinet having at least a lockbar, an approved three-position dial-type combination padlock, or in a similarly protected container or area.

f. Reports of investigation may not be shown or released to the subject of the investigation without the specific approval of the investigating agency. **Under no circumstances will reports of investigation be placed in the subject's personnel record or any record to which the subject may have access.**

g. When being transmitted by mail, or carried by persons not authorized to receive these reports, reports of investigations must be sealed in double envelopes or covers. The inner

container will bear a notation that it is to be opened only by an official designated to receive reports of PSIs.

h. If the results of an investigation are received after the subject has been transferred within DON, the transferring command will forward the results to the gaining command, as appropriate.

2. Results of DSS investigations may not be released outside DoD without the specific approval of DSS.

EXHIBIT 6A

PERSONNEL SECURITY INVESTIGATIONS

	FORMS * REQUIRED	HOW MANY TO SEND	MAIL TO
SSBI	DD 1879 SF 86 FD 258	3 5 2	DEFENSE SECURITY SERVICE OPERATIONS CENTER BALTIMORE P.O. BOX 18585 BALTIMORE, MD 21240-8585
SSBI-PR	DD 1879 SF 86	3 5	DEFENSE SECURITY SERVICE OPERATIONS CENTER BALTIMORE P.O. BOX 18585 BALTIMORE, MD 21240-8585
SPR or CPR	SF 86	1	DEFENSE SECURITY SERVICE OPERATIONS CENTER BALTIMORE P.O. BOX 28989 BALTIMORE, MD 21240-8989
NAC or NACLC	SF 86 FD 258	1 1	DEFENSE SECURITY SERVICE NATIONAL AGENCY CHECK DIVISION OPERATIONS CENTER BALTIMORE P.O. BOX 28989 BALTIMORE, MD 21240-8989
ENTNAC	SF 86 DD 2280	1 1	DEFENSE SECURITY SERVICE NATIONAL AGENCY CHECK DIVISION OPERATIONS CENTER BALTIMORE P.O. BOX 28989 BALTIMORE, MD 21240-8989
NACI or ANACI	SF 86 SF 87	1 1	OFFICE OF PERSONNEL MANAGEMENT OFFICE OF FEDERAL INVESTIGATIONS P.O. BOX 618 BOYERS, PA 16018
FAD NAC or TNAC	SF 85P	1	DEFENSE SECURITY SERVICE NATIONAL AGENCY CHECK DIVISION OPERATIONS CENTER BALTIMORE P. O. BOX 28989 BALTIMORE, MD 21240-8989

* When using the EPSQ without electronic submission, the EPSQ data will be mailed to the address indicated above.

EXHIBIT 6B

REPORT SYMBOLS

Title	Report Symbol	Paragraph
Report of Adverse or Unfavorable Action	DD-OPNAV 5510-1	8-8, 8-9, 8-10, 9-3, 9-18, 10-5
Report of Sabotage, Espionage, or Deliberate Compromise	OPNAV 5510-6D	3-1, 3-2, 3-3, 3-4, 3-5, 3-6, 4-5, 4-11

EXHIBIT 6C

PROCUREMENT OF FORMS

The forms and stock numbers listed below are used to support the Personnel Security Program. These forms can be procured through the normal supply channels.

a. The following forms may be ordered from the Navy supply system:

DD 254	Contract Security Classification Specificiation (12-90) S/N 0102-LF-011-5800
DD 1879	DoD Request For Personnel Security Investigation (Rev. 9/95) S/N 0102-LF-020-1600
DD 2280	Armed Forces Fingerprint Card (Rev. 4-87) S/N 0102-LF-002-2801
OPNAV 5510/413	Personnel Security Action Request (Rev.1-94) S/N 0107-LF-017-1300
OPNAV 5511/14	Security Termination Statement (Rev. 7-78) S/N 0107-LF-055-1171
OPNAV 5520/20	Certificate of Personnel Security Investigation, Clearance and Access (Rev/ 11-79) S/N 0107-LF-055-2101
OPNAV 5521/27	Visit Request/Visitor Clearance Data (Rev. 9-92) S/N 0107-LF-015-1100
FD 258	Applicant Fingerprint Card S/N 0104-LF-400-8610

b. The following forms may be ordered from the General Services Administration:

SF 85	Questionnaire for Non-Sensitive Positions (Rev. 9/95) NSN 7540-00-634-4035
SF 85P	Questionnaire for Public Trust Positions (Rev. 9/95) NSN 7540-01-317-7372

SF 85P-S	Supplemental Questionnaire for Selected Positions (Rev. 9/95) NSN 7540-01-368-7778
SF 86	Questionnaire for National Security Positions (Rev. 9/95) NSN 7540-00-634-4036
SF 86A	Continuation Sheet for Questionnaires SF 86, SF 85P, and SF 85) (Rev. 9/95) NSN 7540-01-268-4828
SF 87	OPM Fingerprint Card (Rev. 4/84) NSN 7540-00-634-4037
SF 312	Classified Information Nondisclosure Agreement (Rev. 1/91) NSN 7540-01-280-5499

CHAPTER 7

PERSONNEL SECURITY DETERMINATIONS

7-1 BASIC POLICY

1. The standard which must be met for security clearance eligibility or assignment to sensitive duties is that, based on all available information, the individual's loyalty, reliability and trustworthiness are such that entrusting them with classified information or assigning the individual to sensitive duties is clearly consistent with the interests of national security.

2. A determination to grant security clearance eligibility, authorize access to classified information, or assign an individual to sensitive duties will be based on an investigation conducted in accordance with the requirements specified in chapter 6.

3. E.O. 10450 and E.O. 12968 establish the standards which provide the basis for personnel security determinations. These standards apply to all U.S. Government civilian and military personnel, consultants, contractors, and other individuals who require access to classified information or assignment to sensitive duties. Appendix F synopsizes these standards.

4. The adjudicative guidelines used for determinations of security clearance eligibility are the same guidelines applied when determining eligibility to occupy a sensitive position. A favorable determination of security clearance eligibility also provides a favorable determination of eligibility to occupy a sensitive position, and vice versa, whether or not the individual requires access to classified information to perform sensitive duties. A determination by the DON CAF that an individual is not eligible for assignment to sensitive duties will also result in the removal of security clearance eligibility. Conversely, a determination that an individual is not eligible for a security clearance will result in the denial of eligibility for assignment to a sensitive position.

5. In making determinations regarding an individual's loyalty, reliability and trustworthiness, all information, favorable and unfavorable, is considered and assessed for accuracy, completeness, relevance, importance and overall significance. The final determination is the result of an overall common sense "whole person" adjudication, reached by application of the guidelines in appendix G.

6. Unless there is a reasonable basis for doubting a person's loyalty to the Government of the United States, decisions regarding appointment or retention in civilian employment or acceptance or retention in the Navy and Marine Corps are governed by personnel policies not under the purview of this regulation.

7. No separation under other than honorable conditions will be taken with respect to any Navy or Marine military member, nor will any action be taken to effect the separation, dismissal, discharge, or other involuntary separation for cause of any DON civilian employee or any contractor/consultant employee under the personnel security cognizance of the DON, in any case where the individual has held access to Sensitive Compartmented Information (SCI) and/or Special Access Programs (SAPs) within 18 months prior to the proposed action, unless approval is first received from the program manager (i.e. the Director of Naval Intelligence (DNI) for SCI access or CNO (N89) for SAP's.

7-2 PERSONNEL SECURITY PROGRAM AUTHORITIES AND RESPONSIBILITIES

1. The authority to determine eligibility for access to classified information or assignment to sensitive duties is vested in the Secretary of the Navy. This authority and the responsibilities for personnel security program management are delegated as follows:

a. <u>The Chief of Naval Operations Special Assistant for Naval Investigative Matters and Security (N09N) will</u>:

(1) Issue DON Personnel Security Policy.

(2) Assign responsibilities for overall management of the personnel security program.

(3) Maintain the DON Personnel Security Appeals Board (PSAB) and appoint members to ensure due process is afforded in appeals of unfavorable personnel security determinations.

b. The President, PSAB will preside over the PSAB, a three member panel appointed by CNO (N09N) which reviews and decides appeals of unfavorable DON CAF determinations. The decision of the PSAB to sustain or reverse determinations made by the DON CAF is final and concludes the administrative appeal process.

c. <u>The Commandant of the Marine Corps will</u>:

(1) Upon notification of the DON CAF determination, take appropriate action to:

(a) Ensure the security information in the Marine Corps Total Force System (MCTFS) is both accurately updated from the DON CAF database and reported to commands.

(b) Ensure actions are initiated, as appropriate, following unfavorable personnel security determinations.

(c) Ensure appropriate documentation of security determinations are entered into the individual's master service record.

(2) Notify commands of clearance eligibility and/or investigative requirements associated with transfers to new assignments, as appropriate.

(3) Maintain continuous liaison with CNO (N09N2), the DON CAF, and the PSAB in all matters involving personnel security determinations on Marine Corps military members.

d. **The Chief of Naval Personnel will**:

(1) Upon notification of the DON CAF determination, take appropriate action to:

(a) Ensure the security information in the military personnel database is both accurately updated from the DON CAF database and reported to commands via the EDVR, and ODCR.

(b) Ensure appropriate actions are initiated following unfavorable personnel security determinations.

(c) Ensure appropriate documentation of security determinations is entered into the individual's master service record.

(2) Notify commands of clearance eligibility and/or investigative requirements associated with transfers to new assignments.

(3) Maintain continuous liaison with CNO (N09N2), the DON CAF, and the PSAB in all matters involving personnel security determinations on Navy military members.

e. **The Deputy Assistant Secretary of the Navy (Civilian Personnel/Equal Employment Opportunity) will**:

(1) Upon notification of the DON CAF determination, take appropriate action to:

(a) Ensure the security information in the Defense Civilian Personnel Data System (DCPDS) is both accurately updated from the DON CAF database and reported to commands.

(b) Ensure appropriate documentation of security determinations is entered into the individual's official personnel folder.

(2) Coordinate with CNO (N09N2) and provide guidance to support the requirements of this regulation regarding assignment of civilians to sensitive positions.

f. **The Director, Department of the Navy Central Adjudication Facility will**:

(1) Adjudicate information from personnel security investigations and other relevant information to determine eligibility for security clearance and SCI access, and/or assignment to sensitive duties and communicate the results of each adjudication to the requesting command.

(2) Validate and certify personnel security clearance eligibility for all DON personnel.

(3) Document personnel security determinations in the Navy Joint Adjudication and Clearance System (NJACS) and the Defense Clearance and Investigations Index (DCII).

(4) Issue a Letter of Intent (LOI) to deny or revoke security clearance eligibility, SCI access or assignment to sensitive duties to every individual for whom an unfavorable personnel security determination is being contemplated.

(5) Issue a Letter of Notification (LON) to every individual for whom an unfavorable personnel security determination has been made, advising the individual of his or her right to appeal the DON CAF determination.

(6) Record and retain rationale underlying each personnel security determination where the investigation or information upon which the determination was made included derogatory information.

(7) Respond to DON command queries regarding the status of personnel security investigations.

(8) Provide clearance certification on behalf of DON personnel to all other DoD and federal agencies when requested.

g. <u>Commanding Officers will</u>:

(1) Control access to classified information for all assigned personnel.

(2) Request PSIs on personnel assigned to the command as appropriate.

(3) Grant interim personnel security clearances as instructed in paragraph 8-5.

(4) Maintain a personnel security record on all assigned personnel, to include a record of security briefings, a record of clearance determinations and a record of access determinations.

(5) Certify the security clearance of assigned personnel to other activities, as instructed by paragraph 11-2.

(6) Administratively withdraw the access when the requirement for access to classified information no longer exists. Debrief the individual in accordance with chapter 4, and notify the DON CAF that clearance and access are no longer required.

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

(8) Continuously evaluate command personnel with regard to their eligibility for access to classified information applying the appendix F standards. Notify the DON CAF when potentially disqualifying information is developed. (The DON CAF will review the information and reevaluate the individual's clearance eligibility using the adjudicative guidelines, provided in appendix G.)

(9) Suspend an individual's access to classified information for cause when warranted, and notify the DON CAF within 10 days. All pertinent information will be forwarded to the DON CAF for a personnel security determination. Once the commanding officer suspends access and reports the information to the DON CAF, access may not be reinstated unless approved by the DON CAF.

(10) Coordinate unfavorable personnel security determination actions concerning personnel assigned to the command. Direct personnel to command assistance programs, as appropriate. Assist affected personnel by explaining the personnel security determination process, provide personnel the

command instructions provided with the LOI, LON, and PSAB notification letters.

(11) Deny access and/or restrict admittance to command areas as deemed appropriate when disqualifying information regarding an individual from another command is revealed. Ensure the individual's parent command, agency or facility is notified of your action, to include the basis for that action. For contractor employees, report disqualifying issues to the DSS Operating Center, Columbus (OCC) (paragraph 9W-13 applies).

7-3 ADJUDICATIVE OFFICIALS

1. In view of the significance that each adjudicative decision can have on a person's career, and to ensure the maximum degree of fairness and equity in these actions a **minimum level of review** is required for all personnel security determinations.

2. To fulfill responsibilities enumerated in paragraph 7-2g, the commanding officer will ensure the local review is conducted by the security manager (GS-11 or military officer).

3. The following applies to the DON CAF and describes the level of adjudicative expertise required to review the identified investigations:

a. SSBI/PR/SII

(1) Favorable Investigations. Completely favorable investigations will be reviewed and determined to be favorable by an adjudicative official in the civilian grade of GS-7/9 or military rank of O-3.

(2) Unfavorable Investigations. Investigations that are not completely favorable will undergo at least two levels of review by adjudicative officials, the second of which must be in the civilian grade of GS-11/12 or military rank of O-4. When an unfavorable personnel security action is contemplated, the LOI to deny or revoke must be approved and signed by an adjudicative official in the civilian grade of GS-13/14 or military rank of O-5. The final notification of an unfavorable personnel security determination or LON, must be approved and signed by an adjudicative official in the civilian grade of GS-14/15 or military rank of O-6.

b. SPR/NACI/NAC/ENTNAC/NACLC/ANACI

(1) Favorable Investigations. Completely favorable investigations will be reviewed and determined to be favorable by an adjudicative official in the civilian grade of GS-5/7 or military rank of O-2.

(2) Unfavorable. Investigations that are not completely favorable must be reviewed by an adjudicative official in the civilian grade of GS-7/9 or military rank of O-3. When an unfavorable personnel security action is contemplated, the LOI to deny/revoke must be signed by an adjudicative official in the civilian grade of GS-11/12 or military rank of O-4. The final notification of unfavorable personnel security determination or LON, must be signed by an adjudicative official in the civilian grade of GS-13 or military rank of O-5.

7-4 PERSONNEL SECURITY DETERMINATIONS

1. A personnel security determination is required when:

a. A personnel security investigation on a nominee for a security clearance or assignment to sensitive civilian duties has been completed;

b. Access to classified information or assignment to sensitive duties is necessary under interim conditions;

c. Questionable or unfavorable information becomes available about an individual in a sensitive position or a position requiring access to classified information;

d. The issues that prompted a previous unfavorable personnel security determination no longer exist and the individual is again being considered for clearance or assignment to sensitive duties.

2. The personnel security adjudicative process is an evaluation of investigative and other related information. It does not determine criminal guilt nor the general suitability for a given position. It assesses past behavior as a basis for predicting the individual's future trustworthiness and potential fitness for a position of responsibility which, if abused, could have unacceptable consequences to national security.

3. All information, favorable and unfavorable, must be considered and assessed to determine initial and continued eligibility for access to classified information or assignment to

sensitive duties. Each case must be weighed on its own merits. The adjudication criteria contained in appendix H is used by the DON CAF in evaluating information in available personnel security investigative files and from other sources, including personnel, medical, legal, law enforcement and security records.

4. Upon receipt of derogatory information at the local command, commanding officers will determine whether, on the basis of all the facts, to suspend or limit an individual's access to classified information, or reassign the individual to nonsensitive duties pending a final determination by the DON CAF. It is essential that all those directly involved in this evaluation process, including security officials, Human Resource Office (HRO) personnel, managers and supervisors, take an objective approach to ensure equity to the subject and the protection of national security.

7-5 TRUSTWORTHINESS DETERMINATIONS

1. As established by the Internal Security Act of 1950, the commanding officer's duty to protect the command against the action of untrustworthy persons is paramount. Normally, the investigative requirements prescribed herein will suffice to enable a determination regarding the trustworthiness of individuals whose duties require access to classified information or who otherwise are appointed to sensitive positions. However, there are certain duties or situations not requiring access to classified information or appointment to a sensitive position, which if performed by untrustworthy persons, could jeopardize the safety or security of people or property of the command or otherwise endanger the national security (including access to restricted areas or sensitive equipment). The commanding officer has the prerogative of requesting a trustworthiness NAC to address such duties or situations except that contractor employees are assessed using the Facility Access Determination (FAD) program discussed in paragraph 7-6.

2. Trustworthiness NACs will be requested using the SF 85P and will be forwarded to DSS for processing. The DON CAF will return the completed investigation to the requesting command for the trustworthiness determination.

3. The criteria provided in appendix G will be used by the requesting command to guide trustworthiness determinations. Trustworthiness determinations are the sole prerogative of the commanding officer. If the commanding officer determines, upon review of the investigation, that allowing a person to perform certain duties or to access certain areas, would pose an

unacceptable risk, that decision is final. No due process procedures are required.

7-6 FACILITY ACCESS DETERMINATION (FAD) PROGRAM

1. Contractor employees are not normally subjected to investigation unless access to classified information is required, in which case they are investigated and cleared under the National Industrial Security Program. Security clearances will not be granted to contractor employees for ease of movement within a restricted, controlled, or industrial area when their duties do not require direct access to classified information, or if they may only have inadvertent access to sensitive information, areas, or equipment.

2. Nonetheless, many DON commands interact with contractors in matters that involve access to sensitive unclassified information or areas critical to the operations of the command which do not satisfy the prerequisites for personnel security clearances but do, however, warrant a judgement of an employee's trustworthiness. To meet this need, the DON Facility Access Determination (FAD) program has been established to support commanding officers in their responsibility under the Internal Security Act of 1950 to protect persons and property under their command against the actions of untrustworthy persons.

3. Commands will include the FAD program requirements in the contract specifications when trustworthiness determinations will be required on the contractor employees.

4. The procedures for requesting and receiving the results of a FAD NAC mirror the procedures for requesting and receiving the results of a trustworthiness NAC. The command will obtain a completed SF 85P from the contractor employee. The completed questionnaire will be reviewed for completeness, accuracy and suitability issues prior to submission. If the contractor appears suitable after the questionnaire review, the request is forwarded to DSS to conduct the NAC. The completed NAC is sent back to the requesting command via the DON CAF. The command will review the NAC results and make a trustworthiness determination applying the adjudicative criteria outlined in appendix G.

5. Commands will provide written notification to the contractor, advising whether or not the contractor employee will be admitted to the command areas or be given access to unclassified but sensitive information. No further information is required. Requests for DSS investigative data protected under the Privacy Act should be referred to DSS.

7-7 UNFAVORABLE DETERMINATIONS PROCESS

1. When an unfavorable personnel security determination is being contemplated by the DON CAF, the DON CAF will issue to the individual concerned a LOI to revoke or deny security clearance eligibility, SCI access or sensitive position eligibility. The LOI advises the individual of the proposed action, the reasons therefor and the rebuttal process associated with the proposed action. The LOI will be sent via the individual's command, with a copy provided to CHNAVPERS (Pers 831) for Navy military members and to Headquarters Marine Corps (HQMC) for Marine Corps military members. When SCI access is involved, copies of the LOI's are sent to SSO Navy or COMNAVSECGRU, as appropriate.

2. The command will immediately present the LOI to the individual and assume a direct role in facilitating the process. The command will determine the individual's intent regarding a response to the LOI, and immediately complete and return the Acknowledgement of Receipt of the Letter of Intent accompanying the LOI, to the DON CAF indicating whether the individual intends to submit a response to the contemplated action and whether the command has granted an extension of time to submit the response. The LOI advises the individual that if they choose not to respond, or if the response is untimely, <u>they will forfeit their rights to appeal</u>.

3. Where mail service may prevent a timely return of the Acknowledgement of Receipt of the Letter of Intent, commands may provide the DON CAF a message or facsimile to acknowledge receipt of the LOI and to indicate the individual's intentions. Facsimile correspondence should be used whenever practicable throughout the process.

4. The command will review the information contained in the LOI to determine whether the individual's access to classified information should be suspended while the unfavorable determination process continues. Commands will ensure all suspension actions are accomplished as specified in paragraph 9-18.

5. The recipient of the LOI will have 15 calendar days from receipt of the LOI to prepare and submit a written response. No outside influence will be permitted to forfeit the individual's opportunity to reply.

6. The commanding officer has the authority to grant the recipient of the LOI up to 45 extension days (for a total of 60 days) for the preparation of a response, provided the DON CAF is

notified of the extension time granted. After 45 extension days, requests for extensions must be directed to the DON CAF with a valid justification.

a. Extensions may be appropriate to enable the individual to obtain a copy of the investigation or information upon which the DON CAF based its intended action, medical or mental evaluation, personal reference letters that will mitigate or rebut the disqualifying information, financial statements, legal counsel or documentation, documentation from rehabilitation institutes, or other related information to support the response.

b. Extensions are not authorized to enable the individual to demonstrate responsibility for an issue that the individual was previously aware of but took no steps to resolve before receiving the LOI. This includes requests for extension to resolve financial or legal matters or to seek treatment for mental, emotional or medical issues presented in the LOI. Extensions are also not authorized to enable mitigation by the passage of time or to otherwise create mitigation not already present.

7. The command must respond immediately after delivery of the LOI to the recipient by forwarding the completed Acknowledgement of Receipt of the Letter of Intent to the DON CAF. Absent command or individual notification of intentions, the DON CAF may issue a final determination after 60 calendar days from the date on the LOI based upon existing information. If expeditious mail service is not used and regular mail service is such as to prevent timely delivery of the individual's response, the command will advise the DON CAF by message or other expeditious means when the "Acknowledgement" is mailed.

8. The DON CAF will adjudicate the response to the LOI within 30 calendar days of receipt and either make a favorable determination and authorize eligibility or issue a LON of denial or revocation of security clearance, SCI access and/or sensitive position eligibility. If a favorable determination is made, individuals will be notified in writing, via their command. If an unfavorable determination is made by the DON CAF, the individual will be notified in writing, citing all factors which were successfully mitigated by the individual's response to the LOI and what unfavorable factors remain dictating denial or revocation. The LON will be sent via the command with a copy to BUPERS (Pers 831) or HQMC for military members and SSO Navy or COMNAVSECGRU, as appropriate, for SCI access issues.

9. The LON will inform the recipient of his/her appeal rights. Upon receipt of the LON, commands must ensure the individual no

longer occupies a sensitive position and has no further access to national security information, as the individual has been determined to no longer meet the requirements.

7-8 APPEALING UNFAVORABLE DETERMINATIONS

1. The Personnel Security Appeals Board (PSAB) is the ultimate appellate authority for unfavorable personnel security determinations made by the DON CAF. The PSAB structure and functioning is described in appendix H. If an individual chooses to appeal an unfavorable DON CAF determination, the appeal may be submitted either verbally or in writing as follows:

a. Individuals may request a personal appearance before an administrative judge (AJ) from the Defense Office of Hearings and Appeals (DOHA). This appearance is intended to provide the individual an opportunity to personally respond to the DON CAF LON and to submit supporting documentation to the AJ, who will make a recommendation to the PSAB. A transcript of the proceedings with any supplemental documentation will be forwarded with the DOHA recommendation and will serve as the individual's appeal to the PSAB.

b. Individuals may submit a written appeal directly to the PSAB via their command and forego the personal appearance. A written appeal should also include supporting documentation when appropriate.

2. Individuals may select either to personally present their appeal to the DOHA AJ or to submit a written appeal forwarded directly to the PSAB. Individuals may not choose both options. Having or not having a personal appearance will not bias the PSAB in making a fair determination.

3. **DOHA PERSONAL APPEARANCES**

a. Individuals desiring to present a personal appeal must request a DOHA hearing within 10 days of receipt of the LON.

b. DOHA will normally schedule the personal appearance to be accomplished within 30 days of receipt of the individual's request.

c. Individuals will be provided a notice designating time, date and place for the personal appearance. For individuals at duty stations within the contiguous 48 states, the personal appearance will be conducted at the individual's duty station or a nearby suitable location. For individuals assigned to duty

stations outside the contiguous 48 states, the site of the personal appearance will be determined by the Director, DOHA or designee at one of the following locations: (1) the individual's duty station; (2) a suitable location near the individual's duty station; or (3) at DOHA facilities located either in the Washington D.C. metropolitan area or the Los Angeles, California metropolitan area.

d. Travel costs for the individual presenting a personal appeal to DOHA will be the responsibility of the individual's command.

e. The individual may be represented by counsel or other personal representative at the individual's expense.

f. Requests for postponement of the personal appearance can be granted only for good cause as determined by the DOHA AJ.

g. Individuals who choose a personal appearance will not have the opportunity to present or cross-examine witnesses. Individuals who desire to present the view of others must do so in writing (e.g. letters of reference, letters from medical authorities, etc.). The appeal should address the disqualifying issues identified by the LON and should present any existing mitigation as defined in appendix G, to include pertinent supporting documentation.

h. The AJ will review the individual's case file, hear the individual's or counsel's or personal representative's presentation and review any documentation submitted by the individual. Then the AJ will develop a recommended determination which will be forwarded along with a transcript of the personal appeal to the PSAB within 30 days of the personal appearance.

i. The value of a command perspective on the PSAB deliberations cannot be overstated. Since appeals presented to DOHA do not have the benefit of a command endorsement, commands are strongly encouraged to submit a position paper directly to the PSAB. However, due to time constraints, the PSAB will only solicit a command position when the appeal contains substantial information that was not included in the individual's rebuttal to the LOI. In these cases the Executive Director, PSAB will contact the command to provide the new information. The command will have 10 days to evaluate the new information and respond to the PSAB.

4. **PSAB WRITTEN APPEAL SUBMISSIONS**

a. The individual has 30 days from receipt of the LON to submit a written appeal to the PSAB. The command may extend the time allowed for an additional 15 days for a total of 45 days. Requests for further extensions can only be approved by the Executive Director, PSAB.

b. The written appeal may be made by counsel or personal representative at the individual's expense.

c. Written appeals should address the disqualifying issues identified by the LON and should present any existing mitigation as defined in appendix G, to include pertinent supporting documentation.

d. Commands are strongly encouraged to provide a command perspective by submitting an endorsement to the individual's appeal.

5. **PSAB PROCEDURES**

a. The PSAB will review the DON CAF case file, the individual's appeal (to include DOHA recommendations and command submissions as provided) and any supporting documentation submitted by the individual. Personal appearances before the PSAB are prohibited.

b. The PSAB will meet on a monthly basis and within 5 days of the Board review will notify the individual, via the individual's command, of the PSAB determination.

c. The PSAB determination is final and concludes the administrative appeals process.

d. The DON CAF will be directed to grant or restore clearances, SCI access eligibility and/or sensitive position eligibility when the PSAB finds for the appellant. When the PSAB finds against the appellant, reconsideration is only possible, if at a later date (generally after 1 year from the date of the final DON CAF determination) the individual's command determines that a valid requirement for access to classified information exists and the issues which caused the unfavorable determination seem to have been mitigated either through the passage of time or other relevant positive developments.

7-9 UNFAVORABLE PERSONNEL SECURITY ACTIONS

1. An unfavorable personnel security determination will result in one or more of the following personnel security actions:

a. Denial or revocation of security clearance eligibility ;

b. Denial or revocation of a Special Access Authorization (including SCI access eligibility);

c. Non-appointment to or non-selection for sensitive assignment;

2. Military members or civilians will not be removed from employment or separated from the service using this regulation as authority if removal or separation can be effected under administrative (not security) regulations.

CHAPTER 8

CLEARANCE

8-1 BASIC POLICY

1. The Department of the Navy Central Adjudication Facility (DON CAF) is designated by the Secretary of the Navy as the single clearance granting authority for the Department of the Navy. The DON CAF issues final security clearances for civilian and military personnel at the request of DON commands and activities, upon affirmation that granting the clearance is clearly consistent with the interests of national security. Once issued, a security clearance remains valid provided the cleared individual continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months.

2. A security clearance is not a de facto authorization for an individual to access classified information. Authorization to access classified information is a separate command level determination dependent on whether an individual who has the requisite security clearance also has a need for access to classified information in the performance of official duties. Access to Sensitive Compartmented Information (SCI) is a separate issue addressed in chapter 9.

3. The DON CAF determines the security clearance for DON personnel using the appendix G adjudicative guidelines to assess the loyalty, reliability and trustworthiness issues documented in personnel security investigations. Security clearance is initially issued upon adjudication of the prerequisite security investigation, and is reestablished upon adjudication of subsequent investigation(s). Certification is provided to a command when a clearance is required to support local access determinations. **Security clearance will be established at the highest level supportable by the prerequisite security investigation.***

*** For the purpose of this regulation the terms "security clearance" and "security clearance eligibility" will be synonymous.**

8-2 RECIPROCAL ACCEPTANCE OF SECURITY CLEARANCES

1. A security clearance determination by an approved agency of the Federal Government will be mutually and reciprocally accepted throughout the Federal Government provided the following

conditions are met: (1) there is no break in continuous government service greater than 24 months; (2) the investigative basis is adequate for the clearance to be granted, and (3) no new derogatory information is identified. The security clearance will be verified by the cognizant CAF, without additional adjudication.

2. A denial or revocation of security clearance eligibility may also be reciprocally accepted by agencies of the Federal Government. However, if the denial or revocation determination was made more than 12 months prior and a new clearance eligibility determination is requested, the new request will be processed in accordance with the reconsideration procedures provided in chapter 10.

3. **Continuous service** for security clearance eligibility purposes is active duty military service (including attendance at the military academies); active status in the military reserve, National Guard, NROTC, active Individual Ready Reserves (IRR), etc.; civilian employment in the Federal Government; employment with a DoD contractor that involves a security clearance under the National Industrial Security Program (NISP) or, a combination of these. Continuous service is maintained with a change from one status to another as long as there is no break greater than 24 months. Retired status does not qualify as **continuous service**.

4. Security clearance eligibility established within DoD will be accepted by the Department of Energy (DOE) and Nuclear Regulatory Commission (NRC) as the basis for access to Restricted Data of the same or lower classification. DOE and NRC clearance determinations are accepted by DoD as follows:

DOE and NRC Clearances	DoD Clearance Eligibility
"L" (For NRC employees, consultant personnel, and for DOE contractor personnel only, access up to Secret except Restricted Data for which access to Confidential only is authorized.)	Secret
"Q"	Secret
"Q" (specifying Top Secret access)	Top Secret

5. Security clearances granted conditionally (and SCI access eligibility established as an exception) are not bound by the reciprocity requirements.

8-3 CLEARANCE PROHIBITIONS

1. Only United States citizens who are either members of the executive branch of the U.S. Government or employees of contractors under the National Industrial Security Program (NISP) are eligible for security clearance. Occasionally, it is necessary for the DON to authorize access for persons not meeting these requirements; paragraph 9-14 governs these situations.

2. When this regulation refers to U.S. citizens, it makes no distinction between those who are U.S. citizens by birth, those who are U.S. nationals, those who have derived U.S. citizenship or those who acquired it through naturalization. For the purpose of issuance of a security clearance, citizens of the Federated States of Micronesia (FSM) and the Republic of the Marshall Islands are considered U.S. citizens. Appendix I provides guidance on validating U.S. citizenship.

3. A security clearance will not be granted for:

a. Persons in nonsensitive civilian positions;

b. Persons (such as guards and emergency service personnel) who may only have inadvertent access to sensitive information or areas;

c. Persons (such as maintenance, food services, or cleaning personnel) who perform unclassified duties within a restricted or controlled area, or other area where classified information may be present, unless access to classified information or materials cannot be reasonably prevented;

d. Persons (such as vendors and other commercial sales or service personnel) who do not require access to classified information and whose access to classified information can be prevented by a cleared escort.

4. The Facility Access Determination (FAD) program is used for trustworthiness determinations for contractor personnel when no access to classified information is required (paragraph 7-6 applies).

5. Elected members of Congress are not processed for security clearance eligibility. They may be granted access to classified information as required for the performance of their duties. Procedures for visits by elected members of Congress requiring access to classified information are provided in paragraph 11-4. Members of congressional staffs may be processed for security

clearance eligibility, as necessary, through the Security Division, Washington Headquarters Services, Department of Defense in accordance with DoD Directive 5142.1, Assistant Secretary of Defense (Legislative Affairs), 2 Jul 82 (NOTAL).

6. State governors are not processed for security clearance eligibility. Commanding officers may grant access to specifically designated classified information to these individuals, on a "need to know" basis, when approved by CNO (N09N2). Staff personnel of the governor's office who require access to DON classified information are investigated and cleared by the DON CAF, as appropriate.

7. Members of the U.S. Supreme Court, the Federal judiciary and the Supreme Courts of the individual states are not processed for security clearance eligibility. They may be granted access to classified information to the extent necessary to adjudicate assigned cases. For SCI, access may be granted upon concurrence from COMNAVSECGRU or SSO Navy.

8-4 RECORDING DETERMINATIONS

1. The Navy Joint Adjudication and Clearance System (NJACS) is the official central repository for DON personnel security determination records and includes clearance, access and investigative data. NJACS data supports management of the DON personnel security program, central management of the reinvestigation program, budget management requirements and congressional reporting requirements.

2. The DON CAF is charged with maintaining the NJACS data. Every security clearance determination made at the DON CAF is recorded in the NJACS. Initial access determinations are recorded in the NJACS. Investigative data forwarded from the Defense Security Service (DSS) and the US Investigative Service (USIS) is included in the NJACS. NJACS personnel security data codes are found in exhibit 8A.

3. The DON CAF formally certifies security clearance determinations to requesting commands. The DON CAF's certification is generated using NJACS data and provides commands with the documentation required to support local access determinations and other local program management requirements. Because the DON CAF certification supports command access determinations, it must be maintained in the individual's local service record or official personnel file until the individual separates, the individual's security clearance is revoked or until the certification is replaced by a more current record. Copies of the DON CAF certification may additionally be

maintained in local security files. The Marine Corps Total Force System (MCTFS) will provide the security clearance certification for Marine Corps military members.

4. The personnel security record maintained in the NJACS database is processed through tape transfers into the DON personnel data systems to include the Officer Distribution Control Report (ODCR), Enlisted Distribution Verification Report (EDVR), Marine Corps Total Force System (MCTFS) and the Defense Civilian Personnel Data System (DCPDS). NJACS data is also reflected on transfer orders. These sources of NJACS data may be used temporarily to support local access determinations when the DON CAF security clearance certification is not found in the individual's service record or official personnel file, pending receipt of a replacement for the DON CAF certification record. In these cases, commands will submit an OPNAV 5510/413 to the DON CAF requesting a security clearance determination. The DON CAF will forward a replacement certification. Procedures for temporary access determinations are found in paragraph 9-7.

5. Additionally, information maintained in the NJACS is electronically entered into the Defense Clearance and Investigations Index (DCII) discussed in appendix E. Commands with DCII access may use DCII data records in lieu of the DON CAF certification records, as appropriate, to support local access determinations.

6. Once issued, the DON CAF security clearance certification remains valid provided the individual continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months. (A change in commands or duties is not a "break in service.")

7. Commands will keep local access records. Paragraph 9-5 addresses access recording requirements.

8-5 INTERIM SECURITY CLEARANCE

1. Commands may grant interim security clearance and access (except for SCI access) pending completion of full investigative requirements and pending establishment of a final security clearance by the DON CAF. Interim clearances are granted, by authority delegated by the Director, DON CAF to the commanding officer under the following conditions:

a. Interim Top Secret security clearance.

(1) The existence of a favorable investigation (e.g. ENTNAC, NAC, NACI, etc., (paragraph 6-2 applies);

(2) A favorable review of the completed personnel security questionnaire (PSQ);

(3) The submission of the SSBI request to DSS; and

(4) A favorable review of local records, as defined in paragraph 6-12.

b. Interim Secret or Confidential security clearance.

(1) A favorable review of investigative request questionnaire;

(2) The submission of an appropriate investigative request to the investigative agency (paragraph 6-14 applies); and

(3) A favorable review of local records (paragraph 6-12 applies).

2. Commands will record interim security clearance actions using OPNAV 5510/413, Personnel Security Action Request, Part III under item 15. Item 22 of OPNAV 5510/413 will reflect the date and type of investigation requested. The interim clearance will be granted by signature of the commanding officer or designee who has been the subject of a favorably completed Single Scope Background Investigation (SSBI). The OPNAV 5510/413 will NOT be forwarded to the DON CAF at this time, but will be held until follow-up action is necessary.

3. It is important to ensure that the request for investigation submitted to support a required final security clearance reaches its destination, especially when interim clearances are granted. Commands that do not use the EPSQ to submit requests electronically, are strongly encouraged to use registered or certified mail for these specific requests so that receipt may be confirmed.

4. If a receipt confirming final clearance is not received within 180 days of submission of the request for investigation, a copy of the OPNAV 5510/413 recording the interim clearance will be boldly marked "TRACER" in item 22 and will be forwarded to the DON CAF. The DON CAF will respond to these tracers within 30 days.

5. The interim clearance may not be continued in excess of 1 year without a current confirmation from the DON CAF that the investigation contains no disqualifying information.

6. When the command receives a Letter of Intent (LOI) from the DON CAF to deny an individual's security clearance, the commanding officer will withdraw any interim security clearances issued and associated access will be suspended. Procedures for suspending access are found in paragraph 9-18.

8-6 GRANTING A SECURITY CLEARANCE

1. The DON CAF is the sole DON security clearance granting authority. The DON CAF adjudicates investigations at the highest level supportable by the completed prerequisite investigation. Investigative requirements are outlined in chapter 6.

2. When it is determined that an individual will require access to classified information to perform assigned duties, commands will review the individual's service record or official personnel folder to ensure the individual has the necessary security clearance certification. (Commands with DCII access will search DCII data to determine clearance eligibility.)

a. When the individual does not have the appropriate security clearance certification, but local records indicate the appropriate investigation exists, the command will submit an OPNAV 5510/413 request to the DON CAF to obtain the required certification. (Commands with DCII access need not request the DON CAF certification, DCII data will suffice.)

b. When the individual has neither the required clearance nor the required investigation to support the security clearance determination, the command will submit the appropriate request for investigation. Upon completion, the investigation will go to the DON CAF where a clearance determination will be made and the requesting command will be subsequently notified. Interim security clearance procedures may be employed as necessary.

8-7 UNIQUE SECURITY CLEARANCE REQUIREMENTS

1. Commanding Officer Clearance. Every commanding officer must have a favorably adjudicated SSBI and the security clearance equivalent to the highest level of classified information maintained at the command. The incumbent commanding officer will review the records of the prospective commanding officer to ensure that the individual has the necessary investigation and security clearance certification to assume command. In the

absence of an incumbent commanding officer, the next senior in the chain of command will ensure the records are reviewed. When the prospective commanding officer does not have the appropriate security clearance certification or SSBI, the incumbent commanding officer will ensure the necessary requests for certification and/or investigation are submitted.

2. Cryptographic Duties. Commands cannot grant interim security clearances for cryptographic duties. Clearance eligibility must be established by the DON CAF before access is allowed to U.S. cryptographic information.

3. Reserve Personnel. Navy and Marine Corps reserve personnel in an "active status" are considered to have continuous service and may be granted access as necessary and supportable by the DON CAF security clearance certification.

4. Individual Ready Reserves (IRR). IRR members will have security clearance established by the DON CAF as necessary. All due process procedures will be afforded IRR members nominated for security clearance.

5. Rating/Military Operations Specialty (MOS) Requirements. To maintain mobility and operational readiness, the Chief of Naval Personnel (Pers-831) or Headquarters Marine Corps (HQMC) may require individuals in specified ratings/MOS to have security clearance (eligibility) established by the DON CAF to support subsequent assignments.

a. Commands will use the continuous evaluation process to maintain security clearance (eligibility) for these specified ratings/MOS. PR's are not required unless the conditions outlined in paragraph 6-2.2g also exist.

b. Commands will forward potentially disqualifying information to the DON CAF for determination of continued eligibility for security clearance.

6. Personnel Assigned to Other Federal Agencies. The DON CAF will establish and provide certification of security clearance eligibility for DON employees assigned to other Federal agencies.

7. Access by Consultants to Government Contracting Activities (GCA). A consultant who is hired by a GCA and will only require access to classified information at a GCA activity or in connection with authorized visits, is not processed for a security clearance under the National Industrial Security Program (NISP). The consultant is considered an employee of the GCA for

security clearance and access purposes and will be adjudicated for security clearance by the DON CAF.

8-8 CLEARANCE UNDER THE NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP)

1. Employees of contractors granted facility clearances under the NISP may be granted personnel security clearances when there is a bona fide requirement to access classified information in connection with performance on a classified contract or R&D program. Contractor personnel security investigations are conducted by the Defense Security Service (DSS). Investigative results are then adjudicated and security clearance eligibility is established by the DSS Operations Center, Columbus (OCC).

2. Employees of contractors requiring access to SCI under the auspices of the DON are adjudicated for SCI access eligibility by the DON CAF. After adjudication of SCI access eligibility, the investigative results are forwarded to DSS OCC for security clearance adjudication.

3. Under previous policy, contractors were delegated authority to act on behalf of the DoD to grant Confidential clearances to qualified employees. This authority has been rescinded. However, contractor-granted clearances granted to employees prior to January 1991, unaffected by upgrade or administrative withdrawal, remain valid.

4. Interim Secret or Confidential security clearances may be granted to eligible contractor employees by DSS OCC on a temporary basis pending completion of a personnel security investigation.

5. Interim Top Secret security clearances may be granted to eligible contractor employees by DSS OCC based on approval from the contracting command or activity. DON contracting commands in receipt of requests for interim Top Secret security clearances will validate the contract, contractor need to know, and necessity for the interim clearance.

6. Commanding officers will report to DSS OCC any adverse or questionable information which comes to their attention concerning a cleared contractor employee assigned to a worksite under their control. An information copy of the report will also be forwarded to the Defense Security Service (DSS) Operating Location Office (OPLOC) identified on the Contract Security Classification Specificiation (DD Form 254). A sample DD 254 is at exhibit 11A of reference (d). Commanding officers will also

report adverse or questionable information to the DON CAF when a cleared contractor employee has SCI access.

7. Commands are responsible to ensure all clearance and access requirements are identified on the DD 254. Command procedures for granting or denying access to classified information for cleared contractor employees is provided in paragraph 9-13.

8-9 CLEARANCE WITHDRAWAL OR ADJUSTMENT

1. Access terminates when an individual transfers from one command another, however clearance requirements will normally remain unaffected. Commands will debrief individuals who are transferring to another command as outlined in paragraph 4-11, but execution of a Security Termination Statement is not required. Commands will make every effort to ensure that the DON CAF security clearance certification is properly filed in the service record or official personnel folder and forwarded to the individuals new command to support future access determinations.

2. Commanding officers will administratively withdraw an individual's access when a permanent change in official duties (i.e. rating/MOS changes) eliminates the requirement for security clearance and access. The command will debrief the individual as outlined in paragraph 4-11 and file the executed Security Termination Statement in the individual's service record or official personnel folder. Commands will notify the DON CAF using OPNAV 5510/413 that the individual no longer requires clearance and access. The DON CAF will adjust the NJACS accordingly.

3. When the level of access required for an individual's official duties changes, the command will adjust the authorized access accordingly, providing the new requirement does not exceed the level allowed by the security clearance. If the level of access required will exceed the level allowed by the DON CAF security clearance certification, commands will ensure the appropriate investigation is requested and may consider granting an interim clearance as specified in paragraph 8-5.

4. The administrative withdrawal or downgrading of a security clearance or access is not authorized when prompted by developed derogatory information. The command may suspend the individual's access for cause, and must report the suspension and/or the derogatory information to the DON CAF. The suspension of access must be accomplished in accordance with paragraph 9-18. (When SCI access is at issue the command Special Security Officer will coordinate the action.) A command report of suspension of access for cause will automatically result in the DON CAF suspension of

the individual's security clearance. The clearance certification will be removed from local records. Once security clearance is suspended by the DON CAF, the individual may not be granted access unless the security clearance is reestablished by the DON CAF.

5. **Transfer in Status (TIS).** The TIS is a process in which an individual may be transferred from one DoD component, command, or activity, to another DoD component, command, or activity in an SCI indoctrinated status. TIS should not be confused with the process of individual's transferring with established security clearance eligibility. Chapter 9 provides additional guidance concerning SCI access.

8-10 DENIAL OR REVOCATION OF SECURITY CLEARANCE

1. Once the DON CAF grants a security clearance it remains valid provided the individual continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months. Commands are ultimately responsible for ensuring that the DON CAF is apprised accordingly when either of these invalidating factors exist. To satisfy this requirement, commands must implement a proactive continuous evaluation program as described in chapter 10. Whenever information develops that suggests an individual may no longer be in compliance with personnel security standards, commands must report the issues to the DON CAF for adjudication using the OPNAV 5510/413. For SCI, refer to reference (c) for reporting requirements. Exhibit 10A provides a checklist of issues that must be reported.

2. In the event the DON CAF determines that an individual either fails or ceases to meet the standards for security clearance, the DON CAF will begin the unfavorable determination process explained in paragraph 7-8. If the DON CAF determines a reported issue does not impact on the individuals security clearance, a security clearance certification will be reissued to the command.

3. Once the DON CAF makes a final unfavorable decision concerning an individual's security clearance, the command must remove all accesses authorized, and debrief the individual in accordance with paragraph 4-11, including execution of a Security Termination Statement even if the individual is appealing the unfavorable DON CAF decision. All previous clearance certificates will be removed and replaced with the LON.

8-11 REESTABLISHING A SECURITY CLEARANCE AFTER A DENIAL OR REVOCATION

1. Following an unfavorable security determination by the DON CAF, a request to reestablish security clearance may be submitted after a reasonable passage of time, normally a minimum of 12 months, when it is determined that the individual appears to meet the appendix G guidelines. Commands shall provide documentation to support the reestablishment of security clearance eligibility.

2. Interim security clearance and/or access and assignment to sensitive civilian positions is <u>not</u> authorized for individuals who have received an unfavorable determination until the DON CAF reestablishes the security clearance. If a favorable determination is not possible, the DON CAF will provide the commanding officer with specific reasons for upholding their previous decision.

EXHIBIT 8A

PERSONNEL SECURITY DATA CODES

1. SECURITY INVESTIGATIONS. Identifies the most recent Personnel Security Investigation (PSI) completed on an individual.

Code	PSI
1	Entrance National Agency Check (ENTNAC)
2	National Agency Check (NAC)
3	NAC plus Written Inquiries (NACI)
4	Background Investigation (BI)
5	Special Background Investigation (SBI)
6	NAC plus 10 years of service (obsolete)
7	NAC plus Special Investigative Inquiry (SII)
8	ENTNAC plus SII
9	Interview oriented BI (IBI)
A	Expanded NAC
B	Local Records Check (LRC) plus NACI requested
C	NACI requested
D	NAC or NACI plus BI or IBI requested
E	NAC plus SBI requested
F	BI/IBI (10-year scope)
G	Periodic Reinvestigation (PR) or BI/IBI
H	NAC plus partial SBI
I	Character Investigation (IRS)
J	PR
K	Limited BI (LBI) (OPM)
L	Minimum BI (MBI) (OPM)
M	SBI plus current NAC
N	NACI plus current NAC
O	SII
P	IBI/BI plus current NAC
Q	MBI plus current NAC
R	LBI plus current NAC
S	SBI plus current BI/IBI
T	IBI/BI requested
U	Other
V	SBI requested
W	LRC
X	MBI expanded
Y	LBI expanded
Z	NACI plus SII
#	Secret PR

2. SECURITY ELIGIBILITY. Provides the level of clearance eligibility established for an individual.

A	No clearance - Investigation reopened
B	SCI denied - Ineligible for clearance
C	Confidential
D	Clearance denied
E	Interim Confidential
F	SCI revoked - Ineligible for clearance
G	Secret - SCI denied
H	Secret - SCI revoked
I	Clearance pending - Investigation reopened
J	No Clearance Required - File created
K	Eligible for SCI w/waiver
L	Restricted to nonsensitive duties/not eligible
M	Top Secret only - SCI revoked
N	Top Secret only - SCI denied
O	Interim Secret
P	Interim Top Secret
Q	No clearance/access required - favorable investigation
R	Clearance revoked
S	Secret
T	Top Secret
U	Interim SCI
V	Top Secret - SCI Eligible
W	Top Secret - SCI requires adjudication
X	Action pending
Y	Pending adjudication/access suspended
Z	Adjudication action incomplete due to loss of jurisdiction
1	LAA Confidential
2	LAA Secret
3	Pending reply to Letter of Intent (LOI)/Statement of Reason (SOR)
4	Clearance administratively withdrawn
5	Position of trust (no clearance determination)
6	SCI denied (no clearance determination)
7	SCI revoked (no clearance determination)

3. CURRENT CLEARANCE/ACCESS AUTHORIZED. Indicates the actual clearance/access currently held by the individual.

A	No clearance - Investigation reopened
B	SCI denied - Ineligible for clearance
C	Confidential
D	Clearance denied
E	Interim Confidential
F	SCI revoked - Ineligible for clearance

G	Secret - SCI denied
H	Secret - SCI revoked
I	Clearance pending - Investigation reopened
J	No Clearance Required - File created
K	Eligible for SCI w/waiver
L	Restricted to nonsensitive duties/not eligible for sensitive duties
M	Top Secret only - SCI revoked
N	Top Secret only - SCI denied
O	Interim Secret
P	Interim Top Secret
Q	No clearance/access required - favorable investigation
R	Clearance revoked
S	Secret
T	Top Secret
U	Interim SCI
V	DCID 1/14 Eligible
W	Top Secret - SCI requires adjudication
X	Action pending
Y	Pending adjudication/access suspended
Z	Adjudicative action incomplete due to loss of jurisdiction
1	LAA Confidential
2	LAA Secret
3	Pending reply to Letter of Intent (LOI)/Statement of Reasons (SOR)
4	Clearance administratively withdrawn
5	Position of trust (no clearance required)
6	SCI denied (no clearance determination)
7	SCI revoked (no clearance determination)

CHAPTER 9

ACCESS TO CLASSIFIED INFORMATION

9-1 BASIC POLICY

1. Access to classified information may be granted only if allowing access will promote the furtherance of the DON mission while preserving the interests of national security.

2. Access to classified information will be limited to the minimum number of individuals necessary to accomplish the mission and will be based on need to know. Additionally, the level of access authorized will be limited to the minimum level required to perform assigned duties. No one has a right to have access to classified information solely because of rank, position, or security clearance.

3. A Classified Information Nondisclosure Agreement (SF 312) must be executed by all persons prior to gaining initial access to classified information.

4. Commanding officers will ensure that personnel under their jurisdiction are briefed in accordance with paragraph 4-5 before granting access to classified information.

5. Under U.S. Navy regulations, the responsibility of the commanding officer for his or her command is absolute. Thus commanding officers have ultimate authority over who may have access to classified information under their control.

6. The Director, Naval Intelligence (DNI) is the Department of the Navy's Senior Official of the Intelligence Community (SOIC) with authority over all DON Sensitive Compartmented Information (SCI) access eligibility matters (paragraph 9-3 applies).

9-2 GRANTING ACCESS TO CLASSIFIED INFORMATION

1. Commanding officers may grant access to classified information to any individual who has an official need to know, an established security clearance, and about whom there is no known unadjudicated disqualifying information.

2. The determination to grant access to classified information is subject to the following restrictions:

a. DoD contractor employees holding only contractor-issued (company) Confidential clearances will not be granted access to Restricted Data, cryptographic information, SCI, or NATO information. (Other restrictions on DoD contractors for access to foreign intelligence information are described in SECNAVINST 5510.31B, Policy and Procedures for Control of Foreign Disclosure in the Department of the Navy, Dec 92).

b. For individuals who have not been determined to be eligible for security clearance, access authorization may be allowed in certian specific circumstances as discussed in this chapter. These unique access authorizations are specifically limited and are not reciprocally acceptable determinations.

c. The degree of access by representatives of foreign governments, including Personnel Exchange Program (PEP) personnel, will be scrupulously limited to that allowed by the Foreign Disclosure Authorization issued by the Navy International Programs Office (Navy IPO) on a case-by-case basis.

d. SCI access program management is governed by reference (c). Paragraph 9-3 synopsizes some of the procedures.

3. Granting access is a command responsibility. Access is formally terminated when it is no longer required in the performance of duties and/or when the individual's security clearance is denied or revoked.

4. Limiting access is the responsibility of each individual possessing classified information. Before allowing others access to classified information, individuals possessing classified information must determine that allowing access is justified based on the others' security clearance eligibility and need to know.

9-3 SENSITIVE COMPARTMENTED INFORMATION (SCI) ACCESS

1. The Navy Department Supplement to DoD Directive S5105.21. M-1, 18 Mar 97, reference (c), contains the policies and procedures for access to and dissemination of SCI.

2. The Director, DON CAF is delegated responsibility for granting, denying, revoking and verifying SCI access eligibility for DON personnel. In addition, the Director, DON CAF is also delegated the authority to adjudicate DON contractor personnel requiring SCI access eligibility under the NISP and reference (c).

3. The following procedures apply to initial requests for the DON CAF SCI access eligibility determinations:

a. A valid requirement or certification of need to know in accordance with reference (c) must be established prior to requesting the DON CAF adjudication for SCI access eligibility.

b. If it is determined that SCI access is required and a valid (e.g. conducted within the past 5 years) Single Scope Background Investigation (SSBI) does not exist, an SSBI request (or SSBI-PR if an outdated SSBI exists) will be sent to the Defense Security Service as directed by chapter 6.

c. If SCI access is required and a valid SSBI exists, the commanding officer will request an SCI access eligibility determination from the DON CAF using the OPNAV 5510/413. The collateral Top Secret security clearance required will be requested in conjunction with the SCI access eligibility request. The OPNAV 5510/413 must accurately reflect the citizenship of immediate family members because reference (c) imposes additional procedural requirements for individuals with foreign national immediate family members.

d. Upon favorable adjudication of the completed SSBI, the DON CAF will forward a final clearance/SCI access eligibility certification letter or message to the requesting command. Upon receipt of the DON CAF certification, the command will ensure the special security officer (SSO) receives a copy of the message or letter to indoctrinate the individual as directed by reference (c) and the security manager will maintain a command record of the clearance and access granted.

4. Requests for exceptions to DCID 1/14 for SCI access eligibility will be prepared as directed by reference (c) and forwarded to the DON CAF using the OPNAV 5510/413.

5. Commanding officers are responsible for establishing and administering a program for continuous evaluation of all personnel with security clearance and/or SCI access eligibility. Key to an active continuous evaluation program is security education. Continuous evaluation requirements are outlined in chapter 10 and in reference (c).

a. Information that could potentially affect an individual's eligibility for SCI access must be reported to the DON CAF with SSO Navy or COMNAVSECGRU as an information addressee in accordance with the procedures outlined in reference (c). The DON CAF will either reaffirm the SCI access eligibility or will

use the unfavorable determinations process outlined in chapter 7. Commanding officers may suspend, or debrief for cause from SCI access in accordance with reference (c). However, the decision to deny or revoke SCI access eligibility resides solely with the DON CAF. Additionally, the authority to review final appeals of unfavorable SCI access eligibility determinations is delegated to the Personnel Security Appeals Board (PSAB). The decision of the PSAB regarding SCI access is final.

b. A Periodic Reinvestigation (PR) is required every 5 years for individuals with SCI access. ALL PR requests will be forwarded to DSS, with the results returned to the DON CAF for adjudication. Chapter 6 describes the PR request process.

6. When an individual who is indoctrinated for SCI access is transferred-in-status to a new command, the gaining command SSO will forward an OPNAV 5510/413 to the DON CAF for revalidation of the SCI access eligibility. The losing command SSO will forward an SSO555 TIS message to the gaining command. Upon receipt of the SSO555 TIS message, the individual may be granted SCI access. Absent potentially disqualifying information, the DON CAF will send an SCI eligibility certification to the gaining command. If the certification is not received by the gaining command within 90 days of the individual's arrival, commands are required to send a copy of the originally submitted OPNAV 5510/413 boldly marked "TRACER." An OPNAV 5510/413 is not submitted on individuals in intelligence MOS/rating/designators (161X/163X, 644X, 654X, 744X, 754X, IS, CT, 26XX).

7. The commanding officer may debrief an individual from SCI access for administrative reasons as provided in reference (c).

8. The DON CAF will record the SCI access eligibility determination in the NJACS which feeds the DON personnel data displayed in the ODCR, EDVR, MCTFS, and DCPDS. SCI access eligibility is also reflected in the DCII.

9-4 CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (SF 312)

1. A Classified Information Nondisclosure Agreement (NdA), Standard Form (SF) 312 must be executed by all personnel as a condition of access to classified information. An example of the SF 312 is provided at exhibit 9A.

2. The current SF 312, (Rev. 1-91), supersedes the SF 189, Classified Information Nondisclosure Agreement, the SF 189-A, Classified Information Nondisclosure Agreement (Industrial/

Commercial/Non-Government) and the SF 312 (Rev. 9-88), Classified Information Nondisclosure Agreement. Previously executed SF 312's remain valid and will be understood to be amended to reflect the language of the most current SF 312 (Rev. 1-91). All NdAs previously executed will be interpreted and enforced in a manner fully consistent with the interpretation and enforcement of the SF 312 (Rev. 1-91).

3. DON military and civilian employees who have not previously signed an SF 312 must sign a current SF 312 before being given initial access to classified information.

4. When the DON CAF initially grants a security clearance, commands will be directed to ensure an SF 312 is appropriately executed as a condition of allowing access to classified information. Personnel who have signed other nondisclosure agreements for specific access (such as Form 1847-1, Sensitive Compartmented Information (SCI) Non-Disclosure Agreement), must also execute the SF 312.

5. If an individual refuses to sign an SF 312, the command will deny the individual access to classified information and report the refusal to the DON CAF.

6. Commanding officers will ensure personnel are provided an explanation of the purpose of the SF 312 and have the opportunity to read the Sections of Titles 18 and 50 of the United States Code and other references identified on the SF 312.

7. The execution of the SF 312 must be witnessed and the witnessing official must sign and date the NdA at the time it is executed. The witnessing official can be any member of the command. The SF 312 must be accepted on behalf of the United States. The accepting official can be the commanding officer, the executive officer, the security manager, or an individual designated in writing by the commanding officer to accept the SF 312 on behalf of the U.S. Government.

8. Executed SF 312's will be maintained for 70 years from date of signature.

9. The completed forms will be forwarded to the following addresses for retention:

Navy military members:
Commander, Naval Personnel Command
Pers 313C1
5720 Integrity Drive
Millington, TN 38055-8310

Marine Corps military members:
Commandant of the Marine Corps
Headquarters US Marine Corps (MMSB-22)
MCCDC
2008 Elliot Road
Suite 114
Quantico VA 22134-5030

All DON civilian personnel:
To their Official Personnel Folder (OPF)

10. A SF 312 need only be executed once by an individual when initially granted access. Administrative withdrawal of clearance, after execution of an SF-312, and subsequent granting of clearance and access will neither require validation of the previous execution nor reexecution of another SF-312.

11. For reservists who will have initial access to classified information, the reserve unit security manager will ensure execution of the SF 312 prior to forwarding the member to the duty assignment in which access to classified information will be required.

12. Contractor, licensee, and grantee employees or other non-government personnel will sign the SF 312 before being authorized access to classified information.

9-5 RECORDING ACCESS

1. The DON CAF maintains the official record of security clearances granted and initial access determinations in the Navy Joint Adjudication and Clearance System (NJACS).

2. Command security managers are responsible for maintaining a record of all access granted to include temporary accesses, special accesses or other program accesses formally granted (e.g. SIOP-ESI, NATO Secret, CNWDI, COSMIC, SCI, and PRP). Requirements for SSO's maintaining records of SCI access determinations are provided in reference (c).

3. Each command may use a method of record maintenance suited to the command's capabilities, such as a computerized database, a

log book, or a form OPNAV 5520/20, and must maintain the record for 2 years after access terminates.

4. The command access record must include the following data elements: Name, SSN, citizenship verification, date and level of access authorized, the basis for the access determination and the name and title, rank or grade of the individual authorizing the access. Interim security clearance and certain temporary accesses are recorded on the OPNAV 5510/413.

5. The command security manager is responsible for notifying an individual's supervisor when access has been granted with specific instructions regarding restrictions or limitations.

9-6 ONE-TIME ACCESS

1. An urgent operational or contractual emergency may arise for cleared personnel to have one-time or short duration access to classified information at a level higher than that for which they are eligible. Processing the individual to upgrade the security clearance would not be practical in these situations, therefore an individual may be granted access at one security classification level above that for which eligible, subject to the following terms and conditions:

a. One-time access may only be granted by a flag or general officer, a general courts-martial convening authority or equivalent Senior Executive Service member, after coordination with command security officials.

b. The individual granted one-time access must be a U.S. citizen, have a current DoD security clearance and have been continuously employed by DoD or a cleared DoD contractor for the preceding 24-month period. One-time access is not authorized for part-time or temporary employees.

c. Review of locally available records has been conducted as provided in paragraph 6-12.1b and revealed no disqualifying information.

d. Whenever possible, access will be limited to a single instance or, at most, a few occasions. If repeated access is required, the proper personnel security investigation will be initiated.

e. Approval for access will automatically expire no later than 30 calendar days from the date access commenced. If the need for access is expected to continue for a period in excess of

30 days, written approval is required from CNO (N09N2). If the need for access is expected to extend beyond 90 days, the command must initiate a request for the appropriate security clearance. Access will not be extended, in any case, beyond 90 days from the date access commenced unless a supporting personnel security investigation is requested.

f. Access at the higher level will only be allowed under the supervision of a properly cleared individual. The supervisor will be responsible for recording (paragraph 9-5.3 applies) the higher level information actually revealed with the dates access was afforded and for retrieving the accessed material daily.

g. Access will be limited to information under the control of the official who authorized the one time access. Access at the next higher level will not be authorized for COMSEC, SCI, NATO or foreign government information.

2. This provision will be used sparingly and repeated use of one time access within any 12 month period on behalf of the same individual is prohibited.

3. A record must be maintained for each individual authorized one time access. The record will include the following information:

a. The name and social security number of the individual;

b. The level of access authorized;

c. Justification for the access, to include an explanation of the compelling reason to grant the higher level access and, specifically, how the DON mission would be furthered;

d. An unclassified description of the specific information to which access was afforded and the duration of the access, to include the dates access was afforded;

e. A listing of the locally available records reviewed and a statement that no significant adverse information concerning the individual is known to exist;

f. The approving authority's signature; and

g. Copies of any pertinent briefings/debriefings given to the individual.

9-7 TEMPORARY ACCESS

1. Temporary access may be granted to DON personnel who have been otherwise determined to be eligible for a security clearance by the DON CAF but do not currently require a security clearance/access to perform assigned duties. Before authorizing temporary access, the commanding officer must determine that it is to the DON's benefit to allow disclosure to an individual who does not require access in the usual performance of duties. Situations in which temporary access may be justified include attendance at a classified meeting or training session, participation in advancement examinations, or annual reserve active duty for training or scheduled inactive duty training.

2. If temporary access is justified, the commanding officer may, after favorable review of locally available records in accordance with paragraph 6-12.1b, allow access or certify to another command the individual's security clearance eligibility as a basis to allow access to classified information.

3. This provision must be monitored very carefully and exercised only when access is needed for a limited time. Authority to allow temporary access does not include access to SCI or NATO information. Procedures for temporary access to SCI are provided by reference (c).

9-8 TEMPORARY ACCESS PENDING RECEIPT OF CLEARANCE CERTIFICATION

1. Temporary access may be granted when a member reports to a command and there are clear indications that a security clearance which could support the access required was previously granted but the DCII is unavailable for local validation and there is no DON CAF security clearance certification in the individual service record or official personnel folder. (This does not apply to SCI access.)

2. Commands will submit an OPNAV 5510/413 to the DON CAF indicating the level of security clearance required (item 20) and will maintain a tickler copy for tracer purposes. If the command does not receive a current DON CAF security clearance certification within 90 days, commands are required to send a copy of the originally submitted OPNAV 5510/413 boldly marked "TRACER." If after 180 days the command does not receive the required certification, temporary access must be terminated. Commands will initiate direct dialog with the DON CAF to determine if a request for security clearance is required.

3. Commands with DCII access may use DCII data in lieu of requesting the DON CAF clearance certification. Instructions for establishing command DCII access can be found in appendix E.

9-9 ACCESS BY RETIRED PERSONNEL

1. Retired personnel, including those on the temporary disability retirement lists, are not entitled to have access to classified information merely by virtue of their present or former status. When a commanding officer decides to grant a retiree access to classified information in the furtherance of the DON mission, a request for access authorization may be submitted to CNO (N09N2) using the guidance contained in paragraph 9-14.

2. As an exception to the above, an active duty flag/general officer may waive the investigative requirement and grant a retired flag/general officer temporary access to classified information when he/she determines that there are compelling reasons in furtherance of a DON program or mission to grant such access. The period of access will not exceed 180 days.

a. Access may only be granted to information classified at a level commensurate with the security clearance held by the retired flag/general officer at the time of his/her retirement. Granting access to SCI is prohibited.

b. Access will be granted only under the condition that the retiree not remove classified materials from the confines of a government installation or other area approved for storage of classified information.

c. The flag/general officer granting the access will inform CNO (N09N2) of this event by a written report within 5 days. The report must identify the retired flag/general officer involved, the classification of the information to which access was authorized, the DON program or mission which is served by granting access, and the period of time for which access is authorized.

d. If continued access beyond the 180 day limit is necessary, the report to CNO (N09N2) must be accompanied by requests for the appropriate personnel security investigation and clearance.

9-10 ACCESS BY RESERVE PERSONNEL

1. Reserve personnel in an "active status" may be granted access as necessary, provided they hold the appropriate security clearance eligibility. For Active Duty for Training (less than 30 days) and inactive duty training (drills) procedures described in paragraph 9-7 may apply.

2. Reserve personnel may also be given access to Communications Security (COMSEC) information necessary to maintain proficiency in their specialty. Details are provided in CMS-1A, Cryptographic Security Policy and Procedures Manual (U), 25 Feb 98, (NOTAL).

9-11 ACCESS BY INVESTIGATIVE AND LAW ENFORCEMENT AGENTS

1. Investigative agents of other departments or agencies may obtain access to classified information only through coordination with the Naval Criminal Investigative Service (NCIS).

2. The NCIS will be responsible for verifying the need to know of the other agency requiring the access.

9-12 ACCESS AUTHORIZATION FOR ATTORNEYS

1. Requests for access authorization for attorneys representing DON personnel will be submitted to CNO (N09N2) via the Office of General Counsel (OGC) or Navy Judge Advocate General (NJAG). Requests will provide a brief summary of the facts of the case and a description of the specific classified information the defense will require to adequately represent his or her client.

2. OGC or NJAG will evaluate the request and certify that access to the specified classified information is necessary and will ensure the attorney requiring the access has completed the necessary investigative request forms. OGC or NJAG will then forward the certified access request, including the investigative request forms, to CNO (N09N2).

3. CNO (N09N2) will submit the request for investigation to DSS and will authorize access, as appropriate. Prior to access the attorney will be required to sign the Classified Information Nondisclosure Agreement (SF 312).

9-13 CONTRACTOR ACCESS

1. Commanding officers may grant access to classified information to contractor employees based on the contractors need to know and the contracting facilities certification of security clearance provided on the classified visit request. Paragraph 11-2 provides visit request details.

2. Commanding officers may, at any time, deny contractor employees access to areas and information under command control for cause. However, suspension or revocation of contractor security clearances can only be effected through DSS. Action taken by a command to deny a contractor access to the command areas and information will be reported to the DSS OCC with an information copy to the DSS Operating Location Office (OPLOC). If SCI access is an issue, a report will also be forwarded to the DON CAF.

3. Contractor-granted Confidential clearances in effect under previous policy are not valid for access to Restricted Data, Formerly Restricted Data, cryptographic or intelligence information, Naval Nuclear Propulsion Information, NATO information (except Restricted), SCI, and foreign government information.

9-14 ACCESS AUTHORIZATION FOR PERSONS OUTSIDE OF THE EXECUTIVE BRANCH OF THE GOVERNMENT

1. When an individual who is outside the Executive Branch of the Government has a special expertise that can be employed in furtherance of the DON mission, a commanding officer may request CNO (N09N2) to authorize the access, provided the individual is a U.S. citizen and the information being accessed is information for which the commanding officer is responsible.

2. A request for access will be submitted to CNO (N09N2) for access authorization. The request will include:

a. Full name, date and place of birth and social security number;

b. The justification of the need for the access;

c. The expertise the individual will bring to the program or project;

d. The classification level, nature and scope of the information to be accessed;

e. The period of time for which access is required (not to exceed 24 months); and

f. The appropriate personnel security investigative request package, completed in accordance with paragraph 6-14.

3. CNO (N09N2) will not accept a request from the individual desiring access. Requests for access must be sponsored by an active duty commanding officer who will assume responsibility for ensuring the individual is briefed on their responsibilities for protecting classified information, that a Classified Information Nondisclosure Agreement (SF 312) is executed and proper safeguards and limitations are employed.

4. Access will be granted only as specifically authorized by CNO (N09N2) and limited to the classified information identified in the request. The access authorization will be effective for the period of time necessary, but no longer than 2 years.

5. Physical custody of classified material will not be allowed.

6. The command will record the access authorized and maintain the record for 2 years after expiration of the access.

9-15 HISTORICAL RESEARCHERS

Individuals outside the Executive Branch of the Government engaged in private historical research projects may be granted access to classified information if steps are taken to ensure that classified information or material is not published or otherwise compromised.

a. Requests for access authorization for DON classified information will be processed by the Director of Naval History, Office of the Chief of Naval Operations (CNO (N09BH)) or the Director of Marine Corps History and Museums (CMC (Code HD)), Headquarters Marine Corps. Upon receipt of a request for access authorization, CNO (N09BH) or CMC (Code HD) will seek to declassify the requested records. If declassification cannot be accomplished, CNO (N09BH) or CMC (Code HD) will:

(1) Prepare a recommendation as to whether the access requested would promote the interests of national security in view of the intended use of the material;

(2) Obtain from the researcher completed investigative request forms appropriate for the level of access required and submit them with the recommendation requesting access

authorization to CNO (N09N2), who will advise whether access is authorized for the specific project;

(3) Have the researcher sign a Classified Information Nondisclosure Agreement (SF 312);

(4) Limit the researcher's access to specific categories of information over which the DON has classification jurisdiction or to information within the scope of the historical research if the researcher has obtained written consent from the DoD or non-DoD departments or agencies with classification jurisdiction over that information;

(5) Retain custody of the classified information at a DON installation or activity or authorize access to documents in the custody of the National Archives and Records Administration; and

(6) Obtain the researcher's written agreement to safeguard the information and to submit any notes and manuscript for review by the DON or other DoD or non-DoD department or agency with classification jurisdiction, to determine that they do not contain classified information.

b. Access authorizations are valid for not more than 2 years from the date of issuance. Extensions may be granted by CNO (N09N2), if recommended by CNO (N09BH) or CMC (Code HD).

9-16 LIMITED ACCESS AUTHORIZATION (LAA) FOR NON-U.S. CITIZENS

1. Although non-U.S. citizens are not eligible for security clearance, access to classified information may be justified for compelling reasons in furtherance of the DON mission, including special expertise. An LAA may be justified in those rare circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed and for which a cleared or clearable U.S. citizen is not available. When justified, an LAA may be considered under the following conditions:

a. Access is limited to classified information relating to a specific program or project;

b. Appropriate foreign disclosure authority determines that access to classified information is not inconsistent with releasability to the individual's country of origin;

c. Physical custody of classified material will not be authorized;

d. LAAs will not be granted to personnel who perform routine administrative or other support duties;

e. Individuals granted LAAs will not be designated couriers or escorts for classified material unless they are accompanied by an appropriately cleared U.S. person;

f. Personnel granted LAA's will not be permitted uncontrolled access to areas where classified information is stored or discussed. Classified information will be maintained in a location that will be under the continuous control and supervision of an appropriately cleared U.S. citizen.

g. An SSBI is completed favorably; where full investigative coverage cannot be completed, a counterintelligence-scope polygraph examination will be required; and

h. A foreign national employee must agree to a counterintelligence-scope polygraph examination before being granted access. Failure to agree will terminate the processing of the LAA request.

2. When an LAA appears to be justified, a commanding officer may submit a request to CNO (N09N2) with the following information:

a. The identity of the individual for whom LAA is requested, including name, date and place of birth, current citizenship, social security number (if held),

b. Status as an immigrant alien or foreign national; if an immigrant alien, the date and port of entry and alien registration number;

c. Date and type of most recent personnel security investigation. If an SSBI has not been completed within the past 5 years, the completed personnel security investigative request package must be enclosed;

d. Level of access required;

e. The position requiring access and the nature and identity of the specific program material (delineated as precisely as possible) for which access is requested;

f. The compelling reasons for the request including an explanation of the special skills or special expertise the individual possesses and the rationale for not employing a cleared or clearable U.S. citizen;

g. An explanation as to how the command plans to control and limit the individual's access;

h. A statement that the candidate has agreed to undergo a counterintelligence scope polygraph examination when needed; and

i. The period of time for which access is required. (Will not exceed 5 years).

3. CNO (N09N2) will review the LAA request to determine if the justification provided meets the program requirements. If the justification is not adequate the LAA request will be promptly returned to the requester. If the justification is adequate, CNO (N09N2) will forward the SSBI request to DSS, however, the decision to authorize limited access can not be made until favorable adjudication of the completed SSBI.

4. CNO (N09N2) will coordinate foreign disclosure decisions with the Navy International Programs Office (Navy IPO), when required.

5. Individuals with LAAs will be placed under the general supervision of appropriately cleared persons. Supervisors will be made fully aware of the limits to access imposed and that physical custody of classified information by the individual is not authorized. A Classified Information Nondisclosure Agreement (SF 312) must be executed by the individual prior to granting access to classified information.

6. Individuals who have been granted a LAA will not be allowed to have access to any classified information other than that specifically authorized.

7. If an individual granted a LAA is transferred to another position, the LAA previously granted is rescinded. The individual will be debriefed in accordance with chapter 4. If the individual is transferring to other duties requiring a LAA, the command will request a new access authorization. If the individual's SSBI is less than 5 years old in these cases a new PSI is not required.

8. Periodic Reinvestigations (PR) are required every 5 years for individuals with LAA. Because LAA's are not authorized for more than 5 years, a new request for LAA must accompany a request for PR. CNO (N09N2) will review the justification and promptly notify the command to either continue the LAA until favorable completion of the PR by DSS or to discontinue access authorized based on lack of justification.

9. Non-U.S. citizens will not be authorized access to foreign intelligence information without approval of the originating agency, or to COMSEC keying materials, Top Secret, Naval Nuclear Propulsion Information (NNPI), TEMPEST, cryptographic or NATO information.

9-17 TERMINATING, WITHDRAWING OR ADJUSTING ACCESS

1. Access terminates when an individual transfers from a command. Commands will debrief individuals as outlined in paragraph 4-11, but execution of a Security Termination Statement is not required because affiliation continues and clearance requirements will normally remain.

2. Commanding officers will administratively withdraw an individual's access when a permanent change in official duties (i.e. rating/MOS changes) eliminates the requirement for security clearance and access and when the individual separates from the DON or otherwise terminates employment. The individual will be debriefed as outlined in paragraph 4-11 and will execute a Security Termination Statement which will be filed in the individual's service record or official personnel folder. Commands will forward an OPNAV 5510/413 to notify the DON CAF that the individual no longer requires clearance and access. The DON CAF will adjust the NJACS accordingly.

3. When the level of access required for an individual's official duties change, the command will adjust the authorized access accordingly, provided the new requirement does not exceed the level allowed by the security clearance. If the level of access required will exceed the level allowed by the DON CAF security clearance certification, the command will request the appropriate investigation and may consider interim clearance procedures as specified in paragraph 8-5.

9-18 SUSPENSION OF ACCESS FOR CAUSE

1. When questionable or unfavorable information becomes available concerning an individual who has been granted access, the commanding officer may suspend access. Suspension of access for cause may only be used as a temporary measure which must be resolved through either a favorable or unfavorable security determination by the DON CAF prior to the individual being transferred to a different command. The commanding officer will forward all pertinent information concerning the individual to the DON CAF for a final security clearance determination.

a. Suspension of access is required when a civilian employee with security clearance is incarcerated (to include Work Release Programs) as the result of a conviction for a criminal offense or is absent without leave for a period exceeding 30 days.

b. Suspension of access is required when a military member with a security clearance is discharged under Other Than Honorable conditions, is incarcerated (to include Work Release Programs) as the result of a conviction for a criminal offense or violations of the Uniform Code of Military Justice (UCMJ), is declared a deserter or is absent without leave for a period exceeding 30 days.

2. Whenever a determination is made to suspend access to classified information the following is required:

a. The individual concerned must be notified of the determination **in writing** by the commanding officer or designee, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security;

b. Commands and activities must report all suspensions to the DON CAF no later than 10 working days from the date of the suspension action using the OPNAV 5510/413 detailing the questionable or unfavorable information which caused the suspension action;

c. Take steps to ensure that the individual's clearance certification is removed from records, the individual's name is removed from all local access rosters and visit certifications, and all coworkers are notified of the suspension;

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

e. Place a copy of the OPNAV 5510/413 report to the DON CAF of the suspension of access in the individual's local service record or OPF, pending a final determination by the DON CAF;

f. Cancel or hold in abeyance any Permanent Change of Station (PCS) orders. Notify CHNAVPERS (Pers-831) for Navy military members or HQ USMC (INTC) for Marine military members under orders.

3. A determination to suspend SCI access for cause will include suspension of the security clearance.

9-19 ACCESS TO AND DISSEMINATION OF RESTRICTED DATA (RD) INCLUDING CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)

1. Restricted Data (RD), as defined in the Atomic Energy Act of 1954 as amended is data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but does not include data declassified or removed from the RD category under Section 142 of the Act.

a. Access to RD within and between DON commands, National Aeronautics and Space Administration (NASA) and contractor activities will be governed by the same procedures and criteria as govern access to other classified information:

(1) Access is required in the performance of official duties.

(2) The individual has a valid security clearance commensurate with the level of access required for the information.

b. Requests for access to RD not under the control of DoD and/or NASA will be made in accordance with DoD 5210.2, Access to and Dissemination of Restricted Data, 12 Jan 78 (NOTAL).

(1) Requests by members of DON commands requiring access to RD at DOE facilities will be made utilizing the DOE Visit Request Form 5631.20, Request for Visit Approval or Access Approval and will be submitted via the appropriate DON certifying official identified by DoD 5210.2 to the Associate Deputy Assistant Secretary for Technical and Environment Support (DP-45), Department of Energy, Washington, DC 20585.

(2) Conflicts in guidance and inquiries relating to access and/or the protection of RD by DON personnel and commands should be referred to CNO (N09N2) for resolution.

c. The following procedures apply to DON commands and personnel who disseminate RD under their control:

(1) Within and between DoD commands, to include DoD contractors, dissemination of RD information will be governed by the same procedures and criteria as govern the dissemination of other classified information; verify the identity of the prospective recipient, verify the prospective recipient's

clearance and insure the prospective recipient has an official "need to know."

(2) Dissemination of RD and Formerly Restricted Data (FRD) outside DoD will be made in accordance with DoD 5210.2.

2. Critical Nuclear Weapon Design Information (CNWDI) is Top Secret Restricted Data or Secret Restricted Data that reveals 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, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive material by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test or replace.

a. Access to and dissemination of CNWDI is of particular concern due to the extreme sensitivity of this type of information. Access must be limited to the absolute minimum number of persons needed to meet mission requirements. To meet this objective, the following special requirements and procedures for controlling CNWDI information have been established:

(1) Final TOP SECRET or SECRET Clearance (as appropriate)

(2) Except in rare instances only U.S. citizens will be granted access. When an immigrant alien possesses unique or very unusual talents and/or skills that are essential to the U.S. Government that are not possessed to a comparative degree by an available U.S. citizen, a request with justification to use such individual will be forwarded to CNO (N09N2) for approval.

(3) Requests by members of DON commands for access to CNWDI at DOE facilities will be made utilizing DOE Visit Request Form 5631.20 and must be submitted via an appropriate DON certifying official to the Associate Deputy Assistant Secretary for Technical and Environment Support (DP-45), Department of Energy, Washington, DC 20585. DoD 5210.2 contains a listing of DON officials authorized to certify access to CNWDI at DOE facilities. Recommendations for changes to the list of DON approved certifying officials will be submitted, with supporting justification to CNO (N09N2) for approval and inclusion in DoD 5210.2.

(4) Verification of "need to know". Certifying officials will not automatically approve requests for access to CNWDI, but will insist upon full justification and will reject any requests

that are not completely justified. Certifying officials have a special responsibility to insure that this "need to know" principle is strictly enforced.

(5) Personnel having a need for access to CNWDI will be briefed on its sensitivity. Briefings and access authorizations will be recorded in appropriate security records and maintained in a manner that facilitates verification. Similarly, personnel whose CNWDI access is terminated (reassignment, etc.) must be debriefed. Individual briefing/debriefing records will be maintained 2 years after access is terminated. Each DON command will establish their own procedures and format for briefing/debriefing.

b. For additional guidance refer to DoD 5210.2 or contact CNO (N09N2).

EXHIBIT 9A

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN _____ AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

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

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

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

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

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

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

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

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

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

(Continue on reverse.)

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)

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

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

SECURITY DEBRIEFING ACKNOWLEDGEMENT

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

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

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

STANDARD FORM 312 BACK (REV. 1-91)

CHAPTER 10

CONTINUOUS EVALUATION

10-1 POLICY

1. A personnel security determination requires an examination of a sufficient amount of information regarding an individual to determine whether the individual is an acceptable security risk. Obviously it is not possible to establish with certainty if an individual will remain eligible for access to classified information. In order to ensure that everyone who has access to classified information remains eligible for a clearance, continuous assessment and evaluation is required.

2. Commanding officers are responsible for establishing and administering a program for continuous evaluation. The continuous evaluation program will rely on all personnel within the command to report questionable or unfavorable information which may be relevant to a security clearance determination.

a. Individuals must be encouraged to report to their supervisor or appropriate security official and seek assistance for any incident or situation which could affect their continued eligibility for access to classified information. Individuals must be familiar with pertinent security regulations and must be aware of the standards of conduct required of individuals holding positions of trust. The ultimate responsibility for maintaining eligibility to access classified information rests with the individual. Reporting requirements for individuals with SCI access authorization are contained in reference (c).

b. Co-workers have an obligation to advise their supervisor or appropriate security official when they become aware of information with potential security clearance significance.

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

3. Keys to an active continuous evaluation program are security education and positive reinforcement of reporting requirements in the form of management support, confidentiality, and employee assistance referrals.

10-2 SECURITY EDUCATION

1. The ability of individuals to meet security responsibilities is proportional to the degree to which individuals understand what is required of them. Therefore, a key component of an effective continuous evaluation program is an effective security education program.

2. Personnel assigned to sensitive duties must receive indoctrination and orientation training on the national security implications of their duties and responsibilities. Along with understanding the prohibitions against improperly handling classified information, personnel must understand the continued trustworthiness expectations placed upon them. This is essential if individuals are to recognize and properly respond to security issues.

3. Annual refresher briefings are required. Commands must advise personnel of pertinent security requirements for the protection of classified information and must inform personnel of security standards required of all individuals who access classified information. The briefing must emphasize the avenues open to personnel should they require assistance or otherwise have difficulty or concerns in maintaining trustworthiness standards.

10-3 EMPLOYEES EDUCATION AND ASSISTANCE PROGRAM

1. E.O. 12968 requires each commanding officer to establish a program for employees with access to classified information to educate employees about personnel security responsibilities and to inform employees about guidance and assistance programs available. The education and assistance program will address issues that may affect employee eligibility for access to classified information and will include assistance for employees who have questions or concerns about financial matters, mental health or substance abuse.

2. Commands should act to identify individuals with personal issues at an early stage and to guide them to programs designed to counsel and assist them. The goal is to assist individuals while there is still a reasonable chance of precluding a long term employment or security clearance-related issue.

10-4 PERFORMANCE EVALUATION SYSTEM

1. For original classification authorities, security managers, security specialists and all other personnel whose duties

significantly involve the creating, handling, or management of classified information, E.O. 12958 requires that the performance contract or rating system will include the management of classified information as a critical element or item to be evaluated. Guidelines on performance management are published by the Office of the Deputy Assistant Secretary of the Navy (Civilian Personnel/Equal Employment Opportunity (ODASN(CP/EEO)) Code DP2). Questions may be addressed to the local Human Resources Office or the ODASN(CP/EEO) Code DP2.

2. In addition, supervisors will comment on the continued security clearance eligibility of subordinates who have access to classified information in conjunction with regularly scheduled performance appraisals. To accomplish this requirement, commands may instruct supervisors to comment in writing, or to include statements on performance appraisal forms and/or separate correspondence addressed to security officials. The intent is to encourage supervisors to refer security concerns as soon as they become apparent, to provide supervisors an opportunity to annually assess their employees regarding continued eligibility to access classified information and for supervisors to be accountable for fulfilling their responsibilities.

10-5 COMMAND REPORTS OF LOCALLY DEVELOPED UNFAVORABLE INFORMATION

1. When questionable or unfavorable information, as identified in appendix F, becomes available concerning an individual who has been granted access to classified information or assigned to sensitive duties, commands will report that information to the DON CAF. Commands should report all information which meets the appendix F standards <u>without attempting to apply or consider any mitigating factors that may exist</u>.

2. When reporting unfavorable information commands are encouraged to use the check list at exhibit 10A, to ensure that the DON CAF has sufficient information upon which to base a determination.

3. If the command determines that the developed information is significant enough to require a suspension of the individual's access for cause, the suspension action must be accomplished in accordance with paragraph 9-18. When suspending SCI access, reference (c) procedures apply.

4. A command report of suspension of access for cause will automatically result in the suspension of the individual's clearance eligibility by the DON CAF.

a. 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 reindoctrination into SCI access) until clearance eligibility has been reestablished by the DON CAF.

b. In cases where unfavorable information was developed at the local command and subsequently resolved by local investigation or inquiry, commands must notify the DON CAF of the inquiry results. Commands may request temporary clearance eligibility. Temporary clearance eligibility authorization will be at the DON CAF discretion and is usually only possible if the local inquiry developed the necessary mitigation and there are no other unresolved security issues or other related pending inquiries or investigation.

5. The DON CAF will evaluate and adjudicate all reported information and promptly notify commands of the determination regarding the individual's continued eligibility for access to classified information (including SCI access) and/or assignment to sensitive duties.

6. If the reported information is incomplete or too limited to allow adjudication, the DON CAF may either request additional information from the command or they may request that the command forward the necessary investigative request forms to the DON CAF in order to open an investigation at DSS to resolve outstanding or missing information.

EXHIBIT 10A

CONTINUOUS EVALUATION CHECK SHEET

1. When questionable or unfavorable information becomes available concerning an individual who has been granted access to classified information or assigned to sensitive duties, commands will report that information to the Department of the Navy Central Adjudication Facility (DON CAF). Commands should report all information without attempting to apply or consider any mitigating factors that may exist. The command report must be as detailed as possible and should include all available information pertinent to the DON CAF determination.

2. The following security issues must be reported to the DON CAF:

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

b. Foreign influence concerns/close personal association with foreign nationals or nations.

c. Foreign citizenship (dual citizenship) or foreign monetary interests.

d. Sexual behavior that is criminal or reflects a lack of judgement or discretion.

e. Conduct involving questionable judgement, untrustworthiness, unreliability or unwillingness to comply with rules and regulations, or unwillingness to cooperate with security clearance processing.

f. Unexplained affluence or excessive indebtedness.

g. Alcohol abuse.

h. Illegal or improper drug use/involvement.

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

j. Criminal conduct.

k. Noncompliance with security requirements.

l. Engagement in outside activities which could cause a conflict of interest.

m. Misuse of Information Technology Systems.

3. When reporting information to the DON CAF, the following pertinent details about each issue should be provided (when the detailed information is available to the command):

a. Nature and seriousness of the conduct.

b. Circumstances surrounding the conduct.

c. The frequency and recency of the conduct.

d. The age of the individual at the time of the conduct.

e. The voluntariness or willfulness of the individual's participation or conduct.

f. The knowledge the individual had of the consequences involved.

g. The motivation for the conduct.

h. How the command became aware of the information.

i. Actions the individual has taken to correct the issue, including medical treatment, counseling, lifestyle changes, or other corrective actions.

j. The stability of the individual's lifestyle or work performance, including demonstrative examples.

k. Cooperation on the part of the individual in following medical or legal advice or assisting in command efforts to resolve the security issue.

4. The DON CAF will evaluate the command report. If the DON CAF review determines that the reported information is not adequate or detailed enough to make a determination, the DON CAF will direct the reporting command to have the individual in question complete an investigative request package. DSS will conduct a Special Investigative Inquiry (SII) to gather the necessary information. The SII results will be returned to the DON CAF for adjudication.

CHAPTER 11

VISITOR ACCESS TO CLASSIFIED INFORMATION

11-1 BASIC POLICY

1. For security purposes, the term visitor applies as follows:

a. A visitor on board a ship or aircraft is a person who is not a member of the ship's company or not a member of a staff using the ship as a flagship.

b. A visitor to a shore establishment is any person who is not attached to or employed by the command or staff using that station as headquarters.

c. A person on temporary additional duty is considered a visitor. Personnel on temporary duty orders, reservists on active duty for training, or those personnel assigned on a quota to a school for a course of instruction, may also be considered as visitors.

d. A cleared DoD contractor assigned to a DON command who occupies or shares government spaces for a predetermined period.

2. Commanding officers will establish procedures to ensure that only visitors with an appropriate level of personnel security clearance and need to know are granted access to classified information.

3. The movement of all visitors will be controlled to ensure that access to classified information is consistent with the purpose of the visit. If an escort is required for the visitor, either a cleared and properly trained military or civilian member or a contractor assigned to the command being visited may be used.

4. As a matter of convenience and courtesy, flag officers, general officers and their civilian equivalents are not required to sign visitor records or display identification badges when being escorted as visitors. Identification of these senior visitors by escorts will normally be sufficient. The escort should be present at all times to avoid challenge and embarrassment and to ensure that necessary security controls are met. If the visitor is not being escorted, all normal security procedures will apply.

5. At the discretion of the commanding officer, the general public may be permitted to visit on an unclassified basis only, (i.e. no classified areas, equipment or information may be divulged to the general public). A written statement of command safeguards will be prepared and implemented to address the possibility of the presence of foreign agents among the visitors.

11-2 CLASSIFIED VISIT REQUEST PROCEDURES

1. When a visit to a DON command will involve access to classified information, the commanding officer of the visitor or an appropriate official of the contractor facility, organization or foreign country which the visitor represents will submit a visit request either by naval message or command/company letterhead to the organization to be visited.

2. Visit requests must include the following information for military and civilian personnel:

a. Full name, rank, rate, or grade (when applicable), date and place of birth, social security number, title, position, UIC/RUC (when applicable), and citizenship of the proposed visitor.

b. Name of employer or sponsor, if other than the originator of the request.

c. Name and address of the activity to be visited, if other than the addressee of the visit request.

d. Date and duration of the proposed visit.

e. Purpose of visit in detail, including estimated degree of access required. When the visit involves access to information, such as NATO or SIOP-ESI, for which specific authorization is required, the command visited will confirm that the visitor has been briefed and authorized such access.

f. Security clearance status of visitor (basis of clearance is not required).

3. The following information is required on a contractor's visit request:

a. Contractor's name, date and place of birth, and citizenship of the proposed visitor;

b. Certification of the proposed visitor's personnel security clearance and any special access authorizations required for the visit;

c. Name of person(s) being visited;

d. Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit;

e. Date or period during which the request is to be valid; and

f. Contractor's name, address, telephone number, assigned Commercial and Government Entity (CAGE) Code and certification of the level of the Facility (Security) Clearance (FCL).

4. Formal visit requests should not be required for employees of the executive branch who are U.S. citizens with whom working relationships have been established. When there is an established working relationship and the clearance level and bounds of need to know of the government employee are known, a visit request is not necessary. Many times there are frequent phone contacts with only occasional visits, but the working relationship is established. The command being visited, not the visitor, will decide whether a formal visit request is needed.

5. DON commands requesting approval for visits to other DON commands may include the phrase, "Reply only if negative," in the request and may assume that approval is granted unless otherwise advised.

6. Requests for visits will be submitted in advance of the proposed visit. Lead time will be established based on local needs to allow sufficient time for processing and to make a determination as to whether or not the visitor should or will be granted access.

7. Visit requests may be transmitted by facsimile, by message or electronically transmitted via electronic mail. When transmitting by facsimile the visit request must be on official letterhead.

8. If a visit requirement comes up suddenly, the above information may be furnished by telephone but it must be confirmed promptly in writing or by message. Message visit requests must include all of the required information listed in paragraph 11-2.

9. Under no circumstances will personnel handcarry their own visit requests to the places being visited.

10. To avoid any question of the legitimacy of the visit request, all visit requests will provide a certification of the visitors need to know in the form of an authorization signature by an official other than the visitor, with command signature authority. For message requests, the fact that the commanding officer released a message for his/her own visit should not be questioned.

11. A visit request that lists more than one name, such as members of an inspection team, is acceptable, even if that request goes to a number of commands who will be inspected by that team or even part of the team provided the purpose of the visit is specific and that all of those listed will be visiting only for that specific purpose. A request for intermittent visits by an individual or group over a specified period of time (not to exceed 1 year) is also acceptable. The command sending an intermittent visit request is responsible for advising the recipient immediately of any significant change to the information supplied.

12. Contractor visits may be arranged for the duration of the contract with the approval of the cognizant contracting command being visited. The contractor, as directed by the NISPOM is responsible for notifying all visited commands of any change in the employee's status that will cause the visit request to be cancelled prior to its stated termination date.

13. Receipt of a fraudulent visit request will be reported to the nearest NCIS office.

14. No additional requirements for visit requests may be imposed by DON commands or activities. If a request is received for a visit requiring access to classified information by a person or under circumstances not addressed in this chapter, the matter will be referred to appropriate higher authority or to CNO (N09N2).

15. 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).

16. Visits involving access to dissemination of SCI are governed by the policies and procedures in reference (c).

11-3 VISITS BY FOREIGN NATIONALS AND REPRESENTATIVES OF FOREIGN ENTITIES

1. Consult SECNAVINST 5510.34, Manual for the Disclosure of Department of the Navy Military Information to Foreign Governments and International Organizations, 4 Nov 93 (NOTAL) concerning foreign visitors, whether or not the visitor requires access to classified, or controlled unclassified, information or material. Visits by foreign nationals and representatives of foreign governments, foreign industry, or international organizations, must be approved, and the disclosure level for classified information determined, for each visitor.

2. Official requests must be submitted by the applicable foreign government (normally its' Washington D.C. embassy) certifying the visitors' national clearances and need to know on their behalf.

11-4 CLASSIFIED VISITS BY MEMBERS OF CONGRESS

1. When a direct request for a Congressional visit which would require disclosure of classified information is received, guidance will be requested from the Office of Legislative Affairs (OLA) by the quickest practical means. If there is inadequate time to coordinate with OLA, the visit may be authorized and disclosure of classified information which meets the requirements of the member of Congress may be made. Immediately thereafter, the OLA will be informed of the visit and the extent of the disclosure. In case there is a question as to whether particular classified information may be furnished to a Member of Congress, no final refusal to furnish such information will be made by a commanding officer. The case will be referred to the Secretary of the Navy through the OLA.

2. Members of Congress, by virtue of their elected status, do not require DoD security clearances. Clearance eligibility is required however, for congressional staff members accompanying a member of Congress (paragraph 8-3.5 applies).

11-5 CLASSIFIED VISITS BY REPRESENTATIVES OF THE GENERAL ACCOUNTING OFFICE

1. Properly cleared and identified representatives of the General Accounting Office (GAO) may request a visit and be granted access to classified DON information in the performance of their assigned duties and responsibilities, with the exceptions noted in paragraph 11-5.3.

2. The GAO normally will give advance notice to commands to be visited. Each announcement will include the purpose of the visit and names of representatives and, if access to classified information may be necessary, will certify the level of security clearance of each GAO representative. Occasionally, the GAO representatives in the Washington metropolitan area receive assignments - such as Congressional requests - which preclude the usual advance written notice of visit, and verbal arrangements are made for visits. To assist the GAO in those instances, the DON GAO liaison office, Assistant Secretary of the Navy, Financial Management & Comptroller (ASN(FM&C)) will provide telephonic authorization for GAO Headquarters and Washington Regional Office personnel whose clearances are on file with DoD. These clearances will be honored provided the GAO representatives are properly identified. GAO personnel can be identified by serially numbered credential cards issued by the Comptroller General. Each card bears the photograph and signature of the holder. Security clearance eligibility of visiting GAO personnel will be verified if access is required.

3. As exceptions to the procedures described above:

a. Commanding officers will not grant access to documents and information specified as not releaseable or requiring approval of the Secretary of the Navy for release, in SECNAVINST 5740.26A, Relations with Legislative Branch Audit and Investigative Agencies, 15 Jan 98.

b. Requests for classified defense information in the area of tactical operations and intelligence collection and analysis will be sent to the ASN(FM&C)) (via the Commandant, U.S. Marine Corps, for USMC cases) by the most expeditious means, to determine the relevance of the information to the statutory responsibilities of the GAO.

4. Questions and problems concerning clearances of individuals and release of classified information in connection with visits by the GAO will be addressed to the ASN(FM&C)) (via the Commandant, U.S. Marine Corps, for USMC cases).

APPENDIX A

DEFINITIONS

Access
The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures that are in force do not prevent the individual from gaining knowledge of such 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.

Active Service (See Continuous Service)

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, the "military departments" as defined in 5 U.S.C. 102, and any other entity within the Executive Branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office.

Annual Training (AT)
A limited period of active duty for training with an automatic reversion to inactive duty when the specified period of training is completed, including the annual active duty for training that Selected Reserve members must perform each year to satisfy training requirements. See inactive duty for training (INACDUTRA).

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.

Applicant
A person, other than an employee, who has received an authorized conditional offer of employment for a position that requires access to classified information.

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.

Break-in-Service
When continuous service is disrupted for a period of time greater than 24 months. See Continuous Service.

Classification
The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

Classified Information
Information that has been determined under Executive Order (E.O.) 12958, or any successor order, E.O. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011) to require protection against unauthorized disclosure.

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

Classification Management
A discipline which seeks to ensure that official information is classified only when required in the interest of national security, is properly identified and retains the classification assigned only as long as necessary.

Clearance
A formal determination that a person meets the personnel security standards and is thus eligible for access to classified information other than that protected in a special access program. There are three types of clearances: Confidential, Secret, and Top Secret. A Top Secret clearance makes an individual eligible for access to Top Secret, Secret, and Confidential classified material; a Secret clearance to Secret and Confidential material; and a Confidential clearance to Confidential material.

Cleared Contractor
Any industrial, educational, commercial, or other entity, grantee, or licensee, including an individual, that has executed an agreement with the Federal Government to perform services enumerated on a classified contract, license, independent research and development (IR&D) program, or other arrangement that requires access to classified information.

Cleared Contractor Employee
As a general rule, this term encompasses all contractor employees granted a personnel security clearance under the National Industrial Security Program.

Cohabitant
A person living in a spouse-like relationship with another person. (See immediate family.)

Command
For the purpose of this regulation, any organizational entity including a unit, ship, laboratory, base, squadron, activity, facility, etc.

Commanding Officer
For the purpose of this regulation, the head of an organizational entity. The term includes commander, officer in charge, naval representative, director, inspector, and any other title assigned to an individual, military or civilian, who, through command status, position or administrative jurisdiction, has authority over an organizational entity.

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

Compelling Need
A senior official's (or designee's) signed determination, based upon an assessment of risk, that a person's services are essential to accomplishing an operation or mission. (See waiver.)

Compromise
A security violation which has resulted in confirmed or suspected exposure of classified information or material to an unauthorized person. A compromise is considered confirmed when conclusive evidence exists that classified material was compromised. A compromise is considered suspected when some evidence exists that classified material has been subjected to compromise.

Condition (See Exception)

Confidential Periodic Reinvestigation
An investigation conducted at 15-year intervals for the purpose of updating a previously completed NAC, ENTNAC, or NACI. The CPR includes the elements of the NACLC.

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 which 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.

Counterintelligence
Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

Critical Nuclear Weapon Design Information (CNWDI)
Top Secret Restricted Data or Secret Restricted Data that reveals 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, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive material by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test or replace.

Defense Clearance and Investigative Index (DCII)
The DCII is the single, automated, central DoD repository which identifies investigations conducted by DoD investigative agencies, and personnel security determinations made by DoD adjudicative authorities.

Deliberate Compromise
Any intentional act done with the intent of conveying classified information to any person not officially authorized to receive it.

Deviation (See Exception)

DoD Component
Includes the Office of the Secretary of Defense; the Military Departments; Chairman of the Joint Chiefs of Staff and the Joint Staff; Directors of Defense Agencies and the Unified Combatant Commands.

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)
A review of records held by certain National agencies including the Federal Bureau of Investigation (FBI). Conducted on a first term enlistee in the Navy or Marine Corps. The FBI check is a name check only.

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.

Executive Branch of the Government
All Federal activities that are not part of the legislative branch (which includes the Congress and congressional staffs, General Accounting Office, General Printing Office) and the judicial branch (which includes the Supreme Court, United States Courts). The executive branch is comprised of executive departments, independent establishments, and government corporations. The departments, offices, and agencies relevant to the personnel security program are Agriculture, Commerce (Patent Office), Defense (the Military Departments and Defense Agencies), Education, Energy, Health and Human Services (Public Health Service, National Institutes of Health, Social Security Administration), Housing and Urban Development, Interior, Justice (Federal Bureau of Investigation, Immigration and Naturalization Service, Drug Enforcement Administration), Labor, State, Transportation (U.S. Coast Guard, Federal Aviation Administration, Maritime Administration), and Treasury (U.S. Customs Service, Internal Revenue Service, U.S. Secret Service). Among the independent establishments and government corporations are Office of Personnel Management, Central Intelligence Agency, General Services Administration, U.S. Postal Service, Nuclear

Regulatory Commission and National Aeronautics and Space Administration.

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.

Foreign National
Any person not a U.S. citizen, U.S. national, or immigrant alien. 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 that capacity.

Formerly Restricted Data
Information removed from the Restricted Data category upon 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.

Head of DoD Component
The Secretary of Defense, the Secretary of the Navy and 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, 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.

Inactive Duty Training (INACDUTRA)
An authorized period of inactive duty training conducted to enhance the participating reservist's readiness for mobilization. Drills are performed either with or without pay. Drills are usually performed per a published schedule established in advance by the unit commanding officer to meet the requirements of the unit.

Intelligence Community
United States organizations and activities identified by executive order as making up the community. The following organizations currently comprise the intelligence community: Central Intelligence Agency; National Security Agency; Defense Intelligence Agency; special offices within the Department of Defense for the collection of specialized foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; and the intelligence elements of the military services.

Interim Security Clearance
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. (Interim access to Sensitive Compartmented Information cannot be approved locally and must be requested from the DON CAF).

Investigation (See Personnel Security Investigation)

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.

JAG Manual Investigation
A proceeding conducted in accordance with the Manual of the Judge Advocate General, chapters II through VI, often ordered by the command having custodial responsibility for classified material which has been compromised or subjected to compromise.

Limited Access Authorization (LAA)
Authorization for access to Confidential or Secret information granted by the Chief of Naval Operations (N09N2) to non-U.S. citizens and immigrant aliens. These authorizations are limited to only that information necessary to the successful accomplishment of assigned duties and are based on a favorable review of the completed Single Scope Background Investigation. The DSS OCC grants LAAs for industry employees.

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**.

Minor Derogatory Information (*See Issue Information*)

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 E.O. 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.

National Industrial Security Program (NISP)
National program to safeguard classified information that is released to contractors, licensees, and grantees of the U.S. Government. The NISP is a single, integrated, cohesive industrial security program to protect classified information and preserve U.S. economic and technological interests.

National Security
The national defense and foreign relations of the United States.

National Security Position
Those positions that support the activities of the U.S. Government concerned with the protection of the nation from foreign aggression and espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the U.S. and positions that require regular use of, or access to, classified information.

Naval Nuclear Propulsion Information (NNPI)
All information, classified or unclassified, concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear powered ships and naval nuclear power plant prototypes, including the associated nuclear support facilities.

Naval Personnel
All Department of the Navy (DON) civilian employees, military officer and enlisted personnel (both regular and reserve), and DON personnel of nonappropriated-fund instrumentalities.

Need for Access
A determination that an individual requires access to a particular level of classified information in order to perform or assist in the performance of a lawful and authorized government function.

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 the performance of a lawful and authorized government function essential to the fulfillment of an official U.S. Government

program. Knowledge, possession of, or access to, classified information will not be afforded to any individual solely by virtue of the individual's office, rank, position, or security clearance eligibility.

Personnel
Any DON civilian, military, or contractor employee.

Personnel Security Investigation (PSI)
Any investigation required 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.

Reciprocity
Acceptance by one agency or program of a clearance or access eligibility determination, whether favorable or unfavorable, made by another. Reciprocity does <u>not</u> include agency determinations of employment suitability.

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 5 year intervals, a Secret periodic reinvestigation (SPR) is normally conducted at 10 year intervals and a Confidential periodic reinvestigation (CPR) is conducted at 15 year intervals.

Scope
The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

Secret Periodic Reinvestigation
An investigation conducted at 10 year intervals for the purpose of updating a previously completed NAC, ENTNAC, or NACI. The SPR includes the elements of the NACLC.

Security
A protected condition which prevents unauthorized persons from obtaining classified information of direct or indirect military value. This condition results from the establishment and maintenance of protective measures which ensure a state of inviolability from hostile acts or influence.

Security Clearance Eligibility (See Clearance)

Security Policy Board (SPB)
The board established by Presidential Decision Directive (PDD) 29 to consider, coordinate, and recommend policy directives for the executive branch of the U.S. government.

Security Violation
Any failure to comply with the regulations for the protection and security of classified material.

Senior Official of the Intelligence Community (SOIC)
The heads of organizations within the intelligence community as defined by E.O. 12333, or their designated representatives. The DoD SOIC's include, Director, National Security Agency; Director, Defense Intelligence Agency; Deputy Chief of Staff for Intelligence, U.S. Army; Assistant Chief of Staff for Intelligence, U.S. Air Force; and the Director of Naval Intelligence, U.S. Navy.

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 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 either special-sensitive, critical-sensitive, noncritical-sensitive, or nonsensitive.

Significant Derogatory Information - (See Issue Information)
Information that could, in itself, justify an unfavorable administrative action, an unfavorable security determination, or prompt an adjudicator to seek additional investigation or clarification.

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 individuals' lives prior to their 16th birthday.

Special Access Program (SAP)
A program established under DoD Directive 0-5205.7, for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Special Investigative Inquiry (SII)
A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations concerning an individual upon whom a personnel security determination has been previously made and who, at the time of the allegation holds a security clearance or otherwise occupies a position that requires a personnel security determination.

Substantial Issue Information - (See Issue Information)

Transmission
Any movement of classified information or material from one place to another.

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; nonappointment to or nonselection to a sensitive position.

Unfavorable Personnel Security Determination
A determination based on an assessment of available information that an individual does not meet the trustworthiness standards required for access to classified information or assignment to sensitive duties.

Unauthorized Disclosure
A communication or physical transfer of classified information to an unauthorized recipient.

United States Citizen (to include 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 U.S.C. 1401(a)(1-7) whenever there is doubt whether a person qualifies as a national of the United States.

Waiver - See Exception.

APPENDIX B

ACRONYMS

AA&E - Arms, Ammunition and Explosives

ACDUTRA - Active Duty for Training

AIS - Automated Information Systems

AJ - Administrative Judge

ANACI - Access National Agency Check with Inquiries

BI - Background Investigation

BUPERS - Bureau of Naval Personnel

CAGE - Commercial and Government Entity Code

CFR - Code of Federal Regulation

CHNAVPERS - Chief of Naval Personnel

CIA - Central Intelligence Agency

CMC - Commandant of the Marine Corps

CNO - Chief of Naval Operations

CNWDI - Critical Nuclear Weapon Design Information

COMNAVSECGRU - Commander, Naval Security Group Command

COMSEC - Communications Security

CONUS - Continental United Stated

COR - Contracting Officer's Representative (formerly Contracting Officer's Security Representative)

CPR - Confidential Periodic Reinvestigation

CS - Critical-Sensitive

DCI - Director, Central Intelligence

DCID - Director, Central Intelligence Directive

DCII - Defense Clearance and Investigations Index

DCPDS - Defense Civilian Personnel Data System

DIA - Defense Intelligence Agency

DNI - Director of Naval Intelligence

DoD - Department of Defense

DoDSI - Department of Defense Security Institute

DOE - Department of Energy

DOHA - Defense Office of Hearings and Appeals

DON - Department of the Navy

DON CAF - Department of the Navy Central Adjudication Facility

DSS - Defense Security Service (formerly Defense Investigative Service (DIS))

DUSD(PS) - Deputy Under Secretary of Defense for Policy Support

EDVR - Enlisted Distribution Verification Report

ENAC - Expanded National Agency Check

ENTNAC - Entrance National Agency Check

E.O. - Executive Order

EOD - Explosive Ordnance Disposal

EPSQ - Electronic Personnel Security Questionnaire

FAD - Facility Access Determination

FBI - Federal Bureau of Investigation

FBI/HQ ID - Federal Bureau of Investigation-Headquarters Identification Division

FCL - Facility (Security) Clearance

FFI - Full Field Investigation

FRD - Formerly Restricted Data

FSM - Federated States of Micronesia

GAO - General Accounting Office

GCA - Government Contracting Activity

HQMC - Headquarters Marine Corps

HRO - Human Resource Office

IBI - Interview oriented Background Investigation

INFOSEC - Information Security

INS - Immigration and Naturalization Service

IRR - Inactive Ready Reserves

ISOO - Information Security Oversight Office

ISP - Information Security Program

ISSM - Information Systems Security Manager

JAG - Judge Advocate General of the Navy

JCS - Joint Chiefs of Staff

LAA - Limited Access Authorization

LBI - Limited Background Investigation

LOI - Letter of Intent

LON - Letter of Notification

LRC - Local Records Check

MBI - Minimum Background Investigation

MCTFS - Marine Corps Total Force System

MOS - Military Operations Specialty

MSRB - Master Service Record Book

MTT - Mobile Training Team

NAC - National Agency Check

NACI - National Agency Check plus Inquiries

NACIC - National Agency Check plus Inquiry with Credit Check

NACLC- 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

NCC - National Computer Center (within DSS)

NCIC - National Crime Information Center

NCIS - Naval Criminal Investigative Service (Formerly NIS/NSIC/NISCOM)

NCS - Noncritical-Sensitive

NISP - National Industrial Security Program

NISPOM - National Industrial Security Program Operating Manual

NJACS - Navy Joint Adjudication and Clearance System

NJAG - Navy Judge Advocate General

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

OASD(C3I) - Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

OCB - (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-FIPC - Office of Personnel Management - Federal Investigation Processing Center

OPNAV - Staff Offices of the Chief of Naval Operations

OSD - Office of the Secretary of Defense

PEP - Personnel Exchange Program

PR - Periodic Reinvestigation

PRP - Nuclear Weapon Personnel Reliability Program

PSA - Presidential Support Activities

PSAB - Personnel Security Appeals Board

PSI - Personnel Security Investigation

PSP - Personnel Security Program

PSQ - Personnel Security Questionnaire

RD - Restricted Data

RUC - Reporting Unit Code

SAP - Special Access Program

SAPOC - Special Access Program Oversight Committee

SCI - Sensitive Compartmented Information

SCIF - Sensitive Compartmented Information Facility

SECNAV - Secretary of the Navy

SF - Standard Form

SII - Special Investigative Inquiry

SIOP-ESI - Single Integrated Operational Plan-Extremely Sensitive Information

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

TIS - Transfer in Status

TNAC - Trustworthiness National Agency Check

TSCA - Top Secret Control Assistant

TSCO - Top Secret Control Officer

UCMJ - Uniform Code of Military Justice

UIC - Unit Identification Code

USIS - US Investigative Service

USO - United Service Organization

USSAN - United States Security Authority, NATO

APPENDIX C

GUIDELINES FOR COMMAND SECURITY INSTRUCTION

1. A written command security instruction or written procedures are necessary to ensure the security requirements contained herein are established for local command operations. In composing a command security instruction or procedures, the security manager must consider whether a function will be required frequently enough to warrant detailed instruction. Consider the size, mission, and scope of the command's authority when selecting topics for instructional elaboration. There is no need to duplicate the requirements contained in this instruction, rather the procedures should supplement the Department of the Navy Information and Personnel Security Program Regulations, and other directives. The guidelines that follow may be helpful in developing the personnel security program portions of your command security instruction.

a. The introduction to the command security instruction should cover the purpose of the instruction, its applicability to all in the command and its relationship to other directives.

b. The majority of the command instruction will concentrate on the command's internal administrative procedures leading to access to classified information or assignment to sensitive duties for command personnel as well as procedures for safeguarding and maintaining classified information. The text will:

(1) Explain each requirement step by step, specifying responsible entities as necessary (eg. if your command is serviced by a centralized personnel office, it will be necessary to spell out the division of personnel security responsibilities between the command security and personnel entities and the centralized personnel office).

(2) Identify the command's security organization, chain of command, including specific areas of responsibility. Elaborate on any requirements peculiar to the command. Indicate organizational relationships and cite any security servicing agreements. Describe procedures for internal security reviews and inspections (including subordinate inspections if appropriate).

(3) Include a security education program using guidelines in chapter 4 of this instruction. Identify personnel responsible for the security education program including specific areas of

responsibility (i.e. briefings and debriefings).

(4) Detail the internal procedures for reporting and investigating compromises and other security violations. Establish channels for reporting counterintelligence matters to the Naval Criminal Investigative Service (NCIS) and procedures for requesting NCIS assistance and identify the NCIS servicing office. If your command has subordinate commands who would be required to forward JAG Manual investigations to you for review, assign responsibilities for review in compromise cases.

(5) Include in this section a list of areas within the command authorized for general visiting and clearly identify all areas that are off-limits to visitors. Assign responsibilities for processing classified visit requests to or from the command.

(6) Formulate guidelines for foreign travel briefings and identify the individual responsible for briefing/debriefing.

(7) If your command hosts foreign exchange personnel/students, or foreign liaison officers, specify any restrictions on movement and caution command personnel regarding their responsibilities.

(8) Assign responsibilities for final preparation of investigative request forms.

(9) Establish procedures for documenting clearance and access granted.

(10) Assign responsibilities for continuous evaluation. Establish procedures for reporting derogatory information to the DON CAF.

(11) Identify the adjudicative guidelines, remind command personnel of their continuing responsibilities to notify security of derogatory information or suspicious behavior.

c. In managing the personnel security program, as with all aspects of security, insure that provisions are in place to monitor the program constantly to assure the procedures are up to date and that they meet the ever changing security needs of your command.

2. Refer to reference (d) for guidance concerning the development of local security requirements for classification management, accounting, control, reproduction, declassification and destruction of classified information.

APPENDIX D

SECURITY INSPECTION CHECKLIST

1. Does the command hold the current edition of SECNAVINST 5510.30A?

2. Does the command hold other references applicable to its security program?

3. Is the security organization in the command defined?

4. Is the security manager designated in writing?

5. Is the security manager identified by name to all command personnel?

6. Does the security manager have direct and ready access to the appointing official?

7. Is the security manager exercising overall management of the program?

8. Does the security manager have sufficient authority and staff to function effectively?

9. Are security assistants assigned?

10. Do the SSO and security manager coordinate and cooperate in the command program?

11. Are command security procedures in writing and current?

12. Does the command have a current written emergency plan?

13. Are security functions performed by another activity covered by a written security servicing agreement?

14. Does the command inspect and evaluate subordinate commands?

15. Do inspections include evaluation of subordinate command security program?

16. Are qualified security inspectors used?

17. Are inspection reports on file?

18. Are discrepancies noted during inspections followed-up and corrected?

19. Does the command have an effective security education program?

20. Are security education materials coordinated with CNO (N09N) when required?

21. Are indoctrination briefings given?

22. Are orientation briefings given?

23. Is on-the-job training given?

24. Are annual refresher briefings given?

25. Are counterintelligence briefings given?

26. Are foreign travel briefings given?

27. Have all personnel with NATO or SIOP-ESI or CNWDI access been briefed as required?

28. Do procedures ensure the Security Termination Statement is executed when required?

29. Are military and civilian personnel made aware that they are subject to administrative sanctions for knowingly, willfully, or negligently committing security violations?

30. Are reports made to appropriate counterintelligence, investigative, and personnel security authorities concerning any employee who is known to have been responsible for repeated security violations?

31. Are counterintelligence matters reported to NCIS when required?

32. Have all personnel been advised of the requirement to report any contact with any individual regardless of nationality, in which unauthorized access is sought, or personnel are concerned that they may be the target of exploitation by a foreign entity?

33. Are investigations conducted and counterintelligence reports made to NCIS where necessary in connection with unauthorized absentees?

34. Are only U.S. citizens nominated for security clearance eligibility determination?

35. Are only U.S. citizens assigned to sensitive duties?

36. Have the policies concerning granting of access to non-U.S. citizens been adhered to?

37. Have the policies concerning the assignment of non-U.S. citizens to sensitive positions been adhered to?

38. Is CNO (N09N) approval obtained before appointment of non-U.S citizens to civilian sensitive positions?

39. Is U.S. citizenship verified before requesting personnel security investigations?

40. Have all civilian positions been designated by sensitivity?

41. Are requests for PSI's kept to the minimum?

42. Is the prohibition against conducting PSI's locally being observed?

43. Is the proper investigation for civilian employment being requested?

44. Is the appropriate investigation being requested for access or assignment?

45. Are PSI's requested only when necessary?

46. Are PSI requests prepared and submitted as required?

47. Is follow-up action taken when appropriate?

48. Are investigative reports controlled and safeguarded as required?

49. Is the filing of investigative reports in official personnel records strictly prohibited and such prohibition observed?

50. Is verification sought when there are indications a prior investigation could satisfy current needs?

51. Are security criteria and adjudication guidelines being applied in personnel security determinations?

52. Are records of personnel security determinations properly maintained?

53. Are adverse personnel security determination procedures being strictly observed?

54. Is there a program for continuous evaluation of eligibility for access or assignment to sensitive duties?

55. Are command clearance and access determinations forwarded to the DON CAF?

56. Are interim clearance procedures followed?

57. Is access granted only to those eligible?

58. Are interim clearances properly granted and recorded?

59. Does the SSO advise the security manager when a final SCI access determination is made and furnish investigation data?

60. Is access to NATO classified information being granted only after final clearance is granted?

61. Are denials or revocations of clearance processed as required?

62. Is access granted only to those with a need to know?

63. Are restrictions on access by non-U.S. citizens being observed?

64. Are personnel with established security clearance eligibility prohibited from gaining access to classified information until they have received an initial security briefing and signed a Standard Form 312, "Classified Information Nondisclosure Agreement"?

65. Are special accesses authorized by the command recorded?

66. Has one time access been granted and properly recorded?

67. Have any Limited Access Authorizations been issued by CNO (N09N)?

68. Is access by foreign nationals or visitors adequately controlled?

APPENDIX E

DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII)

Policy

1. The Defense Clearance and Investigations Index (DCII) is the single, automated central repository that identifies investigations conducted by Department of Defense (DoD) investigative agencies. The DCII also includes data on personnel security determinations made by DoD adjudicative authorities.

2. The data base consists of social security number and alphanumeric index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects in investigative documents maintained by DoD criminal, counterintelligence, fraud, and personnel security investigative activities. Additionally, personnel security adjudicative determinations are indexed alphabetically by subject and numerically by social security number.

Access to the DCII

1. The DCII is operated and maintained by the Defense Security Service (DSS). Access is normally limited to the DoD and other Federal Agencies with adjudicative, investigative and/or counterintelligence missions.

2. Access to a DCII terminal will be from the DSS mainframe computer to a web version. Smartgate Tokens are required on hardware to pass through the DSS firewall to access the DCII system.

3. Commands desiring to gain access to the DCII must submit a written request outlining the justification and specific requirements for query "Read-Only" access to the DCII. The request must be submitted via CNO (N09N2) for approval and endorsement to the Chief, Office of Congressional and Public Affairs, Defense Security Service, (V0105).

4. Upon approval by DSS, a Memorandum of Understanding (MOU) addressing equipment, maintenance, security, privacy, and other command responsibilities will be forwarded directly to the command from DSS.

Security Requirements for the DCII

1. The DCII is an unclassified system that meets the C-2 level of protection under the Computer Security Act of 1987.

2. The information contained in the DCII receives the same protection required by the Privacy Act of 1974.

3. Due to the sensitive nature of the information contained in the database, positions for individuals having direct (password) access to a DCII terminal must have a favorably completed NAC/NACI for "read only" access to the DCII and a favorably completed SSBI/PR is required for those individuals who input into the DCII.

4. To prevent unauthorized access or tampering during nonworking hours, DCII terminals must be located in an area that is secured by guard personnel, an alarm system, or appropriate locking device.

5. When the DCII terminal is operational, access to DCII information shall be controlled and limited to those persons authorized access to that information.

APPENDIX F

PERSONNEL SECURITY STANDARDS

Persons whose conduct and behavior are such that entrusting them with classified information or assigning them to sensitive duties is clearly consistent with the interests of national security include individuals who: are loyal to the United States, comply with laws, have demonstrated dependability in accepting and discharging responsibilities, demonstrate good social adjustment and emotional stability, and have the ability to exercise sound judgement in meeting adversity.

The DON CAF is charged with determining whether an individual is loyal, reliable and trustworthy enough to be eligible for access to classified information or assigned to sensitive duties. In making that determination, the DON CAF evaluates information available which may include information developed by a personnel security investigation and/or information reported by commands. Commanding officers are obligated to report to the DON CAF any information which could impact the loyalty, reliability and trustworthiness evaluation of an individual. Specifically, commands must report any behavior, incident, or allegation which falls under any of following areas of security concern:

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

2. Foreign influence concerns or close personal association with foreign nationals or countries

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

4. Sexual behavior that is criminal or reflects a lack of judgement or discretion

5. Conduct involving questionable judgement, untrustworthiness, unreliability or unwillingness to comply with rules and regulations, or unwillingness to cooperate with security processing

6. Unexplained affluence or excessive indebtedness

7. Alcohol abuse

8. Illegal or improper drug use/involvement

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

10. Criminal conduct

11. Noncompliance with security requirements

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

13. Misuse of Information Technology Systems

APPENDIX G

ADJUDICATION GUIDELINES

1. The following adjudication guidelines were established for all U.S. government civilian and military personnel, consultants, contractors, employees of contractors, and other individuals who require initial or continued access to classified information, access to SCI and/or employment or retention in sensitive duties.

2. While reasonable consistency in reaching adjudicative determinations is desirable, the nature and complexities of human behavior preclude the development of a single set of guidelines or policies that is equally applicable in every personnel security case. Accordingly, the following adjudication policy is not intended to be interpreted as inflexible rules of procedure. The following policy requires dependence on the adjudicator's sound judgment, mature thinking, and careful analysis. Each case must be weighed on its own merits, taking into consideration all relevant circumstances, and prior experience in similar cases as well as the guidelines contained in the adjudication policy, which have been compiled from common experience in personnel security determinations.

3. Each adjudication is to be an overall common sense determination based upon consideration and assessment of all available information, both favorable and unfavorable, with particular emphasis being placed on the nature, extent, and seriousness of the conduct, the circumstances surrounding the conduct, the frequency and recency of the conduct, the individual's age and maturity at the time of the conduct, voluntariness of participation, the presence or absence of rehabilitation, the motivation for the conduct, the potential for pressure, coercion, exploitation or duress and the likelihood of continuation or recurrence of the conduct.

4. The information to be assessed must be fitting to the determination process. Adjudicators will ensure the information's adequacy in terms of E.O. 12968 requirements and that incomplete (missing adjudicatively critical data) and unsubstantiated (uncorroborated "hearsay") information is sufficiently developed before the determination process proceeds.

5. The criteria under which personnel security determinations are made include, but are not limited to the following:

a. Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other acts whose aim is to overthrow the

Government of the United States or alter the form of government by unconstitutional means.

b. Association or sympathy with persons who are attempting to commit, or who are committing sabotage, espionage, treason, terrorism or sedition.

c. Association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means.

d. Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

e. An individual's immediate family, including cohabitants and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress by a foreign power.

f. An individual acts in a way as to indicate a preference for a foreign country over the United States. Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be: (1) the presence of immediate family members or other persons to whom the applicant is bound by affection or obligation in a nation (or areas under its domination) whose interest may be inimical to those of the U.S.; or (2) any other circumstances that could cause the applicant to be vulnerable.

g. Acts of sexual misconduct or perversion indicative of a criminal offense, indicates a personality or emotional disorder and may subject the individual to undue influence or coercion, or reflects lack of judgment or discretion.

h. Conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations that could indicate the individual may not properly safeguard classified information.

i. An individual who is financially overextended who may be at risk of having to engage in illegal acts to generate funds. Unexplained affluence linked to proceeds from financially profitable criminal acts.

j. Excessive alcohol consumption which may lead to

questionable judgment, unreliability, failure to control impulses.

k. Improper or illegal use of any controlled or psychoactive substance, narcotic, cannabis or other dangerous drug.

l. Any emotional, mental and/or personality disorder which, in the opinion of competent medical authority, may cause a defect in judgment, reliability or stability.

m. A history or pattern of criminal activity or dishonest conduct to include any knowing and willful falsification, coverup, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form, or other representation or device used by the DoD or any other Federal agency.

n. Noncompliance with security regulations which could raise doubt about an individual's ability to safeguard classified information.

o. Misuse of Information Technology systems.

6. The listed "Disqualifying Factors" and "Mitigating Factors" in the following adjudication guidelines reflect the consideration of those factors of seriousness, recency, frequency, motivation, etc., to common situations and types of behavior encountered in personnel security adjudications, and should be followed whenever an individual case can be measured against this policy guidance. Common sense may occasionally necessitate deviations from this policy guidance, but such deviations should not be frequently made and must be carefully explained and documented.

7. The "Disqualifying Factors" provided here establish some of the types of serious conduct under the criteria that can justify a determination to deny or revoke an individual's eligibility for access to classified information, or appointment to, or retention in sensitive duties. The "Mitigating Factors" establish some of the circumstances that may mitigate the conduct listed under the "Disqualifying Factors." Any determination must include a consideration of both the conduct listed under "Disqualifying Factors" and any circumstances listed under the appropriate or corresponding "Mitigating Factors."

8. In all adjudications, the protection of the national security shall be the paramount determinant. In the last analysis, a

final decision in each case must be arrived at by applying the standard that the issuance of the clearance or assignment to the sensitive position is "clearly consistent with the interests of national security."

ALLEGIANCE TO THE UNITED STATES

The Concern: An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

Conditions that could raise a security concern and may be disqualifying include:

a. Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;

b. Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

c. Association or sympathy with persons or organizations that advocate the overthrow of the U.S. Government, or any state or subdivision, by force or violence or by other unconstitutional means;

d. Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

Conditions that could mitigate security concerns include:

a. The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

b. The individual's involvement was only with the lawful or humanitarian aspects of such an organization;

c. Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

d. The person has had no recent involvement or association with such activities.

FOREIGN INFLUENCE

The Concern: A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

Conditions that could raise a security concern and may be disqualifying include:

a. An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

b. Sharing living quarters with a persons or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

c. Relatives, cohabitants, or associates who are connected with any foreign government;

d. Failing to report, where required, associations with foreign nationals;

e. Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

f. Conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

g. Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;

h. A substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

Conditions that could mitigate security concerns include:

a. A determination that the immediate family member(s), (spouse, father, mother, sons, daughters, brothers, sisters),

cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;

b. Contacts with foreign citizens are the result of official United States Government business;

c. Contact and correspondence with foreign citizens are casual and infrequent;

d. The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country;

e. Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

FOREIGN PREFERENCE

The Concern: When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

Conditions that could raise a security concern and may be disqualifying include:

a. The exercise of dual citizenship;

b. Possession and/or use of a foreign passport;

c. Military service or a willingness to bear arms for a foreign country;

d. Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;

e. Residence in a foreign country to meet citizenship requirements;

f. Using foreign citizenship to protect financial or business interests in another country;

g. Seeking or holding political office in the foreign country;

h. Voting in foreign elections;

i. Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

Conditions that could mitigate security concerns include:

a. Dual citizenship is based solely on parents' citizenship or birth in a foreign country;

b. Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;

c. Activity is sanctioned by the United States;

d. Individual has expressed a willingness to renounce dual citizenship.

SEXUAL BEHAVIOR

The Concern: Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion. * **Sexual orientation or preference may not be used as a basis for or as a disqualifying factor in determining a person's eligibility for a security clearance.**

Conditions that could raise a security concern and may be disqualifying include:

a. Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

b. Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;

c. Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

d. Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

Conditions that could mitigate security concerns include:

a. The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;

b. The behavior was not recent and there is no evidence of subsequent conduct of a similar nature;

c. There is no other evidence of questionable judgment, irresponsibility, or emotional instability;

d. The behavior no longer serves as a basis for coercion, exploitation, or duress.

*** The adjudicator should also consider guidelines pertaining to criminal conduct and emotional, mental and personality disorders in determining how to resolve the security concerns raised by sexual behavior.**

PERSONAL CONDUCT

The Concern: Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

a. Refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

b. Refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

Conditions that could raise a security concern and may be disqualifying also include:

a. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

b. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

c. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;

d. Personal conduct or concealment of information that may increase an individual's vulnerability to coercion, exploitation or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

e. A pattern of dishonesty or rule violations, to include violation of any written or recorded agreement made between the individual and the agency;

f. Association with persons involved in criminal activity.

<u>Conditions that could mitigate security concerns include</u>:

a. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

b. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

c. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

d. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

e. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

f. A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information;

g. Association with persons involved in criminal activities has ceased.

FINANCIAL CONSIDERATION

The Concern: An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Conditions that could raise a security concern and may be disqualifying include:

a. A history of not meeting financial obligations;

b. Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

c. Inability or unwillingness to satisfy debts;

d. Unexplained affluence;

e. Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Conditions that could mitigate security concerns include:

a. The behavior was not recent;

b. It was an isolated incident;

c. The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);

d. The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;

e. The affluence resulted from a legal source;

f. The individual initiated a good faith effort to repay overdue creditors or otherwise resolve debts.

ALCOHOL CONSUMPTION

The Concern: Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

Conditions that could raise a security concern and may be disqualifying include:

a. Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;

b. Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

c. Diagnosis by a credentialed medical professional (e.g. physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

d. Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

e. Habitual or binge consumption of alcohol to the point of impaired judgment;

f. Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program.

Conditions that could mitigate security concerns include:

a. The alcohol-related incidents do not indicate a pattern;

b. The problem occurred a number of years ago and there is no indication of a recent problem;

c. Positive changes in behavior supportive of sobriety;

d. Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participated frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for a period of

at least 12 months, and received a favorable prognosis by a credentialed medical professional or licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

DRUG INVOLVEMENT

The Concern:

a. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

b. Drugs are defined as mood and behavior-altering substances, and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

(2) inhalants and other similar substances.

c. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Conditions that could raise a security concern and may be disqualifying include:

a. Any drug abuse (see above definition);

b. Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;

c. Diagnosis by a credentialed medical professional (e.g. physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

d. Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

e. Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional. Recent drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will almost invariably result in an unfavorable determination.

Conditions that could mitigate security concerns include:

a. The drug involvement was not recent;

b. The drug involvement was an isolated or aberrational event;

c. A demonstrated intent not to abuse any drugs in the future;

d. Satisfactory completion of a proscribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

EMOTIONAL, MENTAL, AND PERSONALITY DISORDERS

The Concern: Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability or stability. A credentialed mental health professional (e.g. clinical psychologist or psychiatrist), employed by, acceptable to or approved by the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

Conditions that could raise a security concern and may be disqualifying include:

a. A opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

b. Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;

c. A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;

d. Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

Conditions that could mitigate security concerns include:

a. There is no indication of a current problem;

b. Recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured, under control or in remission, and has a low probability of recurrence or exacerbation;

c. The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

CRIMINAL CONDUCT

The Concern: A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Conditions that could raise a security concern and may be disqualifying include:

a. Allegations or admissions of criminal conduct, regardless of whether the person was formally charged;

b. A single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include:

a. The criminal behavior was not recent;

b. The crime was an isolated incident;

c. The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;

d. The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;

e. Acquittal;

f. There is clear evidence of successful rehabilitation.

SECURITY VIOLATIONS

The Concern: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Conditions that could raise a security concern and may be disqualifying include:

a. Unauthorized disclosure of classified information;

b. Violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns include actions that:

a. Were inadvertent;

b. Were isolated or infrequent;

c. Were due to improper or inadequate training;

d. Demonstrate a positive attitude towards the discharge of security responsibilities.

OUTSIDE ACTIVITIES

The Concern: Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer, or employment with:

a. A foreign country;

b. Any foreign national;

c. A representative of any foreign interest;

d. Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

Conditions that could mitigate security concerns include:

a. Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

b. The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

The Concern: Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Conditions that could raise a security concern and may be disqualifying include:

a. Illegal or unauthorized entry into any information technology system;

b. Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;

c. Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

d. Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

Conditions that could mitigate security concerns include:

a. The misuse was not recent or significant;

b. The conduct was unintentional or inadvertent;

c. The introduction or removal of media was authorized;

d. The misuse was an isolated event;

e. The misuse was followed by a prompt, good faith effort to correct the situation.

APPENDIX H

STRUCTURE AND FUNCTIONS OF THE PERSONNEL SECURITY APPEALS BOARD

1. The Department of the Navy Personnel Security Appeals Board (PSAB) is responsible for deciding appeals from Department of the Navy personnel of unfavorable personnel security determinations made by the Department of the Navy Central Adjudication Facility (DON CAF):

a. The PSAB will be comprised of three members at the minimum military grade of 0-6 or civilian grade of GS-14.

b. One member of the board will have a security background and serve as the President of the Board. At least one member will be in the military grade of 0-6. When necessary, the composition of the board will accommodate special circumstances by inclusion of one member reflecting the status of the appellant (e.g., one member will be of Senior Executive Service (SES) grade when the appellant is an SES employee, one member will be from the Marine Corps when the appellant is a Marine, etc.).

c. The President of the PSAB will ensure an attorney is available for all legal questions, guidance or opinions requested by the PSAB.

d. The President of the PSAB will appoint an Executive Director to administer operations of the PSAB.

e. Officials from the DON CAF will neither serve as a member of the board or communicate with board members concerning the merits of an open case.

f. The President of the PSAB will establish procedures to:

(1) Hold monthly board meetings

(2) Determine review procedures to be followed and

(3) Handle other administrative matters.

g. Upon receipt of an appeal, the Executive Director will request the case file from the DON CAF, prepare case files and notify PSAB members.

h. Each case will be reviewed in advance of the PSAB meeting by all three PSAB members. The decision will be based solely on the written record. Hearings will not be held and there will be

no personal presentation before the PSAB. PSAB sitting members will not engage in ex parte communications with appellants or their representatives.

i. The PSAB will act in formal meetings, and its decision will be based on a majority of the votes cast. Only sitting PSAB members may vote on an appeal. The vote results will be recorded by the Executive Director at the time the vote is rendered.

j. The appellant will be notified of the PSAB decision via his/her commanding officer. The DON CAF will be notified of the PSAB decision and may be directed to grant or restore security clearance and or SCI access eligiblity. The DON CAF will retain the completed case file including the PSAB decision letter. A copy of the PSAB decision will also be forwarded to SSO Navy or COMNAVSECGRU, as appropriate and BUPERS for Navy military members, or CMC (CIC) for Marine Corps military members.

k. The appellant will generally be notified of the PSAB decision within 5 days of the board meeting. The written notification will provide the reasons that the PSAB either sustained or overturned the original determination of the DON CAF. The PSAB determination is final and will conclude the appeal process.

2. The PSAB will maintain a redacted file of all decisions which will be subject to review in accordance with the Freedom of Information Act.

APPENDIX I

CITIZENSHIP

REQUIREMENTS

1. Only United States citizens are eligible for a security clearance, assignment to sensitive duties or access to classified information. When compelling reasons exist, in furtherance of the DON mission, including special expertise, a non-U.S. citizen may be assigned to sensitive duties (see chapter 5) or granted a Limited Access Authorization (see chapter 9) under special procedures.

2. When this instruction refers to U.S. citizens, it makes no distinction between those who are U.S. citizens by birth, those who are U.S. nationals, those who have derived U.S. citizenship or those who acquired it through naturalization. For the purpose of issuance of a security clearance, citizens of the Federated States of Micronesia (FSM) and the Republic of the Marshall Islands are considered U.S. citizens.

VERIFICATION OF U.S. CITIZENSHIP

1. First time candidates and candidates for clearance at a higher level than currently held must have their U.S. citizenship status verified before security processing begins. U.S. citizens who hold a current valid security clearance, issued by the DON CAF do not have to submit evidence of citizenship to retain clearance at or below the same level.

2. Navy and Marine Corps officers are required to submit proof of U.S. citizenship before commissioning. Unless an officer's record specifically notes that he/she is not a U.S. citizen, it can be accepted that an officer is a U.S. citizen. Enlistees are also required to submit documentation verifying U.S. citizenship status during enlistment processing. The documents sighted are listed and attested to by a recruiting official on the DD 1966, Application for Enlistment - Armed Forces of the United States.

3. The Immigration Reform and Control Act of 1986 requires personnel offices to verify U.S. citizenship for newly hired government civilian employees. Any employee hired subsequent to implementation of this act is required to provide acceptable proof of U.S. citizenship to the personnel office before appointment can be effected. Previously hired employees were not required to submit proof of U.S. citizenship. The document

utilized by personnel offices as certification to indicate that acceptable proof of U.S. citizenship was cited, may be used as acceptable proof of U.S. citizenship for security clearance purposes, provided the proof of U.S. citizenship is one of the documents listed in paragraph 5 below.

4. The requirement to verify U.S. citizenship for first-time candidates and candidates for clearance at a higher level than currently held is satisfied under the following conditions:

a. A valid Background Investigation (BI) or Special Background Investigation (SBI) completed before 1 September 1979, provided U.S. citizenship was proven at that time; or

b. The record of an officer in the Navy or Marine Corps does not contain evidence of non-U.S. citizenship; or

c. The service record contains a DD 1966 with certification that the documents verifying U.S. citizenship have been sighted; or, for enlisted members, a NAVPERS 1070/601 (Immediate Reenlistment Contract) reflecting that the documentation of U.S. citizenship has been sighted; or

d. When none of these conditions applies, the documentation listed in paragraph 5 below must be sighted.

5. The documentation required to prove U.S. citizenship is generally the same as that required for U.S. passport purposes:

a. If the individual was born in the United States, a birth certificate with a raised seal is valid proof of citizenship. Certification in the form officially issued and certified by the state or county agency is acceptable, provided it shows the birth record was filed shortly after birth and it bears the registrar's signature.

(1) A delayed birth certificate (a record filed more than 1 year after the date of birth) is acceptable, if it shows that the report of birth was supported by secondary evidence as described in paragraph (4) below.

(2) Verification of Birth (DD 372), on which the birth data listed is verified by the registrar, is acceptable for military members.

(3) A hospital birth certificate is acceptable if all of the vital information is given and it has an authenticating or

raised seal or signature. This excludes acceptance of birth certification from commercial birth centers or clinics.

(4) If none of these primary forms of evidence is obtainable, a notice from the registrar that no birth record exists should be submitted. The registrar's notice must be accompanied by the best combination of secondary evidence obtainable. Secondary evidence includes: a baptismal certificate; a certificate of circumcision; affidavits of persons having personal knowledge of the facts of the birth; or other documents such as early census, school or family bible records, newspaper files and insurance papers. The secondary evidence should have been created as close to the time of birth as possible.

(5) All documents submitted as evidence of birth in the United States must be original documents or certified copies. Uncertified copies are not acceptable.

b. If citizenship was acquired by birth abroad to a U.S. citizen parent, a Certificate of Citizenship issued by the Immigration and Naturalization Service; a Report of Birth Abroad of a Citizen of the United States of America (Form FS 240); or a Certification of Birth (Forms FS 545 or DS 1350) issued by a U.S. consulate or the Department of State is acceptable documentation. For personnel born in the Panama Canal Zone, a certificate of birth issued by the Canal Zone Government indicating U.S. citizenship and verified with the Canal Zone Commission is acceptable. Requests for verification of birth in the Panama Canal Zone should be addressed to: Vital Statistics Unit, Administrative Services Division, Panama Canal Commission, APO 34011.

c. In cases of U.S. citizenship by naturalization, a Certificate of Naturalization is required. A Certificate of Citizenship is required if the individual claims to have derived U.S. citizenship through the naturalization of the parent(s). If the individual does not have a Certificate of Citizenship, the Certificate of Naturalization of the parent(s) may be accepted if the naturalization occurred while the individual was under 18 years of age (or under 16 years of age before 5 Oct 1978) and residing permanently in the U.S. Certificates must be originals.

d. A U.S. passport issued to the individual or one in which the individual was included.

LIMITATIONS ON NON-U.S. CITIZENS

1. **"Non-U.S. citizens"** include **foreign nationals** and **immigrant aliens**. Foreign nationals are individuals who are not U.S. citizens or U.S. nationals. Immigrant aliens are foreign nationals who are lawfully admitted to the U.S. for permanent residence.

2. Foreign Representatives are usually non-U.S. citizens (such as exchange officers, foreign scientists, and foreign students) who are employed by or otherwise affiliated with a foreign government. Foreign representatives are governed by foreign disclosure policies and procedures in SECNAVINST 5510.34, Manual for the Disclosure of Department of the Navy Military Information to Foreign Governments and International Organizations, 4 Nov 93 (NOTAL).

3. Under no circumstances will non-U.S. citizens be eligible for access to SCI, SIOP-ESI, CNWDI, NNPI, COMSEC keying material, cryptologic information, intelligence information (unless authorized by the originator), or any special access program information. Non-U.S. citizens are not eligible for access to Top Secret information, Presidential Support Duties or the Nuclear Weapon Personnel Reliability Program (PRP).

4. Enlisted non-U.S. citizens may not enter ratings or military occupation specialties (MOS) which require access to classified information. In the interests of fairness, each non-U.S. citizen entering the Navy or Marine Corps will be advised of these DON security policies affecting assignments, security clearance and access to classified information.

5. Under Executive Order 11935, a non-U.S. citizen cannot be appointed to a civilian position in the federal competitive service without approval from the Office of Personnel Management (OPM) on a case by case basis. OPM's approval of employment is not to be construed as a personnel security determination, authorizing assignment to sensitive duties or access to classified information. See paragraph 5-7 for processing non-U.S. citizens in sensitive positions.

6. Eligibility for clearance of persons who claim both U.S. and foreign citizenship will be determined by application of the adjudication policy on dual citizenship under "Foreign Preference," (see appendix G).

INDEX

PARAGRAPH

A

Abbreviations/Acronyms . . . . . App B
Absentee, unauthorized 3-5
Access (see also Clearance)
  Access for persons outside of the Executive Branch . . . 9-14
  Adjusting access 9-17
  Attorneys 9-12
  CNWDI 9-19
  Contractor access 9-13
  Congressional staffs 11-4
  Continuous evaluation of eligibility 10-1
  Eligibility 9-2
  Facility access determination program 7-6
  Foreign nationals 9-16
  Granting access 9-2
  Granting access to personnel from another military department 6-10
  Historical researchers 9-15
  Investigative and law enforcement agents 9-11
  Limited Access Authorization 9-16
  Members of Congress 8-3
  NATO 6-9
  Need to know 9-2
  One-Time Access 9-6
  Persons outside of the Executive Branch of Government . . 9-14
  Recording Access 9-5
  Reserve personnel in active status 9-10
  Retired personnel 9-9
  SCI (Sensitive Compartmented Information) 6-9, 9-3
  SIOP-ESI 6-9
  Suspension of access 9-18
  Temporary access 9-7
  Terminating access 9-17
  Withdrawing access 9-17
  Visits 11-2
Adjudication
  Adjudicative officials 7-3
  Eligibility for and recording of security determinations . 8-4
  Minimum level of review 7-3
  Personnel security determination authorities 7-2
  Policy 7-1
  Unfavorable determination process 7-7
  Unfavorable personnel security actions 7-9
Adjudication Criteria/Mitigation . . . . . App G
    Allegiance to the United States . . . . . App G-5

Foreign Influence . . . . . App G-6
Foreign Preference . . . . . App G-8
Sexual Behavior . . . . . App G-10
Personal Conduct . . . . . App G-11
Financial Consideration . . . . . App G-13
Alcohol Consumption . . . . . App G-14
Drug Involvement . . . . . App G-16
Emotional, Mental, and Personality Disorders . . . App G-18
Criminal Conduct . . . . . App G-19
Security Violations . . . . . App G-20
Outside Activities . . . . . App G-21
Misuse of Information Technology Systems . . . . . App G-22
Annual refresher briefing 4-8
Applicability of this regulation 1-8
Assistant Security Manager grade requirement 2-6
Attempted suicide 3-4
Attorney General of the United States 1-3

B

Briefings (See security briefings) 4-3

C

Cancellation of personnel security investigations 6-16
"Catch 'Em in CONUS" Program 6-12
Central Adjudication Facility 7-2
Certification of Personnel Security Clearance 8-4
Chief of Naval Operations (N09N) 1-5
Citizenship . . . . . App I
Foreign nationals . . . . . App A, 9-16
Immigrant aliens . . . . . App A
Non-U.S. citizens 9-16
Security requirements 8-3
Verification of U.S. citizenship . . . . . App I
Classified visits 11-2
Classified Information Nondisclosure Agreement (SF 312) . . . 9-4
Clearance 8-1
Administrative withdrawal or adjustment of clearance . . . 8-9
Authority to grant 7-2
Citizenship verification . . . . . App I
Commanding officer's clearance 8-7
Consultants to User Agency 8-7
Cryptographic Duties 8-7
Definition . . . . . App A
Denial or revocation of clearance for cause 8-10
Eligibility 8-4
General Accounting Office personnel 11-5
Granting 7-2, 7-3, 8-6
Individual Ready Reserve (IRR) 8-7

Interim 8-5
Investigative requests 6-2,6-4, 6-5, 6-6, 6-7
Members of Congress 8-3
National Industrial Security Program (NISP) 8-8
NATO security clearances 6-9
Prohibitions 8-3
Rating/MOS Requirements 8-7
Reciprocal acceptance of 8-2
Recording Determinations 8-4
Reestablishing after a denial or revocation 8-11
Reserve Personnel 8-7
Security manager 2-3
Security Termination Statement . . . . . 4-12, Exh 4A
State governors 8-3
Transfer-in-Status (TIS) 8-9
Unique Requirements 8-7
US citizens outside of the executive branch 9-14
Withdrawal/Adjustment 8-9
Combat Operations 1-9
Commanding Officer 2-2
Authority to grant access 9-2
Authority to grant security clearance 8-1
Clearance for 8-7
Restrictions on authority to grant access 9-2
Communications personnel, investigative requirements for . . 8-7
Compromise Investigation
Referral to Naval Criminal Investigative Service 3-2
Continuous Evaluation 10-1
Access 10-1
Co-worker responsibility 10-1
Command responsibility 10-1
Individual responsibility 10-1
Suspension of access 9-18
Supervisor responsibility 10-1
Continuous service 8-2
Controlled PRP positions 6-8
Counterintelligence Matters 3-1
Counterintelligence briefings 4-9
Counterintelligence matters to be reported to NCIS . . . 3-2
Counterintelligence-scope polygraph 9-16
Critical Nuclear Weapon Design Information (CNWDI)
Access controls 9-19
Critical PRP position 6-8
Critical-sensitive position, civilian employee 5-2
Cryptologic Duties 6-8

D

Debriefings 4-11
Defense Central Index of Investigation (DCII) . . . . . App E

Defense Intelligence Agency (DIA) 1-4
Defense Security Service (DSS) 1-4
Definitions . . . . . App A
Denial or revocation of clearance for cause 8-10
Department of Defense 1-4
  Deputy Under Secretary of Defense for Policy Support . . . 1-4
  Defense Intelligence Agency (DIA) 1-4
  Defense Security Service (DSS) 1-4
  DoD Personnel Security Program Regulation (DOD 5200.2-R) . 1-4
  DoD Security Research Center 1-4
  Office of the Assistant Secretary of Defense (OASD (C3I)) . 1-4
Department of the Navy 1-5
  Secretary of the Navy (SECNAV) 1-5
  Special Assistant for Naval Investigative Matters and Security, Office of the Chief of Naval Operations (CNO (N09N)/Director, Naval Criminal Investigative Service (DIRNCIS) 1-5, 7-2
  Director, Department of the Navy Central Adjudication Facility (DON CAF) 1-5, 7-2
  Director of Naval Intelligence (CNO (N2)) 1-5
  Commander, Naval Security Group Command 1-5
  Deputy Chief of Naval Operations (N89), Special Programs Division (SAP) 1-5
  Director, Navy International Programs Office 1-5
Designation of Sensitive positions 5-2

E

Education (See security briefings) 4-1
Emergency access to classified information (see one-time access) 9-6
Emergency appointment of civilians 6-6
ENTNAC follow-up 6-16
Entrance National Agency Check (ENTNAC) 6-2
Espionage 3-2
  NCIS liaison with FBI 3-2
Executive Branch of Government, access by persons outside . 9-14

F

Federal Bureau of Investigation (FBI) 1-3
Federal employees, investigative requirements 6-6
Eligibility for Clearance 8-1
Follow-up actions on investigation request 6-16
Foreign Nationals
  Access by 9-16
  Classified visits 11-3
Foreign Travel Requirements 3-7
Forms procurement . . . . . Exh 6C

G

General Accounting Office, access by 11-5
Granting access 9-2

H

Historical research, access to classified information . . . 9-15
Hostage/Foreign Connection Investigation Interview 6-2

I

Immigrant Aliens 9-16
  Access limitations 9-16
  Clearance prohibition 8-3
Inactive Status
  Reserve personnel, access 9-10
Indoctrination Brief 4-5
Industrial Security
  Access to classified information 8-8, 9-13
  Adverse information 8-8
  Facility Access Determination Program 7-6
  National Industrial Security Program 8-8
  Visits 11-1
Information Security Oversight Office (ISOO) 1-3
Inspections
  Inspections and review 2-2, 2-10
  Requirements for 2-10
  Security Inspection checklist . . . . . App D
Instruction, command guidelines . . . . . App C, 2-2
Interim Clearance 8-5
Investigation, personnel security 6-1
  Access to classified information by non-U.S. Citizens . . 9-16
  Access to NATO or foreign originated information 6-9
  Access to SCI 6-9
  Access to SIOP 6-9
  Agencies authorized to conduct 6-1
  Authority to request 6-1
  Cancellation 6-16
  Certificate of Personnel Security Investigations, Clearance,
    and Access (OPNAV 5520/20) 9-5
  Civilian employment 6-6
  DCII checks . . . . . App E
  Entrance National Agency Check (ENTNAC) 6-2
  ENTNAC Follow-up actions 6-16
  Hostage/Foreign Connection Investigative Interview 6-2
  Local Record Checks 6-12
  Military appointment or enlistment 6-5
  National Agency Check (NAC) 6-2
  National Agency Check plus Inquiry (NACI) 6-2

National Agency Check with Local Agency Checks and Credit Check (NACLC) 6-2
Nuclear weapon PRP 6-8
Periodic Reinvestigation 6-2
Personnel security clearance 8-1
Persons outside of the Executive Branch of Government . . 9-14
Presidential support activities 6-9
Preparation and submission of 6-12, 6-13, 6-14
Reinvestigations 6-2
Rejection 6-16
Request forms 6-13, 6-14
Tracer action 6-16
Transfer of subject of investigation 6-16
Updating 6-2
Validity of 6-1
Investigative Requirements
Access to chemical agents 6-8
Access to NATO 6-9
Access to SCI 6-9
Access to SIOP-ESI 6-9
AIS positions 5-2, 5-3, 6-8
American Red Cross or USO 6-8
Cancellations 6-16
"Catch 'Em in CONUS" Program 6-12
Chemical agent access 6-8
Commanding officer 8-7
Commissioning 6-5
Confidential 6-4
Consultants, Navy-hire 6-7
Contract guard functions 6-8
Cryptographic duties 6-8
Custom inspectors 6-8
Education personnel 6-8
Emergency appointment 6-6
Enlistment 6-5
Follow-up actions on investigation 6-16
Foreign Nationals Hired Overseas 6-8
Intermittent appointees 6-6
Investigative duties 6-8
Limitations on requesting PSIs 6-11
Limited Access Authorization 9-16
Non-Appropriated Fund (NAF) personnel 6-8
Non-U.S. citizens 9-16
Prenomination interview 6-2
Persons outside of the Executive Branch of Government . . 9-14
Positions of trust 7-5
Preparation and submission of investigative forms 6-14
Presidential Support Activities 6-9
PRP 6-8
Safeguarding investigative reports 6-18

Seasonal appointees 6-6
Secret access 6-4
Security manager 2-3, 6-8
Sensitive Compartmented Information (SCI) 6-9
Summer hires 6-6
Temporary employment 6-6
Top Secret access 6-4
Tracer action 6-16
Types of personnel security investigations 6-2
Unescorted entry to Restricted areas 7-6
Validity of prior personnel security investigations . . . 6-10
Verification of prior investigations 6-12
Information Systems Security Manager 2-8

L

Limited access authorization 9-16
Local Record Checks 6-12

M

Marine Corps 7-2

N

National Agency Check (NAC) 6-2
National Agency Check with Written Inquiries (NACI) 6-2
National Agency Check with Local Agency Checks and
Credit Check (NACLC) 6-2
National Security Agency (NSA) 1-4
National Security Council (NSC) 1-3
NATO
Access to 6-9
Investigative requirements for access to 6-9
Security clearances 6-9
Naval Intelligence, Office of 1-5
Special Security Officer, designation of 2-9
Naval Criminal Investigative Service
Counterintelligence briefing 3-1, 4-9
Report of sabotage, espionage, international terrorism or
deliberate compromise 3-2
Navy Personnel Security Appeals Board . . . . . App H, 7-2, 7-8
Noncritical-sensitive positions, Federal employees 5-3
Nonsensitive position, Federal employee 5-3
Non-U.S. citizen in sensitive position 5-7

O

Office of Personnel Management (OPM)
Investigations 6-1, 6-14
Responsibilities 1-3

On-the-job training 4-7
One-time access
  Authorization for one-time access 9-6
OPNAV 5510/413 8-4
  Record of interim clearance 8-5
  Report issues 8-10
  Request clearance certification 8-4, 9-8
  Request SCI access 9-3
  Tracer 6-16
OPNAV 5520/20 9-5
Orientation Briefing 4-6
Other investigative requests for specific performance
  of duty 6-8

P

Personnel Security
  Investigations 6-2
  Personnel Security Appeals Board . . . . . App H, 7-8

Personnel Security Determinations
  Acceptance of personnel security determinations 7-1
  Adjudication guidelines . . . . . App G
  Appeals of 7-8
  Authorities 7-2
  Continuous evaluation 10-1
  Recording 8-4
  Reciprocal Acceptance 8-2
Personnel Security Investigation (see Investigation)
Personnel Security Investigative Requirements
  Appellate Authorities 6-8
  AIS personnel 6-8
  Chemical agent access 6-8
  Civilian employment 6-6
  Clearance authorities 6-8
  Commissioning 6-5
  Communications personnel 6-8
  Consultants, Navy-hire 6-7
  Customs agents, Navy 6-8
  Education personnel 6-8
  Enlistment 6-5
  Foreign nationals 9-16
  Immigrant aliens 9-16
  Intermittent appointees 6-6
  Investigative agents 6-8
  Limitations on requesting PSIs 6-11
  Limited Access Authorizations 9-16
  Local Record Checks 6-12
  NATO, and foreign-originated information 6-9
  Non-appropriated fund personnel 6-8

Non-U.S. citizens 9-16
Personnel Reliability Program 6-8
Presidential Support duties 6-9
Red Cross Personnel 6-8
Seasonal appointees 6-6
Secret access 6-4
Security manager 6-8
Sensitive compartmented information (SCI) 6-9
SIOP-ESI 6-9
Summer hires 6-6
Temporary employment 6-6
Top Secret access 6-4
Unescorted entry to Restricted areas 7-6
Personnel Security Program
Applicability 1-8
Authority 1-2
Citizenship . . . . . App I
Commanding Officer Responsibilities 1-11
Polygraph examination 9-16
Presidential Support duties 6-9
PRP
Initial assignment in the PRP 6-8
Controlled position 6-8
Critical position 6-8
PSAB procedures . . . . . App H, 7-8

R

Reciprocal acceptance of personnel security investigations 6-10
Reciprocal security clearance 8-2
Red Cross, investigative requirements for 6-8
Refresher briefing 4-8
Release of investigative reports to subject 6-18
Reinvestigations 6-2
Access to Confidential 6-2
Access to SCI 6-9
Access to Secret 6-2
Access to Top Secret 6-2
Assignment in a civilian critical-sensitive position . . . 6-2
Assignment to a NATO billet 6-9
Assignment to Presidential Support activities 6-9
Continuation of Limited Access Authorization 9-16
Review of prior investigations 6-11
Reports of investigation, safeguarding 6-18
Reserve Personnel
Access 9-10
Clearance 8-7
Retired, access 9-9
Restricted Data, access 9-19
Retired personnel (military), access 9-9

Revocation of Clearance procedures 7-7, 7-8, 8-10

S

Security Briefings
  Annual refresher briefings 4-8
  Counterintelligence briefings 4-9
  Debriefing 4-11
  Indoctrination 4-5
  Minimum requirements 4-4
  On-the-job training 4-7
  Orientation 4-6
  Policy 4-1
  Responsibility 4-2
  Scope 4-3
Security agreements 2-11
Security Assistants 2-6
Security Training 4-13
Single Scope Background Investigation (SSBI) 6-2, 6-14
Senior Official of the Intelligence Community (SOIC) 1-5
Sensitive Compartmented Information (SCI)
  Access requirements 9-3
  Investigative requirements for access to 6-9
  Responsibility for 1-5, 2-9
Sensitive positions 5-1
SIOP-ESI
  Investigative requirements 6-9
  SIOP-ESI briefing 6-9
Special Access Programs 1-7
  Authority for 1-7
  Investigative requirements 6-9
Special Investigative Inquiry (SII) 6-2
Special Security Officer 2-9
  Duties 2-9
  Grade requirement 2-9
Storage of Investigative reports 6-18
Sabotage, Espionage, International Terrorism or Deliberate
Compromise 3-2
Suicide or attempted suicide 3-4
Suspension of access 9-18, 10-5

T

Temporary access 9-7
Top Secret Control Officer (TSCO) 2-5
  Designation of 2-5
  Grade requirement 2-5
Tracer actions pending investigative requests 6-16
Training for security professionals 4-13
Transferring personnel

debrief 4-11
pending investigation 6-15

U

Unauthorized Absentee 3-5, 9-18
Unfavorable Personnel Security Determinations 7-4, 7-7
Determination process 7-7, 7-8, 7-9
Appeal Process 7-8
Command Responsibilities 7-7, 7-8, 7-9, 10-5
Letters of Intent 7-7
USO Personnel Investigative requirements for 6-8

V

Validity of prior personnel security investigations 6-10
Validity and reciprocal acceptance of personnel security determinations 6-10
Verification of citizenship . . . . . App I
Visits 11-1
Access 11-1
Foreign nationals 11-3
"Need to know" 11-1
Classified visit requests to DON commands 11-2
General Accounting Office 11-5
Immigrant Aliens 11-3
Members of Congress 11-4
Request 11-2

W

Waivers
Security Manager SSBI requirement 2-3
Security Manager Grade requirement 2-3