

THE SECRETARY OF THE NAVY

SECNAV M-5510.30  
JUNE 2006



**DEPARTMENT OF THE NAVY**  
INFORMATION PERSONNEL  
**PERSONNEL SECURITY PROGRAM**  
SECURITY



**PUBLISHED BY  
CHIEF OF NAVAL OPERATIONS (N09N)  
SPECIAL ASSISTANT FOR NAVAL INVESTIGATIVE MATTERS  
AND SECURITY**

June 2006



**DEPARTMENT OF THE NAVY**  
CHIEF OF NAVAL OPERATIONS (N09N2)  
INFORMATION AND PERSONNEL SECURITY  
WASHINGTON NAVY YARD DC 20388-5380

### **FOREWORD**

The Department of Navy (DON) Personnel Security Program (PSP) implements Executive Order (EO) 12968, "Access to Classified Information" and incorporates PSP policies and procedures established by other executive branch agencies

This Manual establishes specific policy set forth in SECNAVINST 5510.30B, "Department of Navy (DON) Personnel Security Program (PSP) Instruction." It is intended to provide maximum uniformity and effectiveness in the application of PSP policies throughout DON. It applies to all DON commands and to all DON military and civilian personnel.

This Manual should be read in its entirety. Major changes to the DON PSP include: updates to national and DoD level program management responsibilities, requires copies of security manager designation letter be provided to CNO(N09N2), mandates formal security manager training, includes attestation policy, clarifies Information Technology (IT) position requirements, details citizenship requirements for sensitive duty assignments, redefines the eligibility determination process for both position sensitivity and clearance eligibility determinations, clarifies eligibility prohibition, clarifies prohibitions for foreign passport, dual citizenship and Smith Amendment issues, redefines interim clearance and temporary access, requires Joint Personnel Adjudication System (JPAS) use for local access records, details the access authorization process for individuals who are ineligible for security clearance and introduces the Automated Continuing Evaluation Program (ACES) and the Electronic Questionnaire for Investigations Processing (e-QIP).

DON commanding officers shall establish and conduct a PSP in compliance with this Manual and SECNAVINST 5510.30B. Questions regarding DON implementation shall be referred to CNO (N09N2).

This manual may be accessed through the Department of the Navy, Navy Electronics Directives System website:  
<http://neds.daps.dla.mil>.

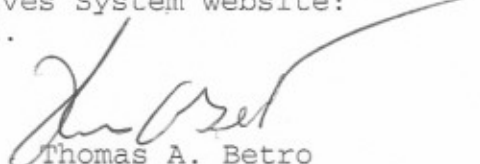
  
Thomas A. Betro  
Special Assistant for Naval  
Investigative Matters and Security

TABLE OF CONTENTS

Paragraph		Page
<b>Chapter 1: Basic Program Policy and Authorities</b>		
1-1	Basic Policy.....	1-1
1-2	Authority.....	1-1
1-3	National Authorities for Security Matters.....	1-2
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.....	1-9
1-7	Special Access Programs.....	1-9
1-8	Applicability.....	1-10
1-9	Combat Operations.....	1-10
1-10	Waivers.....	1-11
1-11	Commanding Officer.....	1-11
1-12	Guidance.....	1-11
1-13	Violations of this Policy Manual.....	1-12
<b>Chapter 2: Command Security Program Management</b>		
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.....	2-3
2-5	Top Secret Control Officer.....	2-5
2-6	Other Security Assistants.....	2-5
2-7	Contracting Officer's Representative.....	2-6
2-8	Information Assurance Manager.....	2-6
2-9	Special Security Officer.....	2-6
2-10	Inspections, Assist Visits, and Reviews.....	2-7
2-11	Security Servicing Agreements.....	2-8
2-12	Standard Program Requirements.....	2-8
2-13	Planning For Emergencies.....	2-9
<b>Chapter 3: Counterintelligence Matters</b>		
3-1	Basic Policy.....	3-1
3-2	Sabotage, Espionage, International Terrorism, Subversion 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
<b>Chapter 4: Security Education</b>		
4-1	Basic Policy.....	4-1
4-2	Responsibility.....	4-1
4-3	Scope.....	4-2
4-4	Minimum Requirements.....	4-3
4-5	Indoctrination.....	4-4
4-6	Orientation.....	4-5
4-7	On-The-Job Training.....	4-6
4-8	Refresher Briefings.....	4-6
4-9	Counterintelligence Briefings.....	4-7
4-10	Special Briefings.....	4-8

4-11	Command Debriefing.....	4-9
4-12	Security Termination Statements.....	4-10
4-13	Training For Security Personnel.....	4-11
4-14	Security Awareness.....	4-11
	Exhibit 4A - Security Termination Statement.....	4A-1
	Exhibit 4B - Nondisclosure Agreement (SF 312) .....	4B-1

**Chapter 5: Sensitive and Information Technology Positions**

5-1	Basic Policy.....	5-1
5-2	Position Designation.....	5-2
5-3	Criteria for Designating Sensitive Positions.....	5-4
5-4	Suitability and Security Investigation and Adjudication.....	5-8
5-5	Security Adjudication Criteria.....	5-9
5-6	Citizenship Requirements.....	5-10
	Exhibit 5A - Investigative Equivalency Table.....	5A-1
	Exhibit 5B - U.S. Citizenship Requirement Waiver Procedures for Persons Nominated to Occupy DON Sensitive and Information Technology (IT) Positions.....	5B-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 Clearance Eligibility.....	6-6
6-5	Investigative Requirements for Military Members.....	6-7
6-6	Investigative Requirements for Civilians in Sensitive Positions and all DON Employees in DON Information Technology (IT) Positions....	6-8
6-7	Investigative Requirements for DON Contractor Personnel.....	6-10
6-8	Specific Duty or Assignment Requirements.....	6-11
6-9	Specific Program Requirements.....	6-14
6-10	Reciprocity and Acceptability of Previously Conducted Investigations	6-16
6-11	Limitations of Requests for Investigation.....	6-18
6-12	Command Responsibilities in PSI Requests.....	6-18
6-13	Personnel Security Investigation Request Forms.....	6-20
6-14	Preparation and Submission of Investigation Requests.....	6-20
6-15	Prioritizing Investigation Requests.....	6-22
6-16	Maintaining Questionnaire Information.....	6-23
6-17	Follow-up Actions on Investigative Requests.....	6-24
6-18	Processing Completed Reports of Investigation.....	6-24
6-19	Safeguarding Reports of Investigation.....	6-25
	Exhibit 6A - PSI Requirements.....	6A-1
	Exhibit 6B - Procurement of Forms.....	6B-1

**Chapter 7: Clearance and Sensitive Assignment Eligibility Determinations**

7-1	Basic Policy.....	7-1
7-2	Authorities and Responsibilities.....	7-2
7-3	Security Clearance and Sensitive Duty Assignment.....	7-5
7-4	DON CAF Determination Process.....	7-6
7-5	Standards for Adjudicative Review.....	7-8
7-6	Requesting Eligibility Determinations.....	7-10
7-7	Reciprocal Acceptance of Eligibility Determinations.....	7-11
7-8	Eligibility Prohibitions.....	7-12
7-9	Unique Eligibility Requirements.....	7-14
7-10	Eligibility Under the National Industrial Security Program.....	7-16

**Chapter 8: Unfavorable Eligibility Determinations and Restrictions**

8-1	Basic Policy.....	8-1
-----	-------------------	-----

8-2	Authorities and Responsibilities.....	8-3
8-3	Restrictions on the Granting or Renewal of Security Clearances.....	8-5
8-4	Unfavorable Determinations Process.....	8-7
8-5	Appeals Process.....	8-9
8-6	Reestablishing Eligibility after a Denial or Revocation.....	8-13
	Exhibit 8A - Structure and Functions of the Personnel Security Appeals Board (PSAB).....	8A-1
	Exhibit 8B - Dual Citizens and Foreign Passports.....	8B-1
	Exhibit 8C - Smith Amendment.....	8C-1

**Chapter 9: Access to Classified Information**

9-1	Basic Policy.....	9-1
9-2	Need-To-Know.....	9-2
9-3	Classified Information Nondisclosure Agreement (SF-312).....	9-3
9-4	Temporary Access (Interim Clearance).....	9-5
9-5	One-Time Access.....	9-7
9-6	Withdrawals or Adjustment of Access.....	9-8
9-7	Suspension of Access for Cause.....	9-9
9-8	Access by Retired Personnel.....	9-11
9-9	Access by Reserve Personnel.....	9-12
9-10	Access by Investigative and Law Enforcement Agents.....	9-12
9-11	Access Authorization in Legal Proceedings.....	9-12
9-12	Contractor Access.....	9-13
9-13	Access Authorization for Persons Outside of the Executive Branch of the Government.....	9-13
9-14	Historical Researchers.....	9-14
9-15	Limited Access Authorization (LAA) for Non-U.S. Citizens.....	9-16
9-16	Personnel Exchange Program Access.....	9-18
9-17	NATO Access.....	9-19
9-18	Sensitive Compartmented Information (SCI) Access.....	9-19
9-19	Access to and Dissemination of Restricted Data (RD) Including Critical Nuclear Weapon Design Information (CNWDI).....	9-21
9-20	Facility Access Determinations.....	9-23

**Chapter 10: Continuous Evaluation**

10-1	Basic Policy.....	10-1
10-2	Security Education.....	10-2
10-3	Employee Education and Assistance Program.....	10-2
10-4	Performance Evaluation System.....	10-3
10-5	Command Reports of Locally Developed Unfavorable Information.....	10-3
10-6	Automated Continuous Evaluation System (ACES).....	10-5
	Exhibit 10A - Continuous Evaluation Check Sheet.....	10A-1

**Chapter 11: Visitor Access to Classified Information**

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

**Appendices**

A	Definitions .....	A-1
B	Acronyms .....	B-1
C	Guidelines for Command Security Manual .....	C-1

D	Security Inspection Checklist .....	D-1
E	Joint Personnel Adjudication System (JPAS) .....	E-1
F	Citizenship Requirements .....	F-1
G	Adjudication Guidelines .....	G-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 (EO) 12968, Access to Classified Information, reference (a) and EO 10450, Security Requirements for Government Employees, reference (b), and in compliance with Department of Defense (DoD) 5200.2-R, DoD PSP Regulation, January 1987, reference (c) and incorporates policies provided in the Navy Department Supplement (NAVSUP) to the DoD Sensitive Compartment Information (SCI) Security Manual DoD DIR 5105.21.M-1 of 18 March 1997, reference (d) and the DON Information Security Program (ISP) Policy Manual, SECNAV M-5510.36 of June 2006 reference (e).

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 them with classified information or assigning them 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 SECNAV (SECNAV) is responsible for establishing and maintaining a PSP in compliance with the provisions of EOs, public laws, NSC, DoD regulations 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 that 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 EO 12958 and further amended by EO 13292. Standards for personnel receiving access thereto are detailed in EO 12968.
2. The **National Security Council (NSC)** provides overall policy guidance on information and personnel security matters.
3. The **Director of National Intelligence (DNI)** is a United States cabinet-level official who serves as the head of the Intelligence Community (IC), and is the principal advisor to the President, the NSC, and the Homeland Security Council for intelligence matters related to national security. The DNI is charged by Public Law 108-458 with establishing and implementing guidelines for the IC for the protection of intelligence sources and methods. The guidelines are issued as National Intelligence Directives and National Intelligence Procedural Guidelines.
4. The **Director of the Information Security Oversight Office (ISOO)** has the responsibility for issuing directives as necessary to implement EO 12958 and provides guidance regarding the Classified Information Nondisclosure Agreement, Standard Form (SF) 312.
5. The **Policy Coordinating Committees (PCC)** are seventeen interagency committees established by National Security Presidential Directive (NSPD-1) to coordinate interagency national security policy issues. The functions of the now defunct Security Policy Board (SPB) were transferred to the Policy Coordinating Committee (PCC) for Records Access and Information Security, which is co-chaired by the Deputy Secretary of Defense and the Principal Deputy Director of National Intelligence (PDDNI). The Interagency Records Access and Information Security PCC considers, coordinates and recommends 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.
6. The **Attorney General of the United States** interprets EO provisions in response to questions arising from implementation upon request from the head of an agency or the Director, ISOO.



7. The **Office of Personnel Management (OPM)** is responsible for oversight and implementation of EO 10450, which prescribes security requirements (including investigations) for federal government employment. Additionally, OPM is the single provider of personnel security investigative products for the DoD.

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

9. 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.

10. The **SECNAV (SECNAV)** is the DON agency head responsible under EO 12968 for establishing and maintaining an effective PSP to ensure that access to classified information by each DON employee is clearly consistent with the interests of national security.

#### **1-4 DOD SECURITY PROGRAM AUTHORITIES**

1. The **Under Secretary of Defense for Intelligence (USD(I))** is the senior DoD official charged by the Secretary of Defense (SECDEF) with responsibility for development of policies and procedures governing information and personnel security policy programs. The **Deputy Under Secretary of Defense (Counterintelligence & Security) (USD) (CI&S)** issues DoD 5200.1-R, Information Security Program Regulation (NOTAL), and DoD 5200.2-R, PSP Regulation, reference (b) (NOTAL).

2. The **Under Secretary of Defense for Policy (USD(TSP&NDP))** administers international security policy and performs administrative support to the SECDEF who is designated the United States Security Authority for North Atlantic Treaty Organization (NATO) (USSAN). The USSAN implements security directives issued by the 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 Network Warfare Command, Commander Information Operations Directorate, Maryland (NNWC/CO IOD,MD). The Director, NSA is authorized by the SECDEF 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 SECDEF.

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 Sensitive Compartmented Information (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)** administers the DoD Industrial Security Program, DoD's Security Education, Training and Awareness Program, and serves as the Executive Agency for PSP automation, including the Joint Personnel Adjudication System (JPAS) and DoD's Electronic Questionnaires for Investigations Processing (e-Qip) program.

6. The **Defense Industrial Security Clearance Office (DISCO)** in Columbus, Ohio makes personnel security eligibility determinations for 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.

7. The **Defense Office of Hearings and Appeals (DOHA)** administers due process procedures for Industrial Security Program unfavorable personnel security determinations and provides hearings and appeals support to DoD military and civilian unfavorable personnel security determinations.

#### **1-5 DON SECURITY PROGRAM MANAGEMENT**

1. The **Secretary of the Navy (SECNAV)** is responsible for implementing a PSP in compliance with the Presidential Directives and the provisions of EO's, public laws, and directives issued by the DNI, SECDEF, DCI, and other program authorities.

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)**

is designated by the SECNAV as the DON senior agency security official under reference (a). The **Assistant for Information and Personnel Security (CNO (N09N2))/Deputy Assistant Director, Information and PSPs (NCIS-24E)** provides staff support for these functions and responsibilities. CNO (N09N)/DIRNCIS is:

a. 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.

(5) Establishing and maintaining the DON Personnel Security Appeals Board (PSAB), appointing a President to preside over the PSAB and appointing board members to ensure proper consideration and deliberation of appeals of unfavorable DON Central Adjudication Facility (DON CAF) personnel security determinations.

b. Responsible for establishing, administering, and overseeing the DON Information Security Program (ISP) and issuing security policy and procedures through reference (e).

3. The **President, Personnel Security Appeals Board (PSAB)** presides over the PSAB, a three-member panel appointed by CNO (N09N) to review and decide appeals of unfavorable DON CAF determinations. The decision of the PSAB to sustain or reverse DON CAF determinations is final and concludes the administrative appeal process.

4. 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 individuals affiliated with the DON. Director, DON CAF has responsibility for:

a. Adjudicating information from personnel security investigations and other relevant information to determine eligibility for access to classified information, and/or assignment to sensitive national security positions and communicate the results via JPAS.

b. Validating and certifying eligibility determinations for all DON personnel.

c. Documenting eligibility determinations in the JPAS system of records.

d. Issuing Letters of Intent (LOI) to deny or revoke eligibility for assignment to sensitive national security positions or access to classified national security information to DON affiliated individuals for whom unfavorable eligibility determination is being contemplated.

e. Issuing Letters of Denial (LOD) (formerly referred to as Letter of Notification (LON)) to DON affiliated individuals for whom unfavorable eligibility determinations have been made, advising of the specific reasons for the unfavorable determination.

f. Recording and retaining the rationale underlying each personnel security eligibility determination where the investigation or information upon which the determination was made included derogatory information.

g. Assisting DON commands with queries regarding the status of personnel security investigations at OPM.

5. The **Department of the Navy Chief Information Officer (DON CIO)** is responsible for providing top-level advocacy in the development and use of Information Management and Information Technology (IM/IT) and to create a unified IM/IT vision for the DON. DON CIO is responsible for ensuring the information technology security for DON Information Technology (IT) systems.

6. The **Commandant of the Marine Corps** is responsible for ensuring personnel security requirements for Marine Corps military members are properly identified to JPAS and that

matters relating to the DON's PSP are appropriately coordinated with CNO (N09N2).

7. The **Chief of Naval Personnel** is responsible for ensuring personnel security requirements for Navy military members are properly identified to JPAS and that matters relating to the DON's PSP are appropriately coordinated with CNO (N09N2).

8. The **Deputy Assistant SECNAV (Office of Civilian Human Resources (OCHR))** is responsible for ensuring personnel security requirements for DON civilian personnel are properly identified to JPAS and that matters relating to the DON's civilian PSP and sensitive position designation are appropriately coordinated with CNO (N09N2).

9. The **Director of Naval Intelligence (CNO(N2)) is a Senior Official of the Intelligence Community (SOIC)**, and administers the SCI program for the Navy, including non-Service DON entities. The **Office of Naval Intelligence (ONI)** is responsible for the security management, implementation, and oversight of SCI security programs for CNO(N2).

10. The **Director, Security and Corporate Services (ONI-05) as Special Security Officer for the DON (SSO Navy)** has been designated as the **Cognizant Security Authority (CSA)**. As CSA, SSO Navy is responsible for implementing SCI security policy and procedures and performs management and oversight of the Department's SCI security program.

11. The **Director of Intelligence, Headquarters, U.S. Marine Corps (DirInt) is a Senior Official of the Intelligence Community (SOIC)** and administers the SCI program for the Marine Corps. The **Office of Naval Intelligence (ONI)** is responsible for the security management, implementation, and oversight of SCI security programs for the DirInt.

12. The **Commander, Naval Network Warfare Command (NETWARCOM), Information Operations Directorate (IOD)** is responsible for the administration of SCI security programs within the Department's cryptologic community.

13. The **Deputy Chief of Naval Operations (CNO (N89)), Special Programs Division** is the DON Special Access Programs Coordinator (SAPCO) and is responsible for the management, administration, support, review, and oversight of the DON SAP security program.

14. The **Director, Navy International Programs Office (Navy IPO)** is delegated the authority to approve or disapprove requests for

access to or transfer of DON technical data or disclosure of DON classified or sensitive unclassified information to foreign governments, international organizations and their representatives in accordance with national disclosure policy.

15. **Commanding Officers** are responsible for day-to-day PSP management:

a. Providing a Security Education, Training and Awareness program for all assigned personnel.

b. Requesting personnel security investigation on personnel assigned to the command, as appropriate.

c. Authorizing and limiting access according to "need-to-know" requirements, and granting temporary access, as necessary and appropriate.

d. Administratively withdrawing access when the requirement for access to classified information no longer exists; debriefing the individual and notifying the DON CAF that security clearance eligibility is no longer required.

e. Maintaining personnel security records of security briefings, access determinations and position sensitivity determinations, ensuring that JPAS data is fully and accurately recorded and maintained.

f. Continuously evaluating command personnel with regard to their eligibility for access to classified information; notifying the DON CAF when potentially disqualifying information is developed.

g. Ensuring personnel are appropriately referred to command assistance programs, as issues dictate.

h. Suspending access to classified information for cause when warranted, notifying the DON CAF within 10 days and forwarding all pertinent information to DON CAF for a personnel security eligibility determination.

i. Ensuring that favorable and unfavorable personnel security eligibility determinations concerning personnel assigned to the command are properly coordinated between supervisors, human resource specialists and security personnel, as appropriate.

j. Ensuring command security officials assist personnel affected by the unfavorable determinations process by explaining the process, providing guidance on obtaining pertinent information and complying with the instructions provided with the LOI, LOD, and PSAB notification letters.

k. Denying or restricting visitor access to command areas, as deemed appropriate, when disqualifying information regarding a visitor is revealed, and ensuring appropriate authorities are notified.

#### **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 Policy manuals: OPNAVINST C5510.101D, NATO Security Procedures (U) (NOTAL); OPNAVINST S5511.35K, Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U) (NOTAL); SECNAVINST 5510.35A, Nuclear Weapon Personnel Reliability Program (PRP); SECNAVINST 5312.12B, Selection of DON Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities; OPNAVINST C8126.1B, 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 5105.21-M-1 of August 1998 (NOTAL) for the protection of SCI.

#### **1-7 SPECIAL ACCESS PROGRAMS**

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 DoD are referred to as DoD Special Access Programs (SAPs). A DoD SAP must be authorized by the SECDEF or by the Deputy Secretary of Defense (DEPSECDEF) and is governed by DoD Directive 0-5205.7, Special Access Program (SAP) Policy of 13 January 1997 (NOTAL), DoD Policy manual 0-5205.11, Management, Administration, and Oversight of DoD Special Access Programs (SAPs) of 1 July 1997 (NOTAL); DoD Directive 5220.22,

National Industrial Security Program of September 2004 (NOTAL); and SECNAVINST S5460.3C, Control of Special Access Programs within the DON (U) (NOTAL). CNO (N7SP) is responsible for the coordination of the approval, administration, support, review, oversight, and reporting of all DON SAPs. The Under SECNAV recommends to the Deputy, Security of Defense, the establishment, modification, or disestablishment of DON SAPs.

#### **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 (e) 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 program 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. "Command" is used as a generic term for the organizational entity and includes ship, laboratory, facility, activity, unit, squadron, etc.

#### **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. This exception does not apply to regularly scheduled training exercises or operations. Exercises are not combat-related 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, Suite 2000, Washington Navy Yard, DC 20388-5380. 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](http://www.navysecurity.navy.mil) provides policy updates, security awareness items and other policy manual materials. Requests for guidance and clarification of this regulation by Marine Corps units may be addressed formally or informally to HQMC (ARS).

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

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

**1-13 VIOLATIONS OF THIS POLICY MANUAL**

1. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice (UCMJ), or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of this policy manual.

2. Civilian employees are subject to criminal penalties under applicable Federal Statutes, a well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of this policy manual.

## CHAPTER 2

### COMMAND SECURITY MANAGEMENT

#### 2-1 BASIC POLICY

1. Commanding officers are responsible for compliance with and implementation of the DON ISP and PSP within their command. The effectiveness of the command's security program depends on the importance given to the program by the commanding officer.

#### 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. Designating a security manager in writing.
- b. Designating a Top Secret Control Officer (TSCO) in writing if the command handles Top Secret information.
- c. Designating an information assurance manager (IAM) in writing if the command processes data in an automated system.
- d. Designating a security officer in writing to manage facilities security.
- e. Designating a special security officer (SSO) in writing to administer the command SCI security program.
- f. Issuing a written command security policy manual. See appendix C and exhibit 2A of reference (e) ISP program.
- g. Establishing 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. Ensuring 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. Preparing an emergency plan for the protection of classified material.
- j. Ensuring that command security inspections, program reviews, and assist visits are conducted for effectiveness of the PSP in subordinate commands.
- k. Ensuring 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.
- l. Ensuring implementation and required use of the Joint Personnel Adjudication System (JPAS).

### **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**.
  - a. A copy of the security manager's designation letter must be forwarded to CNO(N09N2). If practical, the designation letter copy should be scanned by the security manager and sent via e-mail to [navysecurity@ncis.navy.mil](mailto:navysecurity@ncis.navy.mil), providing Unit Identification Code and return e-mail address. Marine Corps commands will forward designation letter via HQMC (ARS).
  - b. Security manager data will be maintained by CNO (N09N2) to promote program management goals and to allow proper registration for security awareness products, notification of training opportunities and policy updates.
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 a military 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 Single Scope Background Investigation (SSBI) completed within the five years prior to assignment.
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. Marine Corps Warfighting Publication 3-40.1 stipulates that the security manager report directly to the chief of staff or executive officer.

5. Commanding officers are required to obtain formal training for their security managers. The Naval Security Manager Course offered by the Naval Criminal Investigative Service (NCIS) Security, Training, Assistance and Assessment Team (STAAT), satisfies this requirement.

#### **2-4 DUTIES OF THE SECURITY MANAGER**

1. The security manager is the key in developing and administering the command's ISP and PSP. The security manager is the principal advisor on information and personnel security in the command (except issues specific to SCI, IT security and SAPs unless officially designated for these additional duties and responsibilities) and is responsible to the commanding officer for the security program management.

a. The duties described here and in chapter 2 of reference (e) 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 to the commanding officer for all program requirements.

b. The security manager must be cognizant of the command security functions and ensure the security program is coordinated and inclusive of all requirements. Security management may involve direct supervision, oversight, coordination, or a combination thereof, to ensure that those individuals in the command who have security duties are kept abreast of changes in policies and procedures, and are provided assistance in solving security problems.

2. The below listed duties (and those provided in chapter 2 of reference (e) 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 vetted 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 in the Joint Clearance and Access Verification System (JCAVS), and that subordinate commands are properly registered for JCAVS, as necessary.

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 Assurance Manager (IAM) 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, exhibit 4A. The original statement is filed in the individual's field service record or official personnel folder (OPF) and a copy in the command files. Marine Corps commands will submit the original Security Termination Statement to MMSB-20, 2008 Elliott Road, Quantico, VA 22134-5030, for inclusion in the Official Military Personnel Folder (OMPF).

m. Ensures all personnel execute a Classified Information Nondisclosure Agreement (SF 312) prior to granting initial access to classified information and records execution of the SF 312 in JCAVS.

## **2-5 TOP SECRET CONTROL OFFICER**

Commands that handle Top Secret material will designate a Top Secret Control Officer (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 favorably adjudicated SSBI completed within five years of initial assignment, with SSBI-PR every five years thereafter. Duties of a TSCO are listed in chapter 2 of reference (e).

## **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 take direction from the security manager and provide support, as needed. Assistant security managers must have an SSBI if they are designated to issue interim or temporary, security clearances; otherwise, the investigative and clearance eligibility 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 **in writing** 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.** Individuals may be assigned to assist the TSCO as needed. The designation will be **in writing**. A person designated as a Top Secret Control Assistant (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 TSCAs. Duties of a TSCA are listed in chapter 2 of reference (e).

## **2-7 CONTRACTING OFFICER'S REPRESENTATIVE**

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 personnel and information security requirements are properly recorded, that industrial security functions are accomplished when classified information is provided to industry for performance on a classified contract, and that personnel security requirements are met when access to DON IT systems is at issue.

## **2-8 INFORMATION ASSURANCE MANAGER**

1. Each command involved in processing data in an information technology system, including access to local area networks and/or INTRANET/INTERNET, must designate in writing a U.S. citizen civilian or military member as an IAM.
2. The IAM is responsible for establishing, implementing and maintaining the DON information system and information assurance program and is responsible to the commanding officer for developing, maintaining, and directing the implementation of the information assurance (IA) program within the command. The IAM advises the commanding officer on all IA matters, including identifying the need for additional IA staff. The IAM serves as the command's point of contact for all IA matters and implements the command's IA program. The IAM coordinates information and personnel security matters with the command security manager, as appropriate. The IAM must have a favorable SSBI completed within five years of initial assignment, which is updated by Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR) every five years. The duties and functions of the IAM are prescribed by "Department of the Navy Information Assurance (IA) Policy," SECNAVINST 5239.3A.

## **2-9 SPECIAL SECURITY OFFICER**

1. Commands in the DON accredited for and authorized to receive, process and store SCI will designate a Special Security Officer (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 (d). 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 shall be referred to the SSO.

2. The SSO and a 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) 6/4, "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 Commander, NETWARCOM (IOD).

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. Qualified personnel will conduct inspections, assist visits, and reviews to examine the command's overall posture. Unless otherwise required, it is unnecessary to conduct separate inspections for security. They may be conducted during other scheduled inspections, but the results of security inspections must be identified as such.

3. A command PSP self-inspection guide is provided as appendix D.

4. Refer to exhibit 2C of (e) 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 that may directly affect the security posture of the command. Append security-servicing agreements to the command security policy manual.

## **2-12 STANDARD PROGRAM REQUIREMENTS**

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

## 2-13 PLANNING FOR EMERGENCIES

Commands will establish a plan for the protection and/or removal of classified National Security Information (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 policy manual. See reference (e), exhibit 2B. "Command" is used as a generic term for the organizational entity and includes ship, laboratory, facility, activity, unit, squadron, etc.

## CHAPTER 3

### COUNTERINTELLIGENCE MATTERS

#### 3-1 BASIC POLICY

Certain matters affecting national security must be reported to the 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, TERRORISM, SUBVERSION, 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 shall promptly notify the servicing NCIS office. If the servicing NCIS office cannot be contacted immediately and the report concerns sabotage, terrorism, espionage, or imminent flight or defection of an individual, the command will immediately contact the Director, NCIS (DIRNAVCRIMINSERV WASHINGTON DC) by classified IMMEDIATE message, with CNO (N09N2) and (NAVY JAG WASHINGTON DC//17//) as an information addressees.

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 the pertinent information to the nearest NCIS office by quickest means available.

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

### **3-6 DEATH OR DESERTION**

When an employee of the DON who has access to classified information dies or deserts, the employee's commanding officer must determine if any unusual indicators or circumstances may have existed that may cause security concern. If such concerns exist, the command will report these concerns by the most expedient means available and provide 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 investigative service provider 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.

3. All personnel with established security clearance eligibility are required to report foreign connections to their security manager. Security managers must report these issues and coordinate resolution with DON CAF, as appropriate.

## 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 that 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 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 that 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 on 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, fax, IT system 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 or assignment to sensitive duties

(including IT duties) 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 annually 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. All 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 induction. 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 or assignment to sensitive IT duties 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 or assignment to sensitive IT duties.

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

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 policy manual 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 checkpoints, destruction, visitors, etc.;

d. Their responsibility to protect classified information;

e. Their obligation to report suspected security violations;

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

5. Additionally, commands must ensure that individuals assigned to DON IT positions receive the requisite information assurance, security awareness, and functional competency training as

required by their designated level of access and scope of duties, and that the training is documented in individual personnel files. Understanding the threats, system vulnerabilities, and protective measures required to counter such threats at each IT access level are key features of a core information assurance awareness program.

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

#### **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; and
- d. Command specific security concerns or problem areas.

e. Attestation of Nondisclosure Agreement requirements.

4. Results of self-inspections, inspector general reports, or security violation investigations provide valuable information for use in identifying command weaknesses;

5. Every individual who is authorized Top Secret clearance eligibility, or who has access to SAP or SCI access, will make a verbal attestation confirming that they will conform to the conditions and responsibilities imposed by law and regulation on individuals granted such eligibility or access. The following applies to DON military and civilian personnel:

a. After reading the entire Classified Information Nondisclosure Agreement (Exhibit 4A) and/or the SCI/SAP Indoctrination Form, individuals initially authorized Top Secret clearance eligibility or access to a specially controlled category or compartmented information (SCI and SAP), shall verbally attest to fully understanding their responsibilities in protecting national security information and adhering to the provisions specifically stated in paragraph 1 of the forms to which they are agreeing.

b. The forms and verbal attestation must be witnessed by one individual in addition to the official presiding over the attestation.

c. Personnel with an existing Top Secret clearance eligibility or SCI/SAP access will verbally attest at the time the required periodic reinvestigation is requested or when granted access to another compartmented program, whichever is sooner.

d. During refresher training, commands will stress the provisions of the Nondisclosure Agreement and the responsibilities inherent for individuals with access to classified information. Security managers will be responsible for recording this training. Execution of the nondisclosure agreement forms will be recorded in JPAS.

#### **4-9 COUNTERINTELLIGENCE BRIEFINGS**

All personnel who have access to material classified Secret or above must receive periodic briefings, annually, on all threats posed by foreign intelligence and terrorist organizations. The security manager is responsible for arranging for the briefing with the local NCIS office.

#### 4-10 SPECIAL BRIEFINGS

1. Special briefings include briefings that are not required as a matter of routine, but which may be required by unique circumstances or other program requirements including:

a. **Foreign Travel Briefing**

(1) 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.

(2) 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).

(3) 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.

(4) Audiovisual material for a formal foreign travel briefings is stocked at servicing NCIS offices.

b. **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.

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

d. **NATO Security Briefing**. All personnel who have access to a SIPRNET terminal accredited to receive and process NATO information must receive a NATO security briefing.

2. Special briefings will be recorded in JPAS as functionality permits, or records may be maintained locally in the form of rosters or other automated format, until JPAS record keeping

functionality is fully deployed.

#### **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 transfer to the Inactive Ready Reserves (IRR);
- d. Expiration of a Limited Access Authorization (LAA);
- e. Inadvertent substantive access to information that 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 chapter 9 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 the provisions of the Classified Nondisclosure Agreement (SF 312) (exhibit 4A) 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 (N09N2);
- 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 4B, 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 two 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 only refusals to CNO (N09N2).

6. The SECDEF 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 (DASD(S&IO) via CNO (N09N2).

#### **4-13 TRAINING FOR SECURITY PERSONNEL**

1. The NCIS Security Training, Assistance, Assessment Team (STAAT) offers the Naval Security Manager Course, DON unique core training developed to train security managers, but also available to security specialists and assistants. For more information on this course, contact the Atlantic STAAT at NAB Little Creek, (757) 462-283 or DSN 253-2834 or the Pacific STAAT at NAS North Island, (619) 545-8934 or DSN 735-8934 or the CNO (N09N2) web page at [www.navysecurity.navy.mil](http://www.navysecurity.navy.mil).

2. A Navy correspondence course entitled "Department of the Navy Introduction to the Information and Personnel Security Program," NAVEDTRA #14210, is available through the command education service officer (ESO).

3. For other security training available to DON personnel, contact the CNO (N09N2) security education specialist at (202) 433-8843 or DSN 288-8843. Security training opportunities are also posted on the CNO (N09N2) web page at [www.navysecurity.navy.mil](http://www.navysecurity.navy.mil).

4. A listing of security disciplines and phone numbers is published periodically and posted on the web page to assist in routing telephone 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 that should be used to promote security awareness.

SECURITY TERMINATION STATEMENT

---



---



---

(Enter the name and address of the Navy or Marine Corps activity obtaining this statement)

1. I HEREBY CERTIFY that I have returned to the Department of the Navy (DON) all classified material which I had in my possession in accordance with the directions contained in the DON Information and Personnel Security Program Regulations SECNAVINST 5510.36, the EKMS-1, CMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 and 3, and EKMS-1 Supplement 1, CMS Policy and Procedures for Navy Electronic Key management System Legacy Accounts/Tier 2S.

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 to any person or agency. I understand that the burden is upon me to ascertain whether or not information is classified and I agree to obtain the decision of the Chief of Naval Operations (CNO) or the CNO's 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 the local Naval Criminal Investigative Service office without delay any incident wherein an attempt is made by an unauthorized person to solicit classified information.

5. I have been informed and am aware that Title 18 U.S.C. Sections 641, 793, 794, 798, 952 and 1924, as amended, and the Internal Security Act of 1950 prescribe severe penalties for unlawfully divulging information affecting the National Defense. I have been informed and am aware that the making of a willfully false statement herein renders me subject to trial 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 military member
Type or print name of witness	Type or print first, middle and last name of employee or service member. Include civilian grade or military rank/rate.
DATE	DATE

---

## CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

---

AN AGREEMENT BETWEEN

AND THE UNITED STATES

---

*(Name of Individual - Printed or typed)*

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.2, 1.3, and 1.4(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

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

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

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

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

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

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

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

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

*(Continue on reverse.)*

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952 and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

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

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

**SECURITY DEBRIEFING ACKNOWLEDGEMENT**

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

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS <i>(Type or print)</i>	SIGNATURE OF WITNESS

**NOTICE:** The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

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

## CHAPTER 5

### SENSITIVE AND INFORMATION TECHNOLOGY POSITIONS

#### 5-1 BASIC POLICY

1. It is important to distinguish authority and responsibilities for employment related determinations. Employment qualification is measured by experience, education, knowledge, skills, and abilities. Qualification determinations are normally made in the DON by the selecting official based on the information provided by the job applicant. Employment suitability, on the other hand, refers to those identifiable character traits and past conduct which are sufficient to demonstrate the likelihood that an employee or applicant will carry out assigned federal government duties with the necessary efficiency and effectiveness. Suitability determinations are typically made after the qualification determination, and are based on an evaluation of the suitability criteria as evidenced in the appropriate completed background investigation.
2. The Office of Personnel Management (OPM) provides the rules and regulations to carry out the employment suitability determination program under Title 5, United States Code of Federal Regulation (CFR). In 5 CFR Part 731, OPM provides the requirements for public trust position suitability determinations. In 5 CFR Part 732, OPM provides the requirements for National Security position suitability determinations.
3. Public trust positions include federal government positions that meet the high and moderate risk levels identified by 5 CFR 731. Public trust positions do not include National Security positions. 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; and (2) positions that require regular use of, or access to, classified information. The DON mission is such that most DON positions are sensitive national security positions.
4. Public trust position determinations are under the purview of Deputy Assistant Secretary of the Navy (Civilian Personnel). DON National Security Position suitability determinations are under CNO (N09N2) purview and are governed by this policy manual.
5. DON IT positions include any position in which the incumbent

has access to DON IT systems and/or performs IT-related duties with varying degrees of independence, privilege, and/or ability to access and/or impact sensitive data and information. Given the direct supporting relationship of DON IT systems to the DON national security mission, most DON IT positions are sensitive.

## 5-2 POSITION DESIGNATION

1. In order to provide the appropriate level of background investigation and suitability adjudication, positions are designated according to potential risk. 5 CRF, 732.201 requires that National Security positions, hereafter referred to as sensitive positions, be formally designated for federal civilians according to the position sensitivity level. A sensitive position is any position whose occupant could bring about, by virtue of the nature of the position, an adverse effect on the national security. There are three sensitivity levels (and one none sensitive level):

- |                                |   |
|--------------------------------|---|
| a. Special-Sensitive (SS)      | Potential for inestimable impact and/or damage  |
| b. Critical-Sensitive (CS)     | Potential for grave to exceptionally grave impact and/or damage                             |
| c. Noncritical Sensitive (NCS) | Potential for some to serious impact and/or damage  |
| d. Non-Sensitive (NS)          | Potential for no impact and/or damage as duties have limited relation to the agency mission |

2. Office of Management and Budget (OMB) Circular A-130, provides the criteria for determining IT position risk levels, considering the level of automated privileges afforded, the level of fiscal privileges afforded, the scope of responsibilities, the level of independence and oversight afforded, and the ability to access sensitive information. The DON's national security mission is a primary consideration in all DON IT position designations. There are three basic DON IT levels and one overarching DON control level:

- a. IT-Designated Approving Authority (DAA) - Exceptional privilege, exceptional control
- b. IT-I - Privileged access

b. IT-II - Limited Privilege, sensitive information access

c. IT-III - No Privilege, no sensitive information access

3. Given the direct supporting relationship, DON IT position levels have been aligned with DON sensitive national security position levels to satisfy the concurrent sensitive position and IT position designation requirements. This combined designation structure satisfies the intent of the national security position structure and the IT position designation structure, and is in keeping with the prerogative of the SECNAV to efficiently and consistently manage national security requirements.

4. 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 appropriate IT authority for IT positions. The commanding officer may establish standard operating procedures (SOP) to discharge this responsibility.

5. The sensitivity and IT level assigned will dictate the personnel security requirements; the greater the sensitivity, the greater the personnel security requirements. Position designations will be at the highest level required by the incumbent's specific duties. When the level of potential damage or privilege and other position characteristics appear to indicate differing levels of designation, the higher designation will always be used.

6. Sensitivity and IT position determinations will be recorded in JPAS (appendix E pertains).

a. Military members will be uniformly designated by community managers according to rating or military occupational specialty (MOS), and should only receive a unique command designation if the member is working outside of their rating or MOS, performing duties at the command that significantly exceed the sensitivity of their normally assigned rating or MOS duties.

b. Contracts involving DON IT systems or IT-related duties will incorporate the security requirements specified herein according to applicable policy and guidance sections of the Defense Federal Acquisition Regulations (DFAR).



c. Command security managers will maintain a separate record of position designation decisions for civilian personnel, identifying the sensitivity level, and listing the criteria most predominately responsible for the assigned sensitivity determination. Access to classified information will normally be predominating. A recommended format is provided in exhibit 5-A.

### 5-3 CRITERIA FOR DESIGNATING SENSITIVE POSITIONS

1. The following criteria for designating position sensitivity for DON employees is based on OPM and DoD criteria. The criteria for designating IT position sensitivity is based on OMB criteria, DoD criteria, and DON requirements:

a. **Special-Sensitive (SS)**: Any position which the head of the agency determines to be at a level higher than critical sensitive:

(1) Due to the greater degree of damage to the national security that an individual could effect by virtue of his/her position, or

(2) Special requirements concerning the position under authority other than EO 10450, such as designations applied under SSO cognizance pertaining to DCID 6/4.

(3) DAAs shall be designated as special-sensitive (SS), due to the degree of damage an individual could effect by virtue of his/her position, including those IT duties in which the incumbent has:

(a) Responsibility for planning, direction and implementation of a major (DON-wide or DoD-wide) IT security program; has responsibility for direction, planning, and design of a major (DON-wide or DoD-wide) computer system, including the hardware and software; or can access a major (DON-wide or DoD-wide) system during the operation or maintenance in such a way and with relatively high risk for causing inestimable damage or realizing extreme personal gain, or

(b) DAA.

b. **Critical-Sensitive (CS)**: Any position that 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 DON (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. (Fiduciary duties involving IT systems are also designated as IT positions as described below.)

(6) Certain IT positions will be designated as CS, and IT-I, due to the potential for grave damage to the national security. CS IT-I positions include those in which the incumbent has:

(a) Responsibility for development and administration of computer security programs, and also including direction and control of risk analysis and/or threat assessment.

(b) Been designated as IAM or IAO.

(c) Significant involvement in life-critical or mission-critical systems.

(d) Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.

(e) Relatively high risk assignments associated with or directly involving the accounting, disbursement or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by a higher authority in the IT-I category to insure the integrity of the system.

(f) Positions involving major responsibility for the direction, planning, design, testing, maintenance,

operation, monitoring and/or management of systems hardware and software.

(g) Other IT positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

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

c. **Noncritical-Sensitive (NCS)**: Any position that 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 marshal, duties associated with ammunitions and explosives).

(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) Responsibility for financial operations subject to routine supervision or approval, but with no funds disbursement or transfer capabilities. (Fiduciary duties involving IT systems are also designated as IT positions as described below.)

(6) Non-management DON mission support positions with authority for independent or semi-independent action.

(7) Duties involving delivery of service to support the DON mission requiring confidence or trust.

(8) Certain IT positions will be designated as NCS, and IT-II, due to the potential for serious damage to the national security. NCS IT-II positions include those in which the incumbent has:

(a) Responsibility for systems design, operations, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the CS

IT-I category.

(b) Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, and Government-developed privileged information involving the award of contracts; including user level access to DON or DoD networks and information systems, system security and network defense systems, or to system resources providing visual access and/or ability to input, delete or otherwise manipulate sensitive information without controls to identify and deny sensitive information.

(c) Duties associated with or directly involving the accounting, disbursement or authorization for disbursement of funds in dollar amounts of less than \$10 million per year; and/or duties that involve the development, writing and administration of, and/or awarding, approving or modifying of contracts which total dollar amounts less than \$10 million per year; or as deemed appropriate by the agency head those commensurate fiscal duties with potential for damage or personal gain.

(d) Other positions as designated by the agency head that involve a degree of access to a system that creates a potential for serious damage or personal gain less than that in CS IT-I positions.

d. **Non Sensitive (NS)**: Only those:

(1) Positions with limited relation to the DON mission, devoid of 5 CFR 732 security risk criteria and 5 CFR 731 public trust risk criteria will be designated as non sensitive.

(2) IT-III positions are designated as Non Sensitive (NS), and are dependent upon very rigorous IT controls to remain non-sensitive and to:

(a) Preclude access to system security and network defense systems, or to system resources;

(b) Preclude visual access to proprietary data, information requiring protection under the Privacy Act of 1974, government-developed privileged information involving the award of contracts, and other protected sensitive information.

(c) Preclude ability to input, delete or otherwise manipulate protected sensitive information.

(d) Except in those cases where sensitive information (e.g., privacy act data but not government furnished information) is stored in contractor-owned and operated computer networks and databases with no interconnection (including data feeds) to DON IT systems or networks, may use other safeguards as authorized by applicable guidance, in lieu of these position designation requirements.

2. Commanding officers are responsible for ensuring that positions that meet the above criteria are properly designated as sensitive. The majority of DON positions are sensitive due to the DON's national security mission.

#### **5-4 SUITABILITY AND SECURITY INVESTIGATION AND ADJUDICATION**

1. Personnel security investigations (PSI) are conducted to gather information for two purposes; to meet OPM requirements for accomplishing employment suitability determinations and to satisfy Executive Branch requirements for making personnel security determinations.

2. After determining the position sensitivity level, the appropriate investigation can be requested. The standards and requirements for PSIs are contained in paragraph 6-4 and exhibit 6A.

3. Upon completion, the investigation is adjudicated to determine suitability and security eligibility. The focus of *suitability* adjudication is whether the employment of an individual can reasonably be expected to promote the efficiency of the service. The focus of a personnel *security* adjudication is whether the assignment or continued assignment in a sensitive position, including sensitive IT positions, or authorization for access to classified information, can reasonably be expected to be clearly consistent with the interest of national security.

4. Employment suitability adjudications are based on standards and criteria established by EO 10450, and are normally made by the employing command. Personnel security determinations are based on criteria established by EO 12968, and found in appendix G, and are made by the DON CAF, as provided in paragraph 7-1.

5. OPM forwards all completed PSIs for DON personnel 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 on civilian personnel must be adjudicated by the command for suitability before the DON CAF security determination can be made. The following workflow procedures have been established to accomplish this requirement:

a. Investigations for non-sensitive or public trust positions will be forwarded to the command for the suitability determination. There is no adjudicative 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. A favorable security determination on a "No Actionable Issue" case will result in an automatic favorable suitability determination. The DON CAF will favorably adjudicate the investigation, as appropriate, and enter the favorable determination in JPAS, thus notifying the command of the favorable determination. The DON CAF will complete the OFI 79A accordingly and forward it to OPM Federal Investigative Services Division (FISD).

(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 will be returned to the DON CAF to make a security clearance eligibility determination. If the suitability determination made by the command is unfavorable, it remains a personnel action and no DON CAF action is required.

#### **5-5 SECURITY ADJUDICATION CRITERIA**

1. The national security adjudication criteria used to determine security clearance eligibility will likewise be applied by DON CAF to determinations of eligibility to occupy a sensitive national security position and a sensitive designated IT position. Assignment to sensitive positions is not authorized for individuals who have received an unfavorable clearance eligibility determination until the DON CAF reestablishes the eligibility.

2. Because the same standards, criteria and procedures are applied to both security clearance and sensitive position

eligibility adjudications, including IT sensitive positions, 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. Likewise, 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, including IT sensitive positions.

3. The prohibitions on security clearance eligibility imposed by the "Smith Amendment" and explained in paragraph 8-3 will likewise be considered to prohibit assignment to sensitive national security positions.

4. 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.

#### **5-6 CITIZENSHIP REQUIREMENTS**

1. Under EO 11935, "Citizenship Requirements for Federal Employment" September 2, 1976, only U.S. citizens may be employed in competitive service positions in the Federal civil service without approval from the OPM. In the absence of qualified available U.S. citizens, non-U.S. citizens may be given excepted service appointments (which do not qualify them for competitive civil service status, promotion or reassignment to another position in the competitive service). The excepted service appointment of a non-U.S. citizen requires approval from OPM and is subject to restrictions imposed by the appropriations act and the immigration law. OPM's employment approval relates to employability and does not consider national security requirements.

2. U.S. citizenship is a basic condition for access to classified information and assignment to a sensitive national security positions. Assignment of non-U.S. citizens in sensitive national security positions requires a waiver of this security standard. Commands considering waiver requests are strongly recommended to contact their resident NCIS Special Agent or servicing NCIS office to obtain a country specific Counter-intelligence (CI) briefing prior to submitting the waiver request. Requests for waiver of U.S. citizenship requirements for assignment to sensitive positions must be submitted to, and approved by, CNO (N09N2) prior to assignment. U.S. citizenship waiver procedures for appointment to sensitive

positions are provided in exhibit 5-B.

3. U.S. citizenship is a basic condition for assignment to a designated sensitive IT position. There are numerous impediments to permitting non-U.S. citizens to be assigned. Limitations on our ability to obtain background information from foreign countries to satisfy national background investigation requirements, disqualifying national security adjudicative criteria pertaining to foreign preference and foreign influence proclivities, and specific national security concerns and challenges related to the counterintelligence interests and priorities of foreign countries (dependent on the person's country of origin) must be considered.

a. DAA: Effective the date of this policy manual, DON non-U.S. citizen employees will NOT be permitted to be assigned or continue assignment to a special-sensitive DAA positions.

b. IT-I: Effective the date of this policy manual, DON non-U.S. citizen employees will NOT be permitted to be assigned to critical sensitive, IT-I, positions, and will NOT be permitted to function as IAM's, or IAO's. DON non-U.S. citizen employees encumbering designated IT-I positions will NOT be permitted to continue assignment unless a waiver request is forwarded to and approved by CNO (N09N2). U.S. citizenship requirements apply to DON employees and contractors assigned to designated IT positions. Waiver procedures are provided in exhibit 5-B.

c. IT-II: Effective the date of this policy manual, DON non-U.S. citizen employees will NOT be permitted to be assigned to noncritical sensitive, IT-II, positions.

d. IT-III: If access to DON IT systems for non-U.S. citizen employees is necessary in the furtherance of the DON mission, then IT-III restrictions will be employed to appropriately limit access to sensitive information. IT-III users will be strictly limited and contained and have access only to that information to which they are specifically entitled and nothing more. IT-III user access will be synonymous with technically prescribed need-to-know.

4. **Dual citizens**: U.S. citizens who are also dual citizens are not specifically excluded from occupying either sensitive or designated IT positions, however, a dual citizenship status raises foreign influence and foreign preference concerns that will likely prohibit interim assignment pending favorable investigation and adjudication of these issues. There are also



legal impediments to conducting PSIs in many foreign countries, which may impact the ability to gather sufficient information upon which to base a favorable personnel security determination.

5. Regardless of whether a non-U.S. citizen is permitted to occupy a sensitive or IT designated position on an approved waiver, non-U.S. citizens are not permitted access to classified IT systems or classified national security information or materials.

6. Foreign representatives are governed by foreign disclosure policies and procedures in SECNAVINST 5510.34A, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Representatives.

a. Foreign representatives include foreign exchange personnel and representatives of foreign nations, coalitions or international organizations considered for access to DON IT systems containing classified or sensitive information.

b. The requirement to integrate foreign exchange personnel into a host command does not include integration into IT systems.

c. Foreign exchange personnel do not fall under the waivers and exceptions process provided in exhibit 5-B. Applicable foreign disclosure requirements apply.

d. Mechanisms will be in place to strictly limit access to only that information which has been cleared for release to the represented foreign nation, coalition or international organization (e.g. for North Atlantic Treaty Organization see DoD Directive 5230.11, and for classified and other sensitive unclassified information see DoD Directive 5230.20 and DoD Instruction 5230.27.)

e. Procedures for sanitizing and configuring changes of automated IT systems must be employed to prevent unauthorized access to sensitive information by foreign nationals.

f. Direct the immediate revocation of access by foreign nationals to local area networks for which adequate controls to prevent unauthorized access to controlled unclassified or protected sensitive information have not been implemented.

g. Before authorizing foreign national access to specific information contained within an IT system, the host command will:

(1) Ensure the information is properly processed for disclosure,

(2) Ensure systems accreditations authorities concur with the access,

(3) Ensure the certification and accreditation documentation for the system is updated to reflect foreign national access, and

(4) Ensure security measures employed adhere to IT security and protection policy.

**EXHIBIT 5A**  
**Investigative Equivalency Table**  
**(For multiple requirements, highest prevails)**

<b>If Position Sensitivity, IT Designation or Access Requirement is:</b>	<b>... and the individual has had the following investigation (with no break in service &gt; 2 yrs):</b>	<b>... and the age of the investigation is :</b>	<b>...then the investigation request required to support the requirement is:</b>
-Special- Sensitive	SSBI , SSBI-PR, Full Field Investigation (FFI)	< 5 yrs	None
-Critical-Sensitive			
-IT-DAA	SSBI , SSBI-PR, FFI	> 5 yrs	SSBI-PR
-IT-I	SBI, BI, LBI, MBI, NACLCL, ANACI, NACI, NAC, NACIC, ENTNAC	Regardless of the age of the investigation	SSBI
-SCI Access			
-Top Secret Access	No previous investigation	N/A	SSBI
-Non-Critical Sensitive	SSBI, SSBI-PR, FFI, BI, MBI, LBI, NACLCL, ANACI	< 10 yrs	None (*See Note)
-IT-II			
-Secret Access	SSBI, SSBI-PR, FFI, BI, MBI, LBI, NACLCL ANACI , NACI, NACIC, NAC, ENTNAC	> 10 yrs	NACLCL (*ANACI for initial hire civilian)
	No previous investigation	N/A	NACLCL (*ANACI for initial civilian)
- Confidential Access	SSBI, SSBI-PR, FFI, SBI, BI, MBI, LBI, NACLCL, ANACI	< 15 yrs	None
	Any investigation	> 15 yrs	NACLCL (*ANACI for initial hire civilians)
-Non-Sensitive	Any investigation which substantially meets or exceeds the scope of the NACI is acceptable for assignment including SSBI, SSBI-PR, FFI, MBI, NACLCL, ANACI, NACIC, NACI	N/A	None
-IT-III			
-No Access	No previous investigation	N/A	NACI

\* EO 10450 requires "Written Inquiries" for all background investigations for initial suitability determinations for federal government civilian employees. The SSBI, SSBI-PR, LBI, MBI, NACI and ANACI all include "Written Inquiries", but the NACLCL does not. Although the basis requirement for assignment to IT-II and IT-III positions is the NACLCL, if the individual is a federal government civilian employee and they have not previously had an investigation, which includes the required "Written Inquiries," then an ANACI must be requested. An ANACI includes all elements of the NACLCL and also includes "Written Inquiries."

**EXHIBIT 5-B**

**U.S. CITIZENSHIP REQUIREMENT WAIVER PROCEDURES FOR PERSONS  
NOMINATED TO OCCUPY DON SENSITIVE  
AND INFORMATION TECHNOLOGY (IT) POSITIONS**

**5B-1 SENSITIVE POSITIONS WITHOUT IT DUTIES**

1. Requests for a waiver of the U.S. citizenship standard for persons nominated to occupy DON sensitive positions without IT duties will include:

a. The full identity of the applicant and the applicant's country of origin;

b. The original completed investigation request forms (SF 86, all releases and fingerprint cards) which CNO (N09N2) will review and forward to OPM, as appropriate;

c. A copy of the OPM employment approval or other documented authority under which the offer of employment to a non-U.S. citizen is permitted, indicating whether the proposed employee will be hired as excepted service, consultant, temporary employee, seasonal or other;

d. Documentation identifying the applicant's immigration status, alien residency and/or other visa status;

e. A detailed justification of the compelling reasons requiring assignment (to include special expertise) signed by the commanding officer;

f. A detailed description of the sensitive duties to be performed or sensitive information to be accessed, including all IT system accesses required;

g. A detailed description of the security measures and mechanisms in place to preclude the individual from having access to classified information and/or controlled unclassified information (CUI), and to address the security risks presented by NCIS during the country-specific counterintelligence briefing. Commands should consult with Navy IPO for additional guidance regarding foreign disclosure of CUI.

2. CNO (N09N2) will review and coordinate the request with the appropriate authorities to determine if sufficient justification

exists and if adequate security protections are in place. If the request conforms to employment and security requirements and is sufficiently consistent with the interests of national security, the requesting command will be advised and the request for investigation will be forwarded to OPM. Upon completion, investigations conducted on non-U.S. citizens occupying sensitive positions will be forwarded to CNO (N09N2) for the required personnel security determination. The command will be advised of the adjudicative results accordingly.

**5B-2 SENSITIVE IT POSITIONS**

1. In general, assignment to a designated IT position requires U.S. citizenship. Waivers may be requested as follows:

<b>Position Sensitivity Designation</b>	<b>Position IT Designation</b>	<b>US Cit Req'd</b>	<b>Waivers Permitted?</b>
Special Sensitive	DAA	Yes	No
Critical Sensitive	IT - I	Yes	For incumbents only - CNO (N09N2) approval required
Noncritical-Sensitive	IT - II	Yes	Infrequent - CNO (N09N2) approval required
Nonsensitive	IT-III	No	Not necessary, technical limitations and protections negate the ability to access sensitive information, and render the positions nonsensitive.

2. There are numerous impediments to permitting non-U.S. citizens to be assigned to designated IT sensitive positions. Limitations on our ability to obtain background information from foreign countries to satisfy national background investigation requirements, disqualifying national security adjudicative criterion pertaining to foreign preference and foreign influence proclivities, and specific national security concerns and challenges related to the counterintelligence interests and priorities of foreign countries (dependent on the person's country of origin) must be considered.

a. DAA: Effective the date of this policy manual, DON non-U.S. citizen employees will NOT be permitted to be assigned, or to continue assignment in DAA positions.

b. IT I: Effective the date of this policy manual DON non-U.S. citizen employees will NOT be assigned to designated IT-I positions, and will NOT be permitted to function as IAM's, or IAO's. Effective the date of this policy manual DON non-U.S. citizen employees encumbering designated IT-I positions will NOT be permitted to continue assignment unless a waiver request is forwarded to and approved by CNO (N09N2). The waiver request will include:

(1) A formal written approval for the assignment by the head of the DON activity that owns the system/information/network.

(2) A detailed justification for the waiver request including compelling need in the furtherance of the DON mission. (Compelling reasons may exist to grant such access in those circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed for a specific DoD requirement and for which a suitable U.S. citizen is not currently available.)

(3) An explanation of the intended transition plan to replace the non-U.S. citizen within five years, with a qualified employee.

(4) If an SSBI has not been recently performed on incumbent, an SSBI/SSBI-PR request will be prepared using an SF86, including a fingerprint card, which will be forwarded to CNO (N09N2) as part of the waiver request package. CNO (N09N2) will review and submit the investigation request to OPM, as appropriate.

(5) CNO (N09N2) waiver approvals will expire 5 years from date of issuance and cannot be renewed.

(6) By December 1 following the end of each fiscal year, the CNO (N09N2) will provide a report to the DUSD(CI&S), USD(I), containing the following:

(a) Number of non-U.S. citizens approved to continue to occupy IT-I positions, broken out by location, i.e., CONUS or OCONUS;

(b) For each location (CONUS or OCONUS), the number of individuals assigned to IT positions by nationality.

c. IT-II: Effective the date of this policy manual, DON will no longer permit the assignment of non-U.S. citizen employees to designated IT-II positions. Requests to waive the U.S. citizenship requirement for designated IT-II positions may be submitted to CNO (N09N2), and must include:

(1) A formal written approval for the assignment by the head of the DON activity that owns the system/information/network.

(2) A detailed justification for the waiver request including compelling need in the furtherance of the DON mission. (Compelling reasons may exist to grant such access in those circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed for a specific DoD requirement and for which a suitable U.S. citizen is not currently available.)

(3) A description of the protections implemented, to include the additional administrative, procedural, physical, communications, emanations, computer, information and personnel security measures implemented to minimize the risk (e.g., How the command plans to control and limit the access.)

(4) If an SSBI has not been recently performed on incumbent, an SSBI/SSBI-PR request will be prepared using an SF86, including a fingerprint card, which will be forwarded to CNO (N09N2) as part of the waiver request package. CNO will review and submit the investigation request to OPM, as appropriate. Interim assignment to IT-II positions for non-U.S. citizens is NOT authorized.

(5) After ensuring that the waiver request meets program parameters, CNO (N09N2) will forward the SSBI request to OPM. No waiver approval authorizations can be issued until favorable adjudication of the SSBI. CNO (N09N2) waiver approvals are valid for five years.

(6) Employees who are performing IT-II duties under waiver authority are not permitted to supervise other employees. Supervisors will be made fully aware of the limits to access(es) imposed and that physical custody of classified information by the non-U.S. citizen employee is not authorized.

d. IT-III: Due to the nature of IT-III user level access, waivers are not necessary.

## 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 Office of Personnel Management (OPM) 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. 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.m. 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 one year service remaining.



## 6-2 TYPES OF PERSONNEL SECURITY INVESTIGATIONS

1. The term "Personnel Security Investigation" (PSI) refers to an information gathering inquiry, where specified information is collected from specified sources to support eligibility determinations for 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 national security positions, 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. Exhibit 6A provides a table demonstrating the equivalency and acceptability of the various. PSIs, defined as follows:

a. **National Agency Check (NAC).** The NAC includes a search of DoD's Defense Clearance and Investigations Index (DCII), OPM's Reimbursable Suitability Investigation (RSI), Federal Bureau of Investigation (FBI) investigative and criminal history files including a technical fingerprint search and files of other federal government agency records as appropriate to the individual's background (Immigration and Naturalization Service (INS), Office of Personnel Management (OPM), Central Intelligence Agency (CIA), etc.). A NAC is an integral part of each Single Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), National Agency Check with Local Agency Check and Credit Checks (NACLIC), National Agency Check with Written Inquiries (NACI) and Access NACI (ANACI). A technical fingerprint search of the FBI files is conducted as part of a NAC, except during an SSBI-PR. Prior to implementation of EO 12968, reference (a) investigative standards for access to national security information, a NAC was conducted for officer commissioning determinations and provided the basis for access up to and including Secret classified information. Since implementation of reference (a), the NAC has continued to be used as the basis for trustworthiness determinations.

b. **National Agency Check with Written Inquiries (NACI).** The NACI is the basic EO 10450 investigative standard for federal government civil service employment suitability determinations. A NACI consists of a NAC plus. Written Inquiries to former employers and supervisors, to references, and to schools covering the previous. five years. NACI's are

insufficient for personnel security eligibility determination purposes or assignment to sensitive duties.

c. **Access NACI (ANACI).** The ANACI is an OPM product that combines the NACI (directed by EO 10450 to determine suitability of civilian employees within the Federal Government) and the NACLIC (directed by EO 12968 to determine security clearance eligibility). The ANACI meets the investigative requirements for appointment to non-critical sensitive positions and for access to Confidential or Secret national security information, for federal civilian employees. The ANACI includes a NAC, a credit check, and written inquiries covering the last five years to law enforcement agencies, to former employers and supervisors, to references, and to schools. (OPM also conducts a Minimum Background Investigation (MBI) and a Limited Background Investigation (LBI) for public trust purposes that are acceptable equivalents to the ANACI.)

d. **National Agency Check with Local Agency and Credit Checks (NACLIC).** The NACLIC is the basic EO 12968 standard for determinations of eligibility to access Confidential and Secret classified national security information. The NACLIC also provides the basis for military suitability determinations for Navy and Marine Corps enlisted members and officers. The NACLIC includes a NAC, credit bureau checks covering all locations where the subject has resided, been employed, or attended school for six months or more for the past seven years, and checks of law enforcement agencies having jurisdiction where the subject has resided, been employed, or attended school within the last five years.

e. **Single Scope Background Investigation (SSBI).** The SSBI is the EO 12968 investigative standard for determinations of eligibility to access Top Secret classified national security information and SCI access eligibility determinations. The SSBI is also the basis for determinations of eligibility to occupy a critical-sensitive or special-sensitive national security position and is required for duties involving a number of special programs. Individuals nominated for SCI access require a pre-nomination interview that is conducted by the SSO or its designee. The SSBI includes the NAC, verification of the subject's date and place of birth, citizenship, education and employment, neighborhood interviews, developed character reference interviews, credit checks, local agency checks, public record checks (i.e., verification of divorce, bankruptcy, etc.), foreign travel, foreign connections and organizational affiliations, with other inquiries, as appropriate. A formal subject interview is conducted, as applicable, as well as a NAC

of the subject's current spouse or cohabitant. The scope of an SSBI covers the most recent 10 years of the subject's life or from the 18th birthday, whichever is the shorter period; however, at least 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 (d) applies). (A Full Field Investigation (FFI) conducted by the FBI, State Department or U.S. Secret Service is usually equivalent to an SSBI.)

f. **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 SSBI Periodic Reinvestigation (SSBI-PR) completed to update requirements for Top Secret/SCI and other sensitive duties, and the NACLIC reinvestigation completed to update requirements for Secret or Confidential eligibility.

(1) **SSBI-PR:** SSBI-PRs are conducted on personnel whose clearance/access to SCI or Top Secret information is based on an investigation that is five years old or more. The SSBI-PR is also required to support personnel security determinations on personnel with continued assignment to NATO billets requiring Top Secret (COSMIC) access, Nuclear Weapons Personnel Reliability Program (PRP) critical positions, critical-sensitive and special-sensitive positions, IT-DAA and IT-I positions, Presidential Support Activities, access to SIOP-ESI, and for Limited Access Authorizations (LAAs) for non-U.S. citizens employees. The SSBI-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) **Phased PR (PPR):** A limited SSBI-PR, conducted under the same circumstances as an SSBI-PR, as warranted by the case. 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, local agency checks, developed character references, and additional investigation when warranted by the facts of the case. If

issues are developed during the fieldwork portion of any PPR, OPM will automatically expand the investigation coverage to full SSBI-PR coverage.

(3) **NACLC.** A NACLC is conducted at 10-year and 15-year intervals to support continued access to Secret and Confidential classified information, respectively. In the past, the NACLC reinvestigation was referred to as a Secret PR (SPR) or Confidential PR (CPR) by DSS, but it always included all the elements of the NACLC. NACLCs are also conducted at five-year intervals for personnel with Secret security clearance in Special Access Programs (SAPs) and those performing Explosive Ordnance Disposal (EOD) or Personnel Reliability Program (PRP) controlled duties. SPRs and CPRs with current eligibility determinations remain valid.

**g. Reimbursable Suitability/Security Investigation (RSI).**

An investigation conducted to resolve personnel security issues that arise after a PSI is conducted, evaluated or adjudicated. RSIs 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 "RSI" applies to limited inquiries, post-adjudication investigations or other additional inquiries conducted by OPM. RSIs do not cover investigations of criminal activity, sabotage, espionage, or subversion. Those are matters under the investigative jurisdiction of the NCIS. RSIs are requested and managed by the DON CAF.

**h. Entrance National Agency Check (ENTNAC).** An obsolete investigation previously conducted to support military suitability determinations for first-term enlistees in the Navy and Marine Corps. It included the basic elements of the NAC but it did not include a technical fingerprint search of FBI files. ENTNACs with current eligibility determinations may still be valid.

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 OPM, 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. **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 reference (d). 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 CLEARANCE ELIGIBILITY

1. Only U.S. citizens are eligible for security clearance. Guidance for validating citizenship status is found in appendix F.

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, SSBI-PR or PPR. For those who have continuous assignment or access to Top Secret, critical sensitive positions, SCI, Presidential Support Activities, COSMIC Top Secret, LAA, PRP, IT-1 duties or SIOP-ESI, the SSBI must be updated every five years by a PR.

b. **Secret/Confidential.** The investigative basis for Secret or Confidential clearance eligibility is a favorably completed NACLIC or ANACI. Clearance eligibility established based on ENTNAC's, NAC's or NACI's prior to NACLIC or ANACI implementation remain valid. For Secret and Confidential clearance, the investigation is updated every 10 and 15-years, respectively.

## 6-5 INVESTIGATIVE REQUIREMENTS FOR MILITARY MEMBERS

1. A NACLIC 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 NACLIC 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 NACLIC when a need exists, if the NACLIC has been initiated and the applicant has acknowledged in writing that, if the NACLIC 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 and forwarded with the SF 86 NACLIC.
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 CHNAVPERS and the CMC. Cases involving loyalty issues of DON personnel will be forwarded to CNO (N09N2) for referral to the Secretary of the Navy for action. Cases involving loyalty of U.S.MC personnel will be forwarded to HQMC (ARS).
5. A previously conducted PSI 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. DON CAF will adjudicate all investigations on military personnel using appendix G criteria. Issue cases that cannot be favorably resolved will be adjudicated as required by reference (a) and exhibit 6B. Investigative and adjudicative requirements for specific ratings or duties, assignments, and programs are found at exhibit 6B. Exhibit 6B requirements are used for PSI planning and programming. Any changes to exhibit 6B requirements must be coordinated, in advance, with CNO (N09N2).

8. **Mobilization.** For the purposes of partial or full mobilization under provisions of Title 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 CIVILIANS IN SENSITIVE POSITIONS AND ALL DON EMPLOYEES IN DON INFORMATION TECHNOLOGY (IT) POSITIONS**

1. U.S. citizenship is a basic condition for eligibility for assignment to a sensitive national security position. Guidance for validating citizenship status. is found in appendix F.

2. Determinations of eligibility for assignment to sensitive national security positions will be based on a PSI prescribed for the designated level of position sensitivity.

a. **Special-Sensitive/IT-DAA.** The investigative basis for assignment to a designated Special-Sensitive/IT-DAA position is a favorably completed and adjudicated SSBI, SSBI-PR, or PPR, in accordance with DCID 6/4. The SSBI must be updated every five years by an SSBI-PR.

b. **Critical-Sensitive/IT-I.** The investigative basis for assignment to a designated Critical-Sensitive/IT-I position is a favorably completed and adjudicated SSBI or SSBI-PR. The SSBI must be updated every five years by an SSBI-PR.

c. **Non-Critical Sensitive/IT-II.** The investigative basis for assignment to a designated Non-Critical Sensitive/IT-II position is a favorably completed and adjudicated ANACI for civilians or NACLIC for military/industry employees.

d. **Non-Sensitive/IT-III.** The investigative basis for assignment to a Non-Sensitive/IT-III position is an NACI.

3. A previously conducted ANACI or SSBI satisfies federal civilian employment suitability requirements for sensitive duty assignment provided there has been no break in service exceeding 24 months; however, a previously conducted NACLIC, ENTNAC or NAC will not (refer to exhibit 6A for investigative equivalencies). An ANACI or SSBI is required for reappointment to a federal government sensitive 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 SECNAV, 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 SECNAV 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.** An ANACI is the minimum requirement for civilian summer hires in all designated non-critical sensitive positions including summer hires, intermittent and seasonal appointees, or work/study and cooperative education program employees. To the extent possible, investigations requested to support sensitive duty assignment should be requested far enough in advance to allow completion and adjudication of the ANACI prior to assignment.

7. **Emergency Appointments.** If the appointee does not have the necessary investigative basis for appointment, he/she may be placed in a non-critical sensitive position only as an emergency measure after the commanding officer determines that delay in appointment would be harmful to the national security, the ANACI 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 NACLIC or ANACI that 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. Additional investigative requirements for assignment to selected job series or duties are established and authorized by chapter 5. Chapter 5 documents the requirements used for PSI planning and budgeting. Changes to chapter 5 must be coordinated, in advance, with CNO (N09N2).

10. **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 requiring access to classified information are managed under the National Industrial Security Program (NISP). Requests for investigation of contractor personnel for security clearance eligibility are processed by the OPM and adjudicated by Defense Industrial Security Clearance Office (DISCO). When SCI access is at issue, reference (d) applies. The DON CAF is the adjudicative authority for all DON contractor personnel requiring SCI access eligibility.

2. Contracts involving sensitive duties, and/or DON IT systems or IT-related duties should incorporate the security requirements specified herein according to applicable policy and guidance sections of the Defense Federal Acquisition Regulations (DFAR).

Non-NISP adjudications for contract personnel are done by the requesting command, using appendix G criteria.

3. Contractor employees who require access to DON controlled/restricted areas, NOT involving sensitive information or IT equipment and not involving access to classified information will be processed under the DON Facility Access Determination (FAD) Program. FAD program procedures are found in paragraph 9-20.

4. **Consultants Hired by a DON Government Contracting Activity (GCA)**. A consultant who is individually hired by a DON command or activity, 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 OPM and adjudicated by the DON CAF, as appropriate.

#### **6-8 SPECIFIC DUTY OR ASSIGNMENT REQUIREMENTS**

1. The following specific duties are assigned minimum investigative or clearance requirements in exhibit 6B and as follows:

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

b. **Personnel Security Clearance Adjudication Officials**. Any person selected to serve with a board, committee, or other group responsible for adjudicating personnel security cases shall have been the subject of a favorably adjudicated SSBI or SSBI-PR completed within the past five 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 SSBI-PR completed within the past five 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 NACLIC/ANACI 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 the appropriate security clearance eligibility established prior to accessing U. S. cryptographic information. 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 materials, require a favorably adjudicated SSBI or SSBI-PR completed within the past five years.

g. **Non-Appropriated Fund (NAF).** NAF employees assigned to positions of trust within DoD will be the subject of a favorably adjudicated NACI completed no greater than 24 months prior to appointment. A favorably completed prior investigation for Federal service which meets or exceeds the NACI standard 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. NAF employees requiring eligibility determination will be processed as prescribed by chapter 7. If access to a DON computer system and/or network is required, the position will be designated and the appropriate PSI will be submitted as directed by chapter 5.

h. **American Red Cross/United Service Organization (U.S.O).** A favorably adjudicated NAC is required on American Red Cross or U.S.O personnel as a prerequisite for assignment to activities overseas. If Red Cross or U.S.O 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 9-13.

i. **Chemical Agents.** Personnel whose duties involve access to or security of chemical agents require a favorably adjudicated NAC completed within the past five years before assignment.

j. **IT.** Employees assigned to IT-DAA designated positions require a favorably adjudicated SSBI or SSBI-PR to DCID 6/4 standards. IT-I designated positions require a favorably adjudicated SSBI or SSBI-PR. The SSBI or SSBI-PR requested for IT-DAA or IT-I positions will be updated every five years by an

SSBI-PR. Employees assigned to IT-II designated positions require a favorably adjudicated NACL/ANACI, which will be updated every ten years by a NACL. Employees assigned to IT-III designated positions require a favorably adjudicated NACI. Specific guidance regarding investigation requirements for IT designated positions, and the IT position sensitivity designation process can be found in chapter 5.

k. **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 NACL or ANACI.

l. **Contract Guards**. Contract guards require a favorably adjudicated NACL.

m. **Foreign Nationals Employed Overseas**. Certain record checks are required before a DON overseas command can employ a foreign national for non-sensitive 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 one year or more after age 18, the Federal Bureau of Investigation-Headquarters/Identification Division (FBI-HQ/ID).

n. **Nuclear Weapon Personnel Reliability Program (PRP)**. SECNAVINST 5510.35A, Nuclear Weapon Personnel Reliability Program (PRP), 26 June 2002, 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 which leads to PRP assignment. The investigative requirements for PRP assignment are based on the position designation. The PRP positions are designated as either **critical** or **controlled**.

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

(2) **Controlled PRP position.** The investigative requirement for initial assignment to a controlled PRP position is a favorably adjudicated NACLIC or ANACI completed within the past five years. The requirement may also be satisfied by a favorably adjudicated ENTNAC, NAC, or NACI completed prior to 26 June 2002, the effective date of SECNAVINST 5510.35A, but no older than five years from date of initial PRP assignment. An existing favorably adjudicated SSBI or SSBI-PR completed within the past five years will also suffice. When there is no investigation to satisfy the requirements for initial assignment, the command must request a NACLIC or ANACI, as appropriate. When requesting a new investigation, the request must be properly annotated to reflect PRP assignment. A NACLIC is required every five years for continued PRP assignment.

2. In addition to the above specific duties, there are minimum investigative and citizenship requirements for assignment to specified facilities necessitated by the nature of the command mission and operational structure. These specific facility requirements are unrelated to specific duties and are enumerated and authorized by chapter 5. Chapter 5 documents the requirements used for PSI planning and budgeting. Changes to chapter 5 must be coordinated, in advance, with CNO (N09N2).

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

#### **6-9 SPECIFIC PROGRAM 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 specifically determined by the SAP manager.

b. **Sensitive Compartmented Information (SCI).** The investigative requirement for access to SCI is a favorably adjudicated SSBI. A SSBI-PR is required to be submitted every five years. The requirements for SCI access are established under Director of National Intelligence (DNI) authority (reference (d) 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 July 1998 (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 five years to grant access to SIOP-ESI, providing a new SSBI or SSBI-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 September 1983, 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 spouse NAC must be requested.

e. **North Atlantic Treaty Organization (NATO).** An equivalent level U.S. security clearance is the basis for access to NATO classified information. OPNAVINST C5510.101D, NATO Security Procedures (U), 17 August 1982 (NOTAL), prescribes the policies and procedures for this program.

(1) The investigative basis for assignment to a NATO billet is a favorably adjudicated SSBI, SSBI-PR, ANACI or NACLIC, depending on the level of clearance and access the billet requires. The investigation must have been completed within the five years preceding the assignment. Continued assignment to a NATO COSMIC billet requires SSBI-PR every five years.

(2) For Navy military members under permanent change of station (PCS) orders to NATO billets, detailers will coordinate with the Naval Personnel Command (NAVPERSCOM) (PERS-483) to ensure that investigations are properly completed. PERS-483 provides policy manuals to ensure that proper investigation requests are submitted for NATO billet candidates. Policy will specify that the command may not execute the PCS orders until specifically released to do so by PERS-483, after verification of investigation and coordination with the DON CAF.

2. A listing of investigation and citizenship requirements for assignment to special programs is provided and authorized by chapter 5. Chapter 5 documents the requirements used for PSI planning and budgeting. Changes to chapter 5 must be coordinated, in advance, with CNO (N09N2).

3. This regulation is not the governing policy manual for the programs listed in this paragraph. Consult the governing policy for a full description of program requirements.

#### **6-10 RECIPROCITY AND ACCEPTABILITY OF PREVIOUSLY CONDUCTED INVESTIGATIONS**

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 by DON CAF. Exhibit 6A provides an equivalency table to assist

in determining if previously conducted investigations meet current requirements.

2. Before initiating a new investigation, command security personnel will search JPAS and other linked automated investigative indices, such as OPM's Special Investigative Inquiry (SII) and DoD's DCII, for evidence of a previously conducted investigation that meets requirements.

a. If subject provides information regarding a previous investigation conducted by an agency other than OPM or DoD, this information must be verified by the DON CAF using a JPAS RRU request to DON CAF. Advise DON CAF via JPAS of the adjudicative requirements, and provide the information regarding subject's previous investigation. DON CAF will verify and respond regarding eligibility and investigative reciprocity.

b. If no record is found of an equivalent investigation, a new investigation will be requested.

3. Adjudicative agencies and commands will not request previous investigative files for adjudicative review unless:

a. The previous investigative file was never properly adjudicated;

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

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

d. The individual is being considered for a higher level of clearance eligibility by the DON CAF, or other official command program requirements.

4. When DON personnel are assigned or detailed to other Federal agencies (e.g., DOE, NRC, etc.), the entity exercising administrative jurisdiction will be responsible for initiating the required personnel security investigation. The completed investigation for all DON personnel will be forwarded to the DON CAF for a security clearance eligibility determination.

5. Conversely, when it becomes necessary for a commanding officer to grant access to personnel from other military departments or DoD agencies who do not have the required security clearance eligibility, the DON command granting access will submit a request for investigation to OPM indicating that



the results are to be forwarded to the individual'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. **Review of Prior Investigations.** Prior PSIs may only be requested for review in support of an official requirement.

a. Official command requirements include higher level of special access, critical PRP positions, or assignment to higher level sensitive duties; acceptance or retention in the Armed Forces; or appointment or retention in civilian employment.

b. All requests must be fully justified and forwarded to Director, Naval Criminal Investigative Service, Code 11C1, Records Management/DON Liaison Office, Building 111, Washington Navy Yard DC 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 explain that the request is not to support a clearance or SCI access adjudication, as only DON CAF is permitted to request investigation for this purpose.

#### **6-11 LIMITATIONS ON REQUESTS FOR INVESTIGATION**

1. PSIs for purposes other than allowed by this policy manual regulation are not authorized unless detailed justification has been submitted to CNO (N09N2) and approved by U.S.D(CI&S).

2. Before requesting an investigation, activities must determine that the individual does not have an investigation that 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 one year service remaining.

#### **6-12 COMMAND RESPONSIBILITIES IN PSI 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. Ensure the investigative requirements for military and civilian employees are accurately recorded in appropriate personnel systems. This data will be used for programming and to validate electronic PSI requests.

b. **Local Records Check (LRC).** Check locally available records (such as personnel, medical, legal, security, base/military police, etc.) 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.

c. **Validate Citizenship.** For individuals who are born outside the United States, extra coverage codes will be entered on the investigative request forms to ensure OPM accomplishes the citizenship validation in accordance with national standards. Commands will also validate citizenship of individuals before submitting initial PSI requests. (Only U.S. citizens are eligible for security clearance or assignment to a sensitive national security position.) Procedures for validating citizenship are contained in appendix F.

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 through review of available personnel records. However, for education verification, extra coverage codes will be entered on investigative request forms to ensure OPM accomplishes the education validation in accordance with SSBI standards. This is not necessary when requesting a NACL/ANACI.

e. Ensure the investigation request is completed and prepared using current guidance to preclude rejection by OPM. Current directions for completing investigation requests can be found at the CNO(N09N2) web site, [www.navysecurity.navy.mil](http://www.navysecurity.navy.mil).

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

3. **Pre-Nomination Interview.** Before a request for an SSBI for SCI access is submitted to OPM, 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 personnel security request form (SF 86), will be explained in a written report that identifies the interviewer and is attached to the SSBI submission (refer to reference (d)). Note: Individuals who are in or selected for command status. (Commanding Officer/Executive Officer) do not require a pre-nomination interview.

## 6-13 PERSONNEL SECURITY INVESTIGATION REQUEST FORMS

1. **Electronic Questionnaires for Investigations Processing (e-QIP).** E-Qip is the federal government standard automated request tool for personnel security investigations (PSI). E-QIP is part of the e-government, e-clearance initiative sponsored by the OPM. E-QIP allows applicants to electronically enter, update, and transmit their personal investigation data over a secure Internet connection to their employing agency or security management office for review and approval in conjunction with the PSI request. Within DoD, e-QIP will only be accessed through JPAS. In DoD, e-QIP will eventually replace the Electronic Personnel Security Questionnaire (EPSQ) and the Standard Form 86, "Questionnaire for National Security Positions." Additional information regarding system use and requirements will be published upon full deployment.

2. **Electronic Personnel Security Questionnaire (EPSQ).** DoD's electronic PSI request tool developed to support Defense Security Service (DSS) investigation request processing has been authorized for use by OPM in the interim, while awaiting e-Qip deployment. Since DSS transferred its PSI mission to OPM in February 2005, EPSQ's can no longer be sent electronically via DSS. As an interim measure, OPM permits DoD activities to mail paper copies of completed and validated EPSQ's, along with Agency use Information, signed release forms and completed fingerprint cards to OPM, to request PSIs. Directions on requesting personnel security investigations from OPM using EPSQ are on the CNO (N09N2) web page at [www.navysecurity.navy.mil](http://www.navysecurity.navy.mil).

3. **Standard Form (SF) 86, "Questionnaire for National Security Positions."** The Standard Form 86 is the currently approved method of requesting PSI products from OPM to support determinations of eligibility for assignment to sensitive national security positions or access to classified national security information. The subject of the investigation completes the SF 86. The Agency Use information and the release forms are imbedded in the SF 86. Requesting commands must attach a completed SF 87 fingerprint card to each request, except for the SSBI-PR. Directions for completing and mailing investigation request packages using the SF 86 are on the CNO (N09N2) web page at [www.navysecurity.navy](http://www.navysecurity.navy).

## 6-14 PREPARATION AND SUBMISSION OF INVESTIGATION REQUESTS

1. The OPM Federal Investigative Services Division (FISD) will accept PSIs submitted electronically via e-QIP or in hardcopy using approved Standard Forms: Standard Form (SF) 86,

Questionnaire for National Security Positions; SF 85P, Questionnaire for Public Trust Positions; SF 85, Questionnaire for Non-Sensitive Positions; and the SF 86A, Continuation Sheet for Questionnaires SF 86, SF 85P and SF 85 when additional space for documentation is required, or printed EPSQ requests. Additionally, the SF 87, OPM Fingerprint Card, and FD 258, Applicant Fingerprint Cards are also required with all requests, except for the SSBI-PR. Details for procuring investigation request forms are provided at exhibit 6B.

2. Directions for completing, preparing and transmitting PSI requests forms are on the CNO (N09N2) web page at [www.navysecurity.navy.mil](http://www.navysecurity.navy.mil). It is very important to follow request directions precisely, especially the directions regarding the "Agency Use" coding, as failure to properly code request will result in returned requests.

a. **NAC** - When requested for trustworthiness determinations: Use the SF 85P, Questionnaire for Public Trust Positions, and an SF 87, Applicant fingerprint card, and mail to OPM.

b. **NACI** - When requested to support suitability determinations for civilian employees assigned to non-sensitive or low risk public trust duties: Use the SF 85, the SF 87, a resume or equivalent and an OF 306, Declaration for Federal Employment.

c. **ANACI** - Required to support suitability determinations for civilian employees initially assigned to non-critical sensitive positions with or without access to classified information: Use the SF 86, Questionnaire for National Security Positions, and the SF 87, Applicant fingerprint card, and mail to OPM. A printed EPSQ may be used in lieu of the SF 86, but an Agency Use Form and the signed release forms, the SF 87, Applicant fingerprint card, a copy of the resume, and a copy of the completed OP-306, must be attached. Detailed directions are provided on the CNO (N09N2) web page at [www.navysecurity.navy.mil](http://www.navysecurity.navy.mil).

d. **NACLC** - Required to support suitability determinations on military officer accessions and initial and continued Secret and Confidential security clearance determinations: Use the SF 86 and SF 87.

e. **SSBI** - Required to support security and suitability determinations for civilian employees in special-sensitive or critical-sensitive positions, and to support security

determinations for DON employees requiring access to Top Secret/SCI information and other identified programs: Use the SF 86 and an FD 258 fingerprint card.

f. **SSBI-PR** - Required to support the continuous evaluation of civilian employees assigned to designated special sensitive or critical sensitive positions and DON employees with access to Top Secret/SCI information and/or other identified programs requiring a SSBI-PR: Use the SF 86 (fingerprint cards are not required).

g. **RSI** - Required to prove or disprove allegations concerning an individual on whom adverse information has been developed and received by the DON CAF subsequent to a favorable security eligibility determination. If deemed appropriate, RSIs are requested by the DON CAF to OPM after coordination with the command. Commands will obtain the SF 86 as directed by DON CAF.

#### **6-15 PRIORITIZING INVESTIGATION REQUESTS**

1. The OPM is the investigative service provider for all DoD PSIs. OPM offers fee for service products with additional costs for priority processing. The DON centrally funds the PSP, and has allocated resources for the following:

a. **Standard Service SSBI**s for critical sensitive positions, Top Secret security clearance, and SCI access determinations. Use service code "**30C.**"

b. **Standard Service SSBI-PR**s for reinvestigating personnel in critical sensitive positions, requiring Top Secret security clearance eligibility and SCI access. Use service code "**18F.**"

c. **Standard Service NACL**C and **Secret-PR** for initial Secret and Confidential security clearance and military accessions and for reinvestigation of all personnel with Secret and Confidential security clearance. Use service code "**08B.**"

d. **Standard Service ANACI** for civilians assigned to non-critical sensitive positions and for initial Secret and Confidential security clearance determinations. Use service code "**09B.**"

2. OPM will only process requests using the service codes listed above as the DON has not authorized funding to conduct "Expedited" or "Priority" service investigations. Requests forwarded with unauthorized service codes will be returned or

rejected.

3. If a mission critical requirement exists for other than standard service, CNO (N09N2) can negotiate priority processing for requests with OPM.

a. Requests that justify priority-processing expense are those in which the subject of the investigation cannot perform assigned duties until the investigation is completed and adjudicated. The vast majority of positions and duties can be performed on an interim or temporary basis while awaiting the results of investigation, so the Departmental requirements for priority processing are minimal.

b. To request priority processing authorization, contact CNO (N09N2) at DSN: 288-8858. You must cite the policy requirement that prevents use of interim or temporary access or assignment to perform assigned duties and necessitates priority service expenditures. Requests for priority processing of Marine Corps investigations will be submitted via HQMC (ARS) at (703) 614-2320 or DSN 224-2320.

#### **6-16 MAINTAINING QUESTIONNAIRE INFORMATION**

1. A tickler copy of the above requests will be locally retained, to include copies of the completed questionnaire, to enable future tracer actions. Commands must ensure appropriate protection of completed questionnaires and will ensure copies are destroyed when DON CAF adjudicative action is complete.

2. Requesting an individual to prepare a questionnaire for PSI purposes using either electronic questionnaires or paper forms constitutes solicitation of personal information that 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 investigation purposes, after being advised of the effect of refusal, commands will terminate the PSI request process and notify DON CAF via RRU. The individual will not be eligible for access to classified information or assignment to sensitive duties unless the information is made available. Personnel indoctrinated for SCI access will be debriefed for cause (refer to reference (d)).

## 6-17 FOLLOW-UP ACTIONS ON INVESTIGATIVE REQUESTS

1. **Rejection of Investigation Requests.** When an investigation request is rejected by OPM because the request was not properly prepared, commands must take immediate corrective action 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. **Request Follow-up.** Commands are required to monitor requested investigations to ensure they are initiated, completed and adjudicated as required. JPAS provides the status of investigations and should be consulted within 30 days of submission of request to ensure the request is initiated. If JPAS reflects the investigation is still pending, query OPM for status. If JPAS reflects the investigation closed at least 3 months ago and you have not received an adjudication decision, a query to the DONCAF is appropriate.
3. **Cancellation of Investigation Requests.** When an investigation is in a pending status and the subject is being released from active duty, discharged, is resigning, or circumstances permanently change to negate the need for the investigation, the command will notify the DON CAF immediately. The DON CAF will direct OPM, as appropriate, to cancel the investigation.
4. **NACLC Follow-up.** A NACLC must be completed on each first-term enlistee to support a military suitability determination. If a first-term enlistee is received without evidence of a completed or pending NACLC, the gaining command must ensure the NACLC is requested regardless of current assignment requirements.

## 6-18 PROCESSING COMPLETED REPORTS OF INVESTIGATION

1. All PSIs requested to support eligibility determinations on DON employees are forwarded to the DON CAF, when complete, for adjudication. The DON CAF will make the required eligibility determination based on the requirements identified on the PSI request.
  - a. When the PSI contains information that requires expansion, adjudication of the PSI will be held in abeyance pending completion of the additional investigative leads.

Temporary access may not continue in these situations.

b. Initial investigations on civilians 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 completed 79A must be returned to the DON CAF for a security determination.

c. Commands will consult JPAS to determine when investigations are completed and when DON CAF adjudication is concluded. Commands must ensure they have properly registered the persons under their control in JPAS so they receive pertinent information and notices.

2. Investigations requested to support trustworthiness determinations and non-sensitive position assignments are not adjudicated by the DON CAF. The DON CAF forwards these investigations to commands for the appropriate trustworthiness and suitability determinations.

#### **6-19 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 that 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 DU.S.D (CI&S) 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 OPM investigations may not be released outside DoD without the specific approval of OPM.

EXHIBIT 6A

<b>PSI REQUIREMENTS BY NAVY DESIGNATOR/RATING</b>			
<b>OFFICER</b>			
<b>OFFICER DESIGNATOR</b>		<b>Required Investigation</b>	<b>Clearance Eligibility Adjudication Required</b>
1000	Unrestricted Line Officer	NACLC	YES
1020	Unrestricted Line Officer - Special Duty Officer	NACLC	YES
1050	Unrestricted Line Officer - Warfare (LT or Above)	NACLC	YES
1100	Unrestricted Line Officer - Fleet Support	NACLC	YES
1110	Unrestricted Line Officer - Surface Warfare	SSBI	YES
1110	Surface Warfare	SSBI	YES
1120	Unrestricted Line Officer - Submarine Warfare	SSBI	YES
1120	Submarine Warfare	SSBI	YES
1130	Unrestricted Line Officer - Special Warfare	SSBI	YES
1130	Special Warfare	SSBI	YES
1140	Special Operations	SSBI	YES
1140	Surface Warfare Training	SSBI	YES
1160	Surface Warfare Training	SSBI	YES
1170	Submarine Warfare Training	SSBI	YES
1180	Special Warfare Training	SSBI	YES
1190	Special Operations Training	SSBI	YES
1300	Air Warfare, Other Than Operational (OTO) (Code 0)	NACLC	YES
1301	Operational Flying Pilot or NFO (LT or above) (Code 1)	NACLC	YES
1302	Operational Flying pilot or NFO (Code 2)	NACLC	YES
1310	OTO Pilot (Code 0)	NACLC	YES
1311	Operational Flying Pilot (Code 1)	NACLC	YES
1312	Operational Flying Pilot (Code 2)	NACLC	YES
1320	Naval Flight Officer (NFO) , OTO (Code 0)	NACLC	YES
1321	NFO (Code1)	NACLC	YES
1322	NFO (Code 2)	NACLC	YES
1372	(NFO) Training	NACLC	YES
1392	(Pilot) Training	NACLC	YES
1440	Engineering (1440 process)	SSBI	YES
1460	Engineering (1440 process)	SSBI	YES
1500	Aerospace Engineering (CAPT and above)	SSBI	YES
1510	Aerospace Engineering Duty (AED)	SSBI	YES
1511	AED (Code 1) Operational Flying Pilot or NFO	NACLC	YES
1512	AED (Code 2) Operational Flying Pilot or NFO	NACLC	YES
1520	AED Aerospace Maintenance (AMD)	NACLC	YES
1540	Aviation Duty Officer (ADO) (Code 0)	NACLC	YES

1541	Aviation Duty Officer (ADO) (Code 1) (LT - CAPT)	NACLCL	YES
1542	Aviation Duty Officer (ADO) (Code 2) (LT - CAPT)	NACLCL	YES
1600	Information Professional - Special Duty Officer	SSBI	YES
1610	Cryptology - Special Duty Officer	SSBI	YES
1620	Merchant Marine - (Deck) Special Duty Officer	NACLCL	YES
1630	Intelligence - Special Duty Officer	SSBI	YES
1650	Public Affairs - Special Duty Officer	SSBI	YES
1670	Merchant Marine - (Engineering) Special Duty Officer	SSBI	YES
1800	Oceanography - Special Duty Officer	NACLCL	YES
1802	Meteorology/geophysicist - Operational Flying Pilot/NFO	NACLCL	YES
1900	Prospective Nurse Corps Officer	NACLCL	YES
1910	Prospective Medical Corps Officer (Sr. Medical Student Program)	NACLCL	YES
1920	Prospective Dental Corps Officer	NACLCL	YES
1930	Prospective Medical Service Officer (Optometry)	NACLCL	YES
1950	Prospective Judge Advocate General Corps Officer (LEP)	NACLCL	YES
1960	Prospective Medical Corps Officer (Med/Ost School Program)	NACLCL	YES
2000	Med. Dept. (Med. Admin.) Officer billet	NACLCL	YES
2100	Staff Corps Officer (Req. Medical Specialty)	NACLCL	YES
2102	Staff Corps Officer billet (Code 2) Op Flying	NACLCL	YES
2200	Staff Corps Officer billet requires Dental Specialty	NACLCL	YES
2300	Staff Corps Off (Code 2) Medical Service Corps Officer	NACLCL	YES
2302	Staff (Code 2) Op flying qualifications Aviation Phys/Exp Psych	NACLCL	YES
2500	Staff Corps. Officer Billet (requires Law Specialty)	NACLCL	YES
2900	Staff Corps. Officer Billet (requires Nursing Specialty)	NACLCL	YES
3100	Staff Corps. Officer Billet (requires Supply Specialty)	SSBI	YES
4100	Staff Corps Officer Billet (requiring Chaplain Specialty)	NACLCL	YES
5100	Staff Corps Officer Billet (requiring Civil Eng. Specialty)	SSBI	YES
6000	Billet filled with any appropriate skilled and LDO	NACLCL	YES
6110	LDO (Line) billet req. management in Deck Specialist (Surface)	NACLCL	YES
6120	LDO (Line) billet req. management in Operation Specialist (Surface)	NACLCL	YES
6130	LDO (Line) billet req. management in Eng/Rep. Specialist (Surface)	NACLCL	YES
6150	LDO (Line) billet req. management in Spec. Warfare Tech. Specialty	SSBI	YES
6160	LDO (Line) billet req. management in Ordnance Specialist (Surface)	NACLCL	YES
6180	LDO (Line) billet req. management in Elec. Specialist (Surface)	NACLCL	YES
6210	LDO - Deck Specialty (Submarine)	SSBI	YES
6230	LDO - Engineering Repair Specialty (Submarine)	SSBI	YES
6260	LDO - Ordnance Specialty (Submarine)	SSBI	YES
6280	LDO - Electronics Specialty (Submarine)	SSBI	YES
6290	LDO - Communications (Submarine)	SSBI	YES
6310	LDO - Aviation Deck Specialty	NACLCL	YES
6320	LDO - Aviation Operations Specialty	NACLCL	YES
6321	LDO - Aviation Operations, Operational Flying (Code 1)	NACLCL	YES
6330	LDO - Aviation Maintenance Specialty	NACLCL	YES

6360	LDO - Aviation Ordnance Specialty	NACLCL	YES
6380	LDO - Avionics Specialty	NACLCL	YES
6390	LDO - Air Traffic Control	SSBI	YES
6400	LDO - Nuclear Power	SSBI	YES
6410	LDO - Admin Specialty	NACLCL	YES
6420	LDO - Information System	SSBI	YES
6430	LDO - Bandmaster	NACLCL	YES
6440	LDO - Cryptologic	SSBI	YES
6450	LDO - Intelligence Specialty	SSBI	YES
6470	LDO - Photography Specialty	NACLCL	YES
6480	PLDO - Explosive Ordnance Disposal	NACLCL	YES
6490	LDO - Security Specialty	SSBI	YES
6510	LDO - Staff Corps Supply Specialty	SSBI	YES
6530	LDO - Staff Corps Civil Engineer	NACLCL	YES
6550	LDO - Staff Corps Paralegal	NACLCL	YES
7110	WO - Boatswain Specialist (Surface)	NACLCL	YES
7120	WO- Operations Technician Specialty (Surface)	NACLCL	YES
7130	WO - Engineering Specialty (Surface)	NACLCL	YES
7140	WO - Repair Technician Specialty (Surface)	NACLCL	YES
7150	WO - Special Warfare Technician Specialty	SSBI	YES
7160	WO - Ordnance Technician Specialty	NACLCL	YES
7170	WO - Specialty Warfare Combatant (Craft Crew)	NACLCL	YES
7180	WO - Electronics Technician (Surface)	NACLCL	YES
7200	WO - Diving Officer	SSBI	YES
7210	WO - Boatswain Specialty (Submarine)	SSBI	YES
7230	WO - Engineering Specialty (Submarine)	SSBI	YES
7240	WO - Repair Tech Specialty (Submarine)	SSBI	YES
7260	WO - Ordnance Tech Specialty (Submarine)	SSBI	YES
7280	WO - Electronics Tech Specialty (Submarine)	SSBI	YES
7310	WO - Aviation Boatswain Specialty	NACLCL	YES
7320	WO - Aviation Operations Technician	NACLCL	YES
7321	WO - Aviation Operations Technician (Operational Flying Code 1)	NACLCL	YES
7340	WO - Aviation Maintenance Technician Specialty	NACLCL	YES
7360	WO - Aviation Ordnance Technician Specialty	NACLCL	YES
7380	WO - Aviation Electronics Technician	NACLCL	YES
7400	WO - Nuclear Power Technician Specialty	SSBI	YES
7410	WO - Ships Clerk Specialty	NACLCL	YES
7420	WO - Communications and INFOSEC	SSBI	YES
7440	WO - Cryptologic Technician Specialty	SSBI	YES
7450	WO - Intelligence Technician Specialty	SSBI	YES
7470	WO - Photographer Specialty	NACLCL	YES
7480	WO - Ordnance Disposal Technician	SSBI	YES
7490	WO - Security Technician Specialty	SSBI	YES

7510	WO - Supply Corps Specialty	SSBI	YES
7520	WO - Food Service Specialty	NACLCL	YES
7530	WO - Civil Engineer Specialty	SSBI	YES
7560	WO - Tech Nurse Specialty	NACLCL	YES
<b>ENLISTED RATING</b>			
<b>AVIATION MAINTENANCE</b>			
AB	Aviation Boatswain's Mate	NACLCL	YES
ABE	Launch/Recovery	NACLCL	YES
ABF	Fuels	NACLCL	YES
ABH	Aircraft Handler	NACLCL	YES
AD	Aviation Machinist's Mate	NACLCL	YES
AV	Aviation Electronic, Electrical & COMPSYSTECH	NACLCL	YES
AE	Aviation Electrician	NACLCL	YES
AT	Aviation Electronics Technician	NACLCL	YES
AM	Aviation Structural Mechanic	NACLCL	YES
AME	Safety Equipment	NACLCL	YES
AO	Aviation Ordnanceman	NACLCL	YES
AS	Aviation Support Equipment Technician	NACLCL	YES
AZ	Aviation Maintenance ADMINMAN	NACLCL	YES
PR	Aircrew Survival EQUIPMENTMAN	NACLCL	YES
<b>AIR CREW OPS</b>			
AC	Air Traffic Controller	NACLCL	YES
AG	Aerographers Mate	NACLCL	YES
AIRC	Air Crew	NACLCL	YES
AIRR	Air Crew Rescue Swimmer	NACLCL	YES
<b>SUPPLY</b>			
DK	Disbursing Clerk	NACLCL	YES
CS	Culinary Specialist (Surface)	NACLCL	NO
PC	Postal Clerk	NACLCL	YES
SH	Ships Serviceman	NACLCL	YES
SK	Storekeeper (Surface)	NACLCL	YES
SK	Storekeeper (Submarine)	NACLCL	YES
<b>ADMIN/ MEDIA</b>			
DM	Illustrator-Draftsman	NACLCL	YES
JO	Journalist	NACLCL	YES
LI	Lithographer	NACLCL	YES
MU	Musician	NACLCL	NO
PH	Photographers Mate	NACLCL	YES
PS	Personnel Specialist	NACLCL	YES
RP	Religious Program Specialist	NACLCL	YES
YN	Yeoman	NACLCL	YES
PS	Personnel Specialist	NACLCL	YES

MC	Mass Communication Specialist	NACL	YES
<b>LEGAL/LAW ENFORCEMENT</b>			
LN	Legalman	NACL	YES
MA	Master at Arms	SSBI	YES
<b>SUBMARINE ELECTRONICS/ COMPUTER</b>			
ETR	Electronics Technician	SSBI	YES
ETV	Electronics Technician	NACL	YES
FT	Fire Control	SSBI	YES
STS	Sonar Technician	NACL	YES
SN	Seaman	NACL	YES
MS	Mess Specialist	NACL	YES
MT	Missile Technician	SSBI	YES
YN(SS)	Yeoman	NACL	YES
MA	Master at Arms	NACL	YES
MM(SS)	Machinist Mate	SSBI	YES
SK	Storekeeper	NACL	YES
<b>MEDICAL/ DENTAL</b>			
DT	Dental Technician	NACL	YES
HM	Hospital Corpsman	NACL	YES
<b>SURFACE COMBAT SYSTEMS</b>			
TM	Torpedoman's Mate	NACL	YES
STG	Sonar Technician	NACL	YES
MN	Mineman	NACL	YES
AECF	Electronics Technician	NACL	YES
AECF	Fire Control Technician	NACL	YES
GM	Gunners Mate	NACL	YES
<b>NUCLEAR FIELD</b>			
ET	Electronics Technician	NACL	YES
EM	Electrician's Mate	NACL	YES
MM	Machinist Mate	NACL	YES
<b>INTELL/CRYPTO</b>			
IS	Intelligence Specialist	SSBI	YES
CTA	Cryptologic Technician Administrative	SSBI	YES
CTI	Cryptologic Technician Interpretive	SSBI	YES
CTM	Cryptologic Technician Maintenance	SSBI	YES
CTO	Cryptologic Technician Communications	SSBI	YES
CTR	Cryptologic Technician Collection	SSBI	YES
CTT	Cryptologic Technician Technical	SSBI	YES

<b>SURFACE OPERATIONS</b>			
OS	Operations Specialist	NACLC	YES
QM	Quarter Master	NACLC	YES
BM	Boatswain Mate	NACLC	YES
IT	Information Systems Technician	SSBI	YES
<b>SEAL/SWCC/ EOD/DIVER</b>			
SEAL	Sea Air and Land	NACLC	YES
SWCC	Special Warfare Combat Crew	NACLC	YES
EOD	Explosive Ordnance Disposal	NACLC	YES
DIVER	Navy Diver	NACLC	YES
<b>SEABEES</b>			
BU	Builder	NACLC	NO
CE	Construction Electrician	NACLC	NO
CM	Construction Mechanic	NACLC	NO
EA	Engineering Aid	NACLC	NO
EO	Equipment Operator	NACLC	NO
UT	Utilitiesman	NACLC	NO
SW	Steelworker	NACLC	NO
<b>SURFACE HULL &amp; ENGINEERING</b>			
DC	Damage Controlman	NACLC	YES
EN	Engineman	NACLC	YES
EM	Electricians Mate	NACLC	YES
HT	Hull Maintenance Technician	NACLC	YES
IC	Interior Communications Electrician	NACLC	YES
MR	Machinery Repairman	NACLC	YES
MM	Machinist Mate	NACLC	YES
GSE	Gas Turbine Systems Technician	NACLC	YES
GSM	Gas Turbine Systems Mechanic	NACLC	YES
<b>MISC</b>			
CMDCM	Command Master Chief Rating	NACLC	YES

**SSBI REQUIREMENTS BY DEPARTMENT OF THE NAVY FACILITY**

<b>UIC</b>	<b>COMMAND</b>
00015	ONI WASHINGTON DC
30199	ONI LIAISON OFF/JOSIC NW UK
30689	ONI NORTHWEST REGIONAL NIC
30692	ONI SPINTCOMM VQ-2 ROTA SPAIN
30735	ONI LIAISON OFFICE ROME IT
30879	DNI BUPERS SPT MILLINGTON TN
30906	ONI SP/SSO CINCUSNAVEUR
30965	ONI LIAISON OFF/ESQUIMALT BC
30975	ONI LIAISON OFF/HALIFAX NOVA S
30980	ONI SSO NORFOLK VA
31193	ONI SPINTCOMM SUITLAND MD
31215	ONI SSO WESTPAC
31221	ONI SPINTCOMM DIV SUITLANT
31269	ONI LIAISON OFFICE OSLO NORWAY
3130B	ONI NAVAL PROGRAM SUPPORT ACT
31712	ONI SP/SSO COMSBPAC REP WC INT
31716	MCIA DET NGIC CHARLOTTESVILLE
31717	MCIA DET CAMP COURTNEY OKINAWA
3183A	ONI DET INDIAN HEAD MD
32043	ONI SP CDR NAVEUR NAPLES ITALY
32661	OST TECHNOLOGY HAZ MAT TRN OFF
32665	ONI SP/SSO JIATF-EAST KEY WEST
32666	ONI CNO SSO
32774	ONI SP/SSO COMPHIBGRU 1 OKIJAP
32998	ONI SUPPORT CENTER OP SDC
33168	ONI SP COMTHIRDFLT SAN DIEGO
3322A	ONI MASINTDET CMO
33300	ONI SP COMSUBPAC PEARL HARBOR
3437B	ONI DETACHMENT FORT SHERIDAN
3461B	ONI SP SWA BAHRAIN DMS LEVEL 2
35100	ONI SSO WHIDBEY
35216	ONI JOINT TRAINING DET NMITC
35262	ONI JOINT TRAINING DET FITC
3583A	ONI FIST-SEA
3584A	ONI FIST-SHORE



35945 ONI JFIC NORFOLK VA  
3681A DNI SUPT DET CNI DAM NECK VA  
3738A DNI NETWARCOM SPT NORFOLK VA  
3850A NAVSUPDET ARLINGTON VA SEA DTY  
39545 ONI INTELCOMM FITCPAC  
39998 OFFICE OF SPECIAL TECHNOLOGY  
40006 NTL MARITIME OPS CTR WASH DC  
40368 NAVAL SUPPORT DET ARLINGTON VA  
40509 DNI SPT DET CNFJ YOKOSUKA  
40627 NAVAL SUPPORT DET KIRTLAND AFB  
41605 ONI SSO JACKSONVILLE  
41745 ONI DET NAVAL WAR COLLEGE NWPT  
42253 ONI SPINTCOMM COMSUBGRU 7 Y JP  
42887 ONI SPINTCOMM CPRF5/7F  
43656 ONI ASTAPSUITLAND MARYLAND  
44860 DNI OPNAV SUPPORT ARLINGTON VA  
45107 ONI SP COMSUBLANT NORFOLK VA  
45508 ONI NAVNETWARCOM OPS  
45532 ONI MASINTDET PATRICK AFB FL  
45771 FITCPAC SAN DIEGO GDIP  
45979 ONI TACTICAL HUMINT  
46378 ONI SSO COMSTRKFITWINGPAC  
46379 ONI SPINTCOMM CNFK CNIC  
46571 ONI LI PACIFIC PEARL HARBOR  
46645 DNI TACTICAL INTEL SUPPORT  
46804 DNI OPNAV SUPPORT/CNO-IP  
46805 DNI SUPPORT SUITLAND MD  
46806 ONI NAVY TACTICAL HUMINT SEADU  
47167 ONI SPINTCOMM/SSO NMITC V BCH  
47169 ONI SP/SSO ANTISUBWAROPCTR  
47441 ONI LI WCONUS SAN DIEGO  
47696 ONI SSO/FIWC VIRGINIA BCH VA  
48037 ONI SSO NAPLES  
48168 ONI SSO COMNAVBASE GTMO BAY  
48390 ONI SSO SAN DIEGO  
48696 ONI NVSUPPACT CROF SOUDA BAY G  
48909 ONI SUBMARINE COMP SUITLAND  
49663 OMA CIA NON-REIMB  
49913 ONI SSO DET NEWPORT  
52848 ONI DETACHMENT ATLANTIC FLEET  
52849 ONI DETACHMENT PACIFIC FLEET  
62845 ONI JDISS PMO SUITLAND  
65260 ONI SP JICPAC PEARL HARBOR  
65290 ONI SP/SSO NAVINFOWARACT/GDIP

65894 CENTRAL INTELLIGENCE AGENCY  
66674 ONI SSO GROTON CT  
66701 ONI COMSUBGRU 6 CHARLESTON  
68166 ONI SUITLAND MD  
69039 MCIA DET QUANTICO VA  
69040 MCIA DET SUITLAND  
69041 MCIA DET FAYETTEVILLE  
69042 MCIA DET CAMP SMITH  
69064 ONI SSO PEARL HARBOR  
30508 NSGA Fort Meade, MD  
31186 NSGA Fort Meade, MD  
31590 NSGA Fort Meade, MD  
31592 NSGA Fort Meade, MD  
31937 NSGA Fort Meade, MD  
32690 NSGA Fort Meade, MD  
32695 NSGA Fort Meade, MD  
35450 NSGA Fort Meade, MD  
39754 NSGA Fort Meade, MD  
39896 NSGA Fort Meade, MD  
40074 NSGA Fort Meade, MD  
41963 NSGA Fort Meade, MD  
41992 NSGA Fort Meade, MD  
45069 NSGA Fort Meade, MD  
45487 NSGA Fort Meade, MD  
47684 NSGA Fort Meade, MD  
48002 NSGA Fort Meade, MD  
48549 NSGA Fort Meade, MD  
62936 NSGA Fort Meade, MD  
3000B NSGA Fort Meade, MD  
3121B NSGA Fort Meade, MD  
3122B NSGA Fort Meade, MD  
3147B NSGA Fort Meade, MD  
3262A NSGA Fort Meade, MD  
3746A NSGA Fort Meade, MD  
4188A NSGA Fort Meade, MD  
00069 COMNAVSECGRU Fort Meade, MD  
33389 NSGA Groton, Groton Sub Base, CT  
35459 NSGA Groton, Groton Sub Base, CT  
47685 NSGA Groton, Groton Sub Base, CT  
65991 NSGA Groton, Groton Sub Base, CT  
31080 NSGA Fort Gordon, GA  
39900 NSGA Fort Gordon, GA  
39901 NSGA Fort Gordon, GA  
41246 NSGA Fort Gordon, GA  
41247 NSGA Fort Gordon, GA  
3480B NSGA Fort Gordon, GA

3777A NSGA Fort Gordon, GA  
30996 NSGA Norfolk (includes NSGD Brunswick)  
31931 NSGA Norfolk (includes NSGD Brunswick)  
35014 NSGA Norfolk (includes NSGD Brunswick)  
35293 NSGA Norfolk (includes NSGD Brunswick)  
35477 NSGA Norfolk (includes NSGD Brunswick)  
40007 NSGA Norfolk (includes NSGD Brunswick)  
41245 NSGA Norfolk (includes NSGD Brunswick)  
42052 NSGA Norfolk (includes NSGD Brunswick)  
45158 NSGA Norfolk (includes NSGD Brunswick)  
45485 NSGA Norfolk (includes NSGD Brunswick)  
47678 NSGA Norfolk (includes NSGD Brunswick)  
48590 NSGA Norfolk (includes NSGD Brunswick)  
48914 NSGA Norfolk (includes NSGD Brunswick)  
63902 NSGA Norfolk (includes NSGD Brunswick)  
69054 NSGA Norfolk (includes NSGD Brunswick)  
3302A NSGA Norfolk (includes NSGD Brunswick)  
4359A NSGA Norfolk (includes NSGD Brunswick)  
39898 NSGA Medina, Medina Annex, MRSOC, TX  
43707 NSGA Medina, Medina Annex, MRSOC, TX  
47680 NSGA Medina, Medina Annex, MRSOC, TX  
49720 NSGA Medina, Medina Annex, MRSOC, TX  
49721 NSGA Medina, Medina Annex, MRSOC, TX  
49722 NSGA Medina, Medina Annex, MRSOC, TX  
3776A NSGA Medina, Medina Annex, MRSOC, TX  
31188 NSGA Sugar Grove, WV  
32725 NSGA Sugar Grove, WV  
31216 NSGA Yokosuka, Japan  
45079 NSGA Yokosuka, Japan  
66756 NSGA Yokosuka, Japan  
69027 NSGA Yokosuka, Japan  
30020 NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
30043 NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
30048 NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
30055 NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
30057 NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
32901 NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
39897 NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
47446 NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
49763 NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
66986 NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
3159B NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
3758A NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
4342A NSGA Denver, CO (includes NSGD Potomac and Diego Garcia)  
31743 NSGA San Diego, San Diego, CA  
31932 NSGA San Diego, San Diego, CA

35455 NSGA San Diego, San Diego, CA  
45082 NSGA San Diego, San Diego, CA  
48517 NSGA San Diego, San Diego, CA  
63896 NSGA San Diego, San Diego, CA  
4360A NSGA San Diego, San Diego, CA  
31608 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
35016 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
40075 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
40132 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
41726 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
43456 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
43457 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
44594 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
45489 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
45516 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
47681 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
69055 NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
3778A NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
4526A NSGA Hawaii, Kunia, HI (includes NSGD KBay)  
32104 NSGA Misawa Japan (Includes NSGD Seoul)  
32710 NSGA Misawa Japan (Includes NSGD Seoul)  
35465 NSGA Misawa Japan (Includes NSGD Seoul)  
45490 NSGA Misawa Japan (Includes NSGD Seoul)  
46452 NSGA Misawa Japan (Includes NSGD Seoul)  
48001 NSGA Misawa Japan (Includes NSGD Seoul)  
49656 NSGA Misawa Japan (Includes NSGD Seoul)  
66752 NSGA Misawa Japan (Includes NSGD Seoul)  
30756 NSGA Menwith Hill, UK (Includes NSGD Digby)  
32428 NSGA Menwith Hill, UK (Includes NSGD Digby)  
32691 NSGA Menwith Hill, UK (Includes NSGD Digby)  
39899 NSGA Menwith Hill, UK (Includes NSGD Digby)  
41725 NSGA Menwith Hill, UK (Includes NSGD Digby)  
44598 NSGA Menwith Hill, UK (Includes NSGD Digby)  
63908 NSGA Menwith Hill, UK (Includes NSGD Digby)  
3053B NSGA Menwith Hill, UK (Includes NSGD Digby)  
3261A NSGA Menwith Hill, UK (Includes NSGD Digby)  
32694 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)  
39892 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)  
39893 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)  
49606 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)  
49945 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)  
49947 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)  
49948 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)  
49949 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)  
49950 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)  
49952 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)

- 49953 Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)
- 3028A Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)
- 3047B Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)
- 3226B Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)
- 3317A Naval Information Warfare Activity (NIWA), Suitland, MD (includes NSGD and NIWA Dets)
- 42813 NSG Field Office Great Lakes, RTC Great Lakes, NSG Field Office Pensacola, CNC Corry Station, NSG Field Office Paris Island, NC Marine, NSG Field Office San Diego, MCB Marine San Diego

**EXHIBIT 6B**

**PROCUREMENT OF FORMS**

These forms can be procured through the normal supply channels using the form and stock numbers provided.

**From the Navy supply system:**

DD 254	Contract Security Classification Specification (12-90) S/N 0102-LF-011-5800
OPNAV 5511/14	Security Termination Statement (Rev. 9/05)
FD 258	Applicant Fingerprint Card S/N 0104-LF-006-9600

**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. 1/00) NSN 7540-01-280-5499

The SF 85, SF 85P, SF 86 and SF-86A may also be downloaded from OPM's web site at: [www.opm.gov](http://www.opm.gov). Select "Site Index" from the home page, select "F" from alphabetical listing, select "Forms" from topics, select "Standard Forms (SF)" from electronic forms, then select the form you want.

## CHAPTER 7

### CLEARANCE AND SENSITIVE ASSIGNMENT ELIGIBILITY DETERMINATIONS

#### 7-1 BASIC POLICY

1. No individual will be given access to classified information or assignment to sensitive duties unless a favorable personnel security determination has been made regarding his/her loyalty, reliability and trustworthiness. A PSI is conducted, as detailed in chapter 6, to gather information pertinent to these determinations.
2. The national security standard which must be met for personnel security clearance eligibility and eligibility for assignment to sensitive national security positions is that, based on all available information, the individual's loyalty, reliability and trustworthiness are such that entrusting them with access to classified information or assignment to a sensitive position is clearly consistent with the interests of national security.
3. In making personnel security eligibility determinations, all information, favorable and unfavorable, is considered and assessed for accuracy, completeness, relevance, importance and overall significance.
4. The eligibility determination is the result of an overall common sense "whole person" adjudication, reached by application of the evaluation criteria in appendix G. This criteria is based on EO 10450 and EO 12968 requirements and applies 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.
5. The DON CAF establishes eligibility for all DON affiliated civilian and military personnel, after adjudication of the prerequisite security investigation. The DON CAF reestablishes eligibility after adjudication of each subsequent investigation. In the interest of efficiency, **DON CAF establishes eligibility at the highest level supportable by the prerequisite security investigation.**
6. Once established, eligibility remains valid provided the individual continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months.

7. Eligibility does not expire and is not invalidated by overdue reinvestigation.

8. The personnel security adjudicative process evaluates investigative and other related information. It does not determine criminal guilt or 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 sensitive position that, if improperly executed, could have unacceptable consequences to national security.

9. 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.

#### **7-2 AUTHORITIES AND RESPONSIBILITIES**

1. The authority to determine eligibility for access to classified information or assignment to sensitive national security positions is vested in the SECNAV. This authority and the associated responsibilities are delegated as follows:

a. The Chief of Naval Operations, Special Assistant for Naval Investigative Matters and Security (N09N) will:

- (1) Issue DON PSP policy.
- (2) Assign responsibilities for overall management of the PSP.

b. The Director, Department of the DON CAF will:

(1) Adjudicate information from PSIs and other relevant information to determine eligibility for access to classified information, and/or assignment to sensitive national security positions in a timely manner.

(2) Ensure personnel security determinations are properly documented in JPAS and communicated to the employing activity.

(3) Assist DON commands with queries regarding the status of PSIs at OPM, and facilitate resolution of request changes, and corrections.



c. Commanding officers will:

(1) Establish and maintain a security education program to instruct personnel on security responsibilities and expectations.

(2) Request PSIs on personnel assigned to the command, as appropriate, and monitor requests to ensure necessary action is accomplished.

(3) Request eligibility determinations, as appropriate, and monitor requests to ensure necessary action is accomplished.

(4) Authorize, grant, limit and control access to classified information, as appropriate.

(5) Ensure JPAS accurately reflects all personnel under the commands PSP and initiate action to correct any personnel identifying data inaccuracies recorded in JPAS.

(6) Maintain complete and accurate personnel security records of security briefings, PSI and eligibility determination requests, local access determinations and position sensitivity determinations of all assigned personnel in JPAS.

(7) Continuously evaluate command personnel with regard to their eligibility for access to classified information applying the exhibit 10A criteria. Notify the DON CAF when potentially disqualifying information is developed.

(8) Ensure that personnel security eligibility determinations concerning personnel assigned to the command are properly coordinated between supervisors, human resource specialists and security personnel, as appropriate.

(9) Ensure personnel are appropriately referred to command assistance programs, as issues dictate.

d. Employees will:

(1) Fully and accurately complete personnel security questionnaires and cooperate with personnel security investigators.

(2) Be aware of the personnel security eligibility standards and advise and consult with local security officials whenever information develops that could effect eligibility.

2. PSP eligibility determinations rely on personnel management systems to provide critical program data including accurate and current employee personal identifying data (such as name, date of birth, social security number, citizenship, etc.) and accurate and current position requirements data (such as the position sensitivity designation, investigation requirement, security clearance eligibility requirement), to fill JPAS data fields. To support accurate and current personnel security processing, the responsibilities for critical personal and requirements data are as follows:

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

(1) Ensure personnel security requirements for DON civilian personnel are properly identified to JPAS.

(2) Ensure personnel identifying data is accurately reflected and updated in the Defense Civilian Personnel Data System (DCPDS).

(3) Coordinate with CNO (N09N2) and DON CAF on all matters regarding assignment of civilians to sensitive national security positions.

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

(1) Ensure personnel security requirements for Navy military members are properly coded in military personnel data systems, which ultimately update JPAS.

(2) Ensure personnel identifying data is accurately reflected and updated in the military personnel data systems.

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

(4) Coordinate with CNO (N09N2) and the DON CAF on all matters involving personnel security eligibility determinations on Navy military members.

c. **The Commandant of the Marine Corps will:**

(1) Ensure personnel security requirements for Marine Corps military members are properly identified in military personnel data systems, which ultimately update JPAS.

(2) Ensure personnel identifying data is accurately

reflected and updated in the military personnel data systems.

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

(4) Coordinate with CNO (N09N2) and the DON CAF on all matters involving personnel security eligibility determinations on DON military members.

### **7-3 SECURITY CLEARANCE AND SENSITIVE DUTY ASSIGNMENT**

1. In making eligibility determinations, DON CAF applies the appendix G personnel security eligibility standard consistently to both sensitive national security position determinations and security clearance eligibility determinations. These determinations cannot be made exclusive of each other. A determination that an individual is not eligible for assignment to a sensitive national security position will also result in the removal of eligibility for security clearance. Likewise, a determination that an individual is not eligible for a security clearance will result in the denial of eligibility for assignment to a sensitive national security position.

2. Security clearance eligibility is not 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 eligibility also has a need for access to classified information in the performance of official duties, as explained in chapter 9.

3. A favorable sensitive duty assignment eligibility determination by DON CAF does not mandate the employing command to make such assignment. Rather it establishes that an employee has been determined to be eligible for such assignment based on national security standards, depending on the operational needs and the suitability requirements of the employing activity.

4. As the PSP has evolved, the terminology used to refer to program concepts has also evolved.

a. The term "security clearance *eligibility*" has replaced "*security clearance*," when referring to a formal determination made by an authorized adjudicative entity that an individual meets national security standards. Security clearance *eligibility* is officially recorded and subject to due process procedures. *Security clearance* now refers to a state that exists

whenever eligibility has been properly established by an authorized adjudicative entity *and* access has been properly authorized by the command. *Security clearance* is understood to exist at the level of access authorized.

b. When a command authorizes access to classified information pending completion and formal adjudication of the required PSI, this action was termed "interim clearance" in the past. However, EO 12968 standards more accurately refer to this action as "temporary access" because it is an access determination under command purview. It is not a clearance determination and it carries no due process benefits. Detailed guidance for *temporary access* is provided in paragraph 9-4.

#### **7-4 DON CAF DETERMINATION PROCESS**

1. To ensure uniform application of the national security standards, the SECNAV established the DON CAF under the DIRNCIS as the single DON authority for personnel security adjudication.

2. The DON CAF adjudications eligibility to access classified information or perform sensitive duties for DON civilian and military personnel, at the request of commands and activities, upon affirmation that establishing the eligibility is clearly consistent with the interests of national security.

3. The adjudication process assesses the probability of future behavior that could have an adverse effect on national security. Few situations allow for positive, conclusive evidence of certain future conduct, therefore, the adjudicative process is an attempt to judge whether the circumstances of a particular case of demonstrated past conduct, behaviors and activities suggest a probable degree of future conduct, behavior or activities which would be inconsistent with the interests of national security.

4. DON CAF adjudicators weigh each case on its unique merits, making common sense evaluations of the "whole person," with consideration for the nature and seriousness of past conduct; the circumstances surrounding the conduct; the frequency and recency of the conduct; the age of the individual; the voluntariness of participation; and the absence or presence of rehabilitation; applying the adjudication criteria provided in appendix G.

5. In determining eligibility, DON CAF adjudicators evaluate all available favorable and unfavorable information from personnel security investigative files and from other sources, including personnel, medical, legal, law enforcement and security records.

a. PSIs are reviewed to ensure compliance with EO 12968 standards. Investigations that do not meet EO 12968 standards are returned to OPM for correction.

b. If investigative limitations preclude compliance with EO 12968 standards, the Director DON CAF may permit adjudication of the deviant investigation in his discretion and considering the needs of the DON, provided the investigative coverage is substantially sufficient to support the adjudication.

(1) Whenever an eligibility determination is based on an investigation that does not meet EO 12968 standards, the deviation of standards will be recorded in JPAS.

(2) Reciprocity does not apply to eligibility determinations made with a deviation of investigative standards.

6. Although it is intended to rarely occur, considering the needs of the service the Director DON CAF may permit an affirmative eligibility determination when disqualifying issues have not been fully mitigated. There are two circumstances in which this exception to appendix G adjudication criteria could occur, and both must be recorded in JPAS.

a. Conditional exception - Eligibility may be authorized or continued by DON CAF when disqualifying issues are present, with the provision that one or more additional compensatory measures be fulfilled. These measures or "conditions" will be fully defined to the individual concerned and the employing command, with the understanding that failure to fulfill the conditions will result in unfavorable determinations processing. Conditional eligibility determinations are usually reserved for situations in which the employee has exceptional skill or merit or has made exceptional contribution to the DON mission, and the employing activity is willing to provide the necessary resources to manage the defined risk and conditions.

b. Waiver exception - SCI access eligibility may be established or continued despite the presence of substantial issue information that would normally preclude access, such as the existence of foreign national family members. The waiver typically involves one specific disqualifying factor, which is waived due to meritorious circumstances. Reference (d) provides guidance on SCI access eligibility standards and waivers. Although not approved under DON CAF authority, DON CAF likewise records "Smith Amendment" waivers authorized by the SECNAV in JPAS as waivers.

7. In the interest of efficiency, DON CAF adjudicators establish eligibility at the highest level supportable by the prerequisite investigation. DON CAF adjudicators reestablish eligibility after adjudication of each subsequent investigation.

8. All DON CAF eligibility determinations are recorded in the JPAS on a daily basis.

9. The rationale underlying each unfavorable personnel security determination and each favorable personnel security determination (where the investigation or information upon which the determination was made included significant derogatory information as outlined in appendix G) is documented and maintained in a readily retrievable system. In the case of favorable determinations, whenever a case has information that could reasonably be concluded differently by another adjudicator, a rationale must be maintained.

#### 7-5 STANDARDS FOR ADJUDICATIVE REVIEW

1. In view of the significance that each eligibility determination 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 eligibility determinations.

a. Command evaluations of unfavorable information will be accomplished by the Security Manager (GS-11 or military officer or equivalent level security specialist) to achieve a commensurate minimal level of review.

b. DON CAF evaluations of information will be accomplished as follows:

(1) SSBI/SSBI-PR/PPR/RSI

(a) Favorable Investigations. Completely favorable investigations may be finally adjudicated after one level of review by an adjudicative official in the civilian grade of GS-9/11 or military rank of O-2/3.

(b) Unfavorable Investigations. Investigations that are not completely favorable will undergo at least two levels of review by adjudicative officials, the second of which will be in the civilian grade of GS-11/12 or military rank of O-3/4.

(2) NACLC/ANACI

(a) Favorable Investigations. Favorable investigations may be finally adjudicated after one level of review by an adjudicative official in the civilian grade of GS-7 or military rank of O-1.

(b) Unfavorable Investigations. Investigations that are not favorable will be reviewed by an adjudicative official in the civilian grade of GS-9/11 or military rank of O-2/3 prior to favorable determination.

(3) Unfavorable Continuous Evaluation Program (CEP). Information will be reviewed by an adjudicative official in the civilian grade of GS-7/9 or military rank of O-1/2, with a second level review by a GS-11/12 or military rank of O-3/4.

(4) LOI/LOD authorities. When an unfavorable personnel security action is contemplated, the LOI to deny or revoke will be approved and signed by an adjudicative official in the civilian grade of GS-12/13 or military rank of O-4/5. The final notification of unfavorable personnel security determination or LOD will be approved and signed by an adjudicative official in the civilian grade of GS-14/15 or military rank of O-5/6.

2. To ensure the maximum degree of accuracy and consistency, a **minimum level of training and experience** is required for all

DON CAF adjudicators making personnel security eligibility determinations.

a. Absent second level review, completely favorable investigations will be reviewed by an adjudicator who has attended the DSS Basic Adjudicator course, or equivalent, and had at least 6 months supervised adjudicative experience.

b. Second level review will be accomplished by an adjudicator who has attended the DSS Basic Adjudicator course, or equivalent, and has had at least 12 months supervised adjudicative experience.

c. Final unfavorable determination letters will be signed by an adjudicator who has attended the DSS Basic Adjudicator and Advanced Adjudicator course, or equivalent, and has had at least 12 months supervised adjudicative experience.

## 7-6 REQUESTING ELIGIBILITY DETERMINATIONS

1. A personnel security eligibility determination is required when an individual is initially nominated to perform sensitive national security duties or for access to classified information; a PSI is completed on an individual who occupies a sensitive position or has access to classified information; unfavorable information becomes available about an individual who occupies a sensitive position or has access to classified information; or the issues that prompted a previous unfavorable personnel security eligibility determination no longer exist and the command again requires the individual to perform sensitive duties or to have access to classified information.
2. When it is determined that an individual will require access to classified information to perform assigned duties, commands will consult JPAS to determine if the necessary security clearance eligibility was previously established. If it appears that the prerequisite investigation was completed but not properly adjudicated, or if eligibility was established by an adjudicative entity other than DON CAF, the command will use JPAS to request that DON CAF reciprocally establish the required eligibility.
3. When the individual indicates that eligibility was established by a non-DoD entity, that eligibility determination may not be visible in JPAS. The command will gather details concerning the eligibility and investigation, and using JPAS will request that DON CAF "reciprocally" establish the required eligibility. Paragraph 7-7 provides details on reciprocal acceptance of eligibility determinations. DON CAF will either verify eligibility and reciprocally re-establish or will direct the command to request the necessary PSI, as appropriate.
4. When it is determined that the individual does not have the investigation or eligibility required, the command will submit the appropriate request for investigation. Upon completion, the investigation will be forwarded to the DON CAF where the required eligibility determination will be made and recorded in JPAS. Commands need NOT submit a separate eligibility request to DON CAF. DON CAF acts on the eligibility requirements recorded on the PSI request. For detailed instruction on the proper preparation of investigation request forms see the CNO(N09N2) web page at [www.navysecurity.navy.mil](http://www.navysecurity.navy.mil). Temporary access (interim clearance) procedures may be employed as necessary; paragraph 9-4 provides details.
5. Upon receipt of derogatory information, 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 non-sensitive duties pending a final eligibility determination by the DON CAF. Paragraph 9-17 provides guidance on suspending access for cause. Regardless of the local access determination, commands report all information outlined in exhibit 10A to DON CAF via the JPAS incident report function, and use other available means to forward relevant supporting documentation. DON CAF adjudicates the information and may validate continued eligibility, request more information or further investigation, or begin the unfavorable determinations process.

#### **7-7 RECIPROCAL ACCEPTANCE OF ELIGIBILITY DETERMINATIONS**

1. A personnel security eligibility 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: (a) there is no break in continuous service greater than 24 months; (b) the investigative basis is adequate for the eligibility to be established, and (c) no new derogatory information is identified. Eligibility will be verified by the DON CAF, without additional adjudication.

a. Continuous service for eligibility purposes is active duty military service (including attendance at the military academies); active status in the military reserve, National Guard, Naval Reserve Office Training Corps (NROTC), active Individual Ready Reserves (IRR), etc.; civilian employment in the federal government; employment with a DoD contractor that involves a security clearance eligibility under the 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.

b. Chapter 6 requirements and the equivalency tables in exhibit 6A are provided to assist in determining the adequacy of investigation.

c. Derogatory information includes any un-adjudicated information as outlined in exhibit 10A.

2. Whenever security clearance eligibility has been established, DON CAF will not request 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 security clearance eligibility; or

c. The most recent eligibility determination was conditional or based on a waiver or deviation.

3. Eligibility determinations established with waiver, deviation or condition are not bound by reciprocity rules. Subparagraph's 7-4.5 and 7-4.6 provide details on adjudications made as exception to rules.

4. Unfavorable personnel security eligibility determinations are not bound by reciprocity, but may also be accepted by agencies of the federal government, in their discretion.

#### **7-8 ELIGIBILITY PROHIBITIONS**

1. Only U.S. citizens who are employees of the executive branch of the U.S. Government (including employees of contractors under the NISP are eligible for security clearance or assignment to sensitive duties. Appendix F provides guidance on validating U.S. citizenship.

a. Occasionally, it is necessary for the DON to authorize access or assignment for persons not meeting these requirements; paragraph 9-15 governs these situations.

b. 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, and those who have derived U.S. citizenship or those who acquired it through naturalization.

c. For security clearance eligibility purposes, a U.S. citizen is a person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands, or Panama Canal Zone (if the father or mother (or both) is or was a citizen of the U.S.).

2. Eligibility will not be established for persons who hold a foreign passport. The use and/or possession of a foreign passport is an appendix G disqualifying criteria which may indicate a preference for a foreign country over the U.S., raising questions regarding the persons inclination to only make decisions that serve the best interests of the U.S.

Additionally, possession and use of a foreign passport facilitates foreign travel unverifiable by the U.S.

3. Eligibility will not be established for persons who are not in a position which requires eligibility including persons in non-sensitive or public trust civilian positions; persons (such as guards and emergency service personnel) who may only have inadvertent access to sensitive information or areas; persons (such as maintenance, food services, or cleaning personnel) who perform non-sensitive, unclassified duties in areas where classified information can be reasonably prevented; or 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. The FAD program is used for trustworthiness determinations for contractor personnel when no access to classified information is required (chapter 9 applies).

4. Eligibility will not be established for persons identified in Section 1071 of the Floyd D. Spence National Defense Authorization Act for fiscal year 2001, amended 2004. Commonly referred to as the "Smith Amendment," this mandate was enacted to preclude the initial granting or renewal of security clearance eligibility by the DoD under specific circumstances. DON CAF will determine applicability of Smith amendment after adjudication of the prerequisite PSI. Smith amendment waiver provisions and details are provided in chapter 8. The specific circumstances include:

a. Persons convicted in any court of the U.S. (federal or state court including courts martial) of a crime, for which they are sentenced to incarceration *and consequently served* imprisonment for a term exceeding one year;

b. Persons currently using unlawful controlled substances, or are addicted to controlled substances (as defined in Section 102 of the Controlled Substances Act (21 USC. 802));

c. Persons who are mentally incompetent, as determined by a mental health professional approved by the DoD;

d. Persons discharged or dismissed from the Armed Forces under dishonorable conditions.

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.

6. 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 NETWARCOM (IOD) or SSO Navy. Chapter 9 provides access procedures.

#### **7-9 UNIQUE ELIGIBILITY REQUIREMENTS**

1. **Commanding Officer Clearance.** Every commanding officer must have a favorably adjudicated SSBI and eligibility determination that is at least equivalent to the highest level of classified information maintained at the command.

a. The incumbent commanding officer will review the records of the prospective commanding officer to ensure that the individual has the necessary investigation and clearance eligibility determination 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.

b. When the prospective commanding officer does not have an adjudicated SSBI completed within the past 5 years, the incumbent commanding officer will ensure that the required SSBI request is submitted.

2. **Cryptographic Duties.** Commands cannot grant interim access for cryptographic duties. The DON CAF must establish clearance eligibility 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, when supported by the commensurate DON CAF security clearance eligibility.

4. **Individual Ready Reserves (IRR).** IRR members will have security clearance eligibility 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 NAVPERSCOM

(PERS-483) or CMC (HQMC) require individuals in specified ratings/MOS to have security clearance eligibility established by the DON CAF to support potential subsequent assignments.

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

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

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 a Command or Activity.** An individual who is direct-hired as a consultant by a government contracting office/activity and will only require access to classified information at that activity or in connection with authorized visits, is not processed for a security clearance under the NISP.

a. For eligibility and access purposes, the consultant is managed by the contracting activity as an employee and the DON CAF adjudicates eligibility.

b. Consultants hired by (or under contract to) a DoD contractor to provide professional or technical assistance are considered employees of the contractor and processed under the NISP if eligibility is required. (Additional contractor requirements can be found in the NISPOM).

8. 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), 14 Jun3 2000 (NOTAL).

9. State governors may be processed for security clearance eligibility by the Department of Homeland Security (DHS). Commanding Officers may grant access to specifically designated classified information to these individuals, on a **"need-to-know"** basis. Staff personnel of the governor's office who require access to DON classified information are investigated and vetted by the DHS, as appropriate.

**7-10 ELIGIBILITY UNDER THE NATIONAL INDUSTRIAL SECURITY PROGRAM**

1. Employees of contractors granted facility clearances under the NISP may have personnel security clearance eligibility established 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 OPM and the results are forwarded to the DISCO, the DoD adjudicative facility responsible for establishing security clearance eligibility for DoD contractors.
2. Employees of contractors requiring access to DON SCI are adjudicated for SCI access eligibility by the DON CAF. After adjudication of SCI access eligibility, the investigative results are forwarded to DISCO for security clearance eligibility determination.
3. Access to Secret or Confidential classified information may be permitted for eligible contractor employees by DISCO on a temporary basis, pending completion of the appropriate PSI.
4. Access to Top Secret classified information may be permitted for eligible contractor employees by DISCO on a temporary basis, pending completion of the appropriate PSI. DON contracting commands in receipt of requests for interim Top Secret access will validate the contract, the contractor's need-to-know, and the necessity for the interim access.
5. Commanding officers will report to DISCO, via JPAS, any adverse or questionable information that 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) Cognizant, Security Office (CSO) identified on the Contract Security Classification Specification (DD Form 254). A sample DD 254 is at exhibit 11A of reference (e). Commanding Officers will also report adverse or questionable information to the DON CAF when a cleared contractor employee has SCI access, or is a consultant whose clearance eligibility has been established by the DON CAF.
6. Commands are responsible for ensuring all clearance eligibility and access requirements are identified on the DD 254. Command procedures for granting or denying access to classified information for cleared contractor personnel are provided in paragraph 9-12.

## CHAPTER 8

### UNFAVORABLE ELIGIBILITY DETERMINATIONS AND RESTRICTIONS

#### 8-1 BASIC POLICY

1. No individual will be given access to classified information or assigned to sensitive duties unless a favorable eligibility determination has been made regarding his/her loyalty, reliability and trustworthiness. A PSI is conducted, as detailed in chapter 6, to gather information pertinent to these determinations.

2. The eligibility determination is the result of overall common sense "whole person" adjudication, reached by application of the evaluation criteria in appendix G. This criteria is based on EO 10450 and EO 12968 requirements which 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.

3. Eligibility determinations are restricted to U.S. citizens determined to require eligibility to execute official U.S. government functions and duties (including employees of contractors under the NISP. Eligibility will not be established for individuals who hold a foreign passport. Eligibility will not be established for individuals identified in Section 1071 of the Floyd D. Spence National Defense Authorization Act for fiscal year 2001, amended 2004. Paragraph 8-3 provides details on restrictions.

4. The personnel security adjudicative process evaluates investigative and other related information. It does not determine criminal guilt or 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 sensitive position that, if improperly executed, could impact national security.

5. DON CAF is the single DON authority for making favorable and unfavorable eligibility determinations. The employing command is responsible for making the basic employment suitability determinations and evaluating potential nexus issues using personnel suitability regulations, however, only the DON CAF can make a determination that an employee is ineligible to occupy a sensitive national security position based on this policy manual.

6. Commands are ultimately responsible for ensuring that the DON CAF is apprised whenever information develops that suggests an individual may no longer be in compliance with personnel security standards. Commands will report the issues to the DON CAF for adjudication using JPAS. (For SCI access, refer to reference (d) for reporting requirements.) Commands must implement a proactive continuous evaluation program as described in chapter 10, to satisfy this requirement. Exhibit 10A provides a checklist of issues that must be reported.

7. Regardless of an individual's intent to appeal, once the DON CAF makes an unfavorable eligibility determination, the command must remove all accesses authorized and debrief the individual in accordance with paragraphs 4-11 and 9-7, and remove civilian employees from designated sensitive positions.

8. Unless there is a reasonable basis for doubting a person's loyalty to the U.S., 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 policy manual.

9. DON civilian employees or military members shall not be removed from employment or separated from service due to failure to meet the requirements of this policy manual if removal or separation can be effected under OPM regulations or administrative (non-security) military regulations. However, administrative actions contemplated in this regard shall in no way affect or limit the responsibility of the DON CAF to continue to adjudicate the issue for unfavorable security determination, as warranted and supported by the criteria and standards contained in this policy manual.

10. 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 SCI and/or SAPs within 18 months prior to the proposed action, unless approval is first received from the program manager (i.e. the DNI for SCI access or CNO (N7SP) for SAPs).



## 8-2 AUTHORITIES AND RESPONSIBILITIES

1. The authority to determine eligibility for access to classified information or assignment to sensitive national security positions is vested in the SECNAV. This authority and the associated responsibilities for unfavorable personnel security determinations are delegated as follows:

a. The Chief of Naval Operations, Special Assistant for Naval Investigative Matters and Security (N09N) will:

- (1) Issue DON PSP policy.
- (2) Assign responsibilities for overall management of the PSI program.
- (3) Maintain the DON PSAB and appoint members to ensure timely due process is afforded in appeals of unfavorable DON CAF personnel security determinations.

b. The Director, Department of the Navy Central Adjudication Facility (DON CAF) will:

- (1) Adjudicate information from PSIs and other relevant information to determine eligibility for access to classified information, and/or assignment to sensitive national security positions.
- (2) Issue a LOI to deny or revoke eligibility for assignment to sensitive national security positions or access to classified national security information to every individual for whom an unfavorable eligibility determination is being contemplated, providing a detailed statement of reasons and rationale specific to the appendix G adjudication disqualifying eligibility criteria.
- (3) Issue a LOD (formerly referred to as a LON) to every individual for whom an unfavorable eligibility determination has been made, providing a detailed statement of reasons and rationale specific to the appendix G adjudication disqualifying eligibility criteria.

c. The President, Personnel Security Appeals Board (PSAB) will:

- (1) Preside over the PSAB, a three-member panel appointed by CNO (N09N), which reviews and provides final decisions on appeals of unfavorable DON CAF determinations. The

PSAB decision is final and concludes the administrative appeals process.

(2) Ensure the PSAB meets at least monthly and provides notice of the PSAB to sustain or reverse determinations made by the DON CAF within 5 days of determination. PSAB structure and function is provided in exhibit 8A.

d. Commanding officers will:

(1) Administratively withdraw 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, via JPAS, that security clearance eligibility is no longer required.

(2) Continuously evaluate command personnel with regard to their eligibility for access to classified information and/or assignment to a sensitive position, applying the criteria outlined in exhibit 10A. Forward all potentially disqualifying information to DON CAF via JPAS. The DON CAF will review the information and reevaluate the individual's clearance eligibility using the appendix G adjudicative guidelines.

(3) Ensure individuals are appropriately referred to command assistance programs, as issues dictate.

(4) Suspend an individual's access to classified information for cause when warranted, and notify the DON CAF within 10 days. (Once access is suspended and reported to DON CAF, it may not be reinstated unless approved by the DON CAF.)

(5) Ensure command security officials acknowledge receipt and comply with instructions in correspondence (e.g., LOI, LOD, PSAB letters), related to unfavorable determinations, notify DON CAF or PSAB immediately if command no longer has cognizance over the individual, and promptly respond as appropriate.

(6) Ensure security officials assist personnel who are undergoing the unfavorable determinations process, by explaining the personnel security eligibility determination process, providing the appendix G adjudication criteria used by DON CAF, and providing guidance on obtaining pertinent information used in the DON CAF proposed determinations.

(7) Ensure final DON CAF unfavorable personnel security eligibility determinations are immediately coordinated with

supervisors, human resource specialists and security personnel so that necessary actions are quickly taken to officially remove personnel accordingly from access to classified information and assignment to sensitive duties.

(8) Deny visitor access 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 both the Contractor's Facility Security Officer (FSO) and to the DISCO.

e. The individual will:

(1) Be aware of the personnel security eligibility standards and continuing evaluation criteria and to seek the advice of the local security officials whenever information develops that could effect eligibility.

(2) Provide thorough, accurate and timely responses to requests for information from personnel security investigators, security officials, DON CAF adjudicators or PSAB representatives.

2. To be accurate and efficient, the unfavorable determination process relies on a full and frank exchange of pertinent information and timely action by all responsible parties; timely adjudicative action at DON CAF, timely and thorough response from individual as facilitated by command security officials, and prompt appeal consideration at PSAB. Timelines for the unfavorable determinations process are in paragraph 8-4.

### **8-3 RESTRICTIONS ON THE GRANTING OR RENEWAL OF SECURITY CLEARANCES**

1. Eligibility determinations are restricted to only U.S. citizens who are employees of the executive branch of the U.S. government (including employees of contractors under the NISP.

a. Eligibility will only be established for persons who are in a position that requires eligibility, based on evaluation of the appropriate completed PSI and in conformance with appendix G, adjudicative criteria. Exceptions to this restriction are rare.

b. Eligibility will not be established for persons who hold a foreign passport.

(1) The use and/or possession of a foreign passport is disqualifying for security clearance, unless the use or possession is in furtherance of the DoD mission and officially approved by the appropriate agency of the U.S. government.

(2) To eliminate this as a disqualifier, individuals may return foreign passports to the appropriate country embassy or consulate or, if impractical, the individual may elect to destroy the foreign passport as witnessed by a DON security official. Procedures and details on relinquishing foreign passports are found at exhibit 8B.

(3) Individuals who hold foreign passports normally have dual citizenship issues that may also prevent a favorable security clearance determination. Command guidance in addressing dual citizenship issues is provided at exhibit 8B.

c. Eligibility will not be established for persons identified in Section 1071 of the Floyd D. Spence National Defense Authorization Act for fiscal year 2001, amended 2004. Exceptions to this restriction are rare and are explained in exhibit 8C.

2. Section 1071 of the Floyd D. Spence National Defense Authorization Act for fiscal year 2001, amended Title 10, United States Code, was established to preclude the initial granting or renewal of a security clearance by the DoD under four specific circumstances. Commonly referred to as the "Smith Amendment," this mandate applies to DoD civilians, contractors and military members at the time of nomination for initial security clearance eligibility or after periodic reinvestigation for continued eligibility, and who:

a. Have been convicted in any court of the U.S. (federal or state court including courts martial) of a crime for which they were sentenced to incarceration *and consequently served* imprisonment for a term exceeding one year;

b. Is an unlawful user of, or is addicted to, a controlled substance (as defined in Section 102 of the Controlled Substances Act (21 USC. 802));

c. Is mentally incompetent, as determined by a mental health professional approved by the DoD;

d. Have been discharged or dismissed from the Armed Forces under dishonorable conditions.

3. The DON CAF will determine whether the provisions of the "Smith Amendment" apply to Navy or Marine Corps military or civilian members after full investigation and adjudication. Details concerning application of Smith Amendment by DON CAF are provided in exhibit 8C.

4. The SECNAV may authorize a meritorious waiver of the Smith Amendment prohibitions, upon command nomination and PSAB review. Details concerning the meritorious waiver appeal process are provided in Exhibit 8C.

#### **8-4 UNFAVORABLE DETERMINATIONS PROCESS**

1. When an unfavorable personnel security eligibility 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 therefore and the rebuttal process associated with the proposed action. The LOI will be sent certified or registered mail, via the individual's command, with a copy to NAVPERSCOM (PERS-483) for Navy military members and to HQMC (ARS) for Marine Corps military members. For SCI access, SSO Navy or NETWARCOM (IOD) will receive copies, 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 via JPAS, 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, absence an approved extension, or if the response is untimely, they will forfeit their right to appeal.

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. If the individual is no longer affiliated with the command, DON CAF will be immediately notified and the LOI will be returned to DON CAF.

5. 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. Individuals with interim or temporary access will have their access removed immediately. Commands will ensure all suspension actions are accomplished as specified in chapter 9. 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, faxed, or forwarded via JPAS.

8. The DON CAF will adjudicate the response to the LOI within 30 calendar days of receipt and will either make a favorable determination and authorize eligibility or issue a Letter of Denial (LOD) ((previously known as Letter Of Notification (LON)) of the unfavorable determination.

a. If a favorable determination is made, individuals will be notified in writing, via their command and the decision recorded in JPAS.

b. If the DON CAF makes an unfavorable determination, the individual will be notified in writing, citing all factors that were successfully mitigated by the individual's response to the LOI and what unfavorable factor(s) remains to cause the unfavorable determination. The LOD will be sent via the command with a copy to NAVPERSCOM (PERS-483) or HQMC (ARS) Marine Corps military members and SSO Navy or NETWARCOM (IOD), as appropriate, for SCI access issues. The final decision will be reflected in JPAS.

9. The LOD will inform the recipient of his/her appeal rights. Upon receipt of the LOD, 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 for access to national security classified information.

#### **8-5 APPEALS PROCESS**

1. The Personnel Security Appeals Board (PSAB) is the final appellate authority for unfavorable personnel security determinations made by the DON CAF. The structure and functions of the PSAB are detailed in exhibit 8A. If an individual chooses to appeal an unfavorable DON CAF determination, the appeal may be made by personal appearance 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

LOD and to submit supporting documentation to the AJ, who will make a recommendation to the PSAB. A transcript of the proceedings of the personal appearance along with any supplemental documentation will be forwarded with the DOHA AJ's 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 LOD.

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 or by video-conference (VTC). 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 (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 LOD 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 that will be forwarded along with a transcript of the personal appeal to the PSAB generally 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 DOHA personal appearance presents substantial information not included in the individual's rebuttal to the LOD. When this happens, a PSAB representative will contact the command to request the new information. The command will have 10 days to respond.

#### 4. PSAB WRITTEN APPEAL SUBMISSIONS

a. The individual has 30 days from receipt of the LOD 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 President, PSAB or designee.

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 LOD and should present any existing mitigation as defined in appendix G, to include pertinent supporting documentation.

d. Commands will provide a command perspective by submitting an endorsement to the individual's written 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. The PSAB may also request additional information from the appellant via the command.

b. Personal appearances before the PSAB are prohibited.

c. The PSAB will meet at least monthly and within five days of the Board decision will notify the individual, via the individual's command, of the PSAB determination.

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

(1) The PSAB will direct the DON CAF to grant or restore eligibility when the PSAB finds for the appellant. The DON CAF will adjust the JPAS record to re-establish eligibility within five days of receipt of the PSAB determination letter.

(2) When the PSAB finds against the appellant, reconsideration is only possible, if at a later date (at least one year from the date of the final PSAB decision) 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. Paragraph 8-6 explains the reconsideration process. A copy of the PSAB determination letter will be provided to DON CAF for inclusion in the adjudicative record.

## 8-6 REESTABLISHING ELIGIBILITY AFTER A DENIAL OR REVOCATION

1. Following an unfavorable security determination, a request to reestablish eligibility may be submitted after a reasonable passage of time, normally a minimum of 12 months after the concluding unfavorable determination either by PSAB if appeal rights were exercised or by DON CAF if appeal rights were NOT exercised, provided;

a. The issues which caused the unfavorable determination appear to have been mitigated as outlined by appendix G, either through the passage of time or other relevant positive developments, and

b. The command has a current requirement for the individual to have access to classified information or assignment to sensitive duties.

2. Reconsideration requests are formally submitted from the commanding officer of the employing activity to the Director, DON CAF. Reconsideration requests are fully detailed and justified, providing all relevant documentation to demonstrate the mitigation and support the reestablishment of eligibility.

3. DON CAF will assess the request and reestablish eligibility, if appropriate. If a favorable determination is not possible, the Director, DON CAF will provide the commanding officer with specific reasons for upholding the previous decision.

4. Pending DON CAF reconsideration, temporary/interim access and/or temporary assignment to sensitive positions is **not authorized** for individuals who have received an unfavorable eligibility determination.

**EXHIBIT 8A**

**STRUCTURE AND FUNCTIONS OF THE PERSONNEL SECURITY APPEALS  
BOARD (PSAB)**

1. The Department of the Navy Personnel Security Appeals Board (PSAB) is responsible for deciding appeals of unfavorable personnel security determinations (including SCI access) made by the DON CAF.

a. The PSAB will be comprised of a President at the minimum grade of GS-15, a military member at the minimum military grade of O-6, and a third member at the minimum military grade of O-5 or civilian grade of GS-14.

b. CNO (N09N) will formally appoint the President, PSAB.

(1) The President of the Board will have significant background and experience in the government PSP. Alternates at the minimum grade of GS-14 who have a personnel security background may be delegated to preside over Board meetings, as determined necessary by the PSAB President.

(2) The other board members, one military and one civilian grade, will be appointed by the President, PSAB, and may not be security professionals but should have DON service and experience and be knowledgeable of DON operations.

(3) 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:

(1) Establish Standard Operating procedures for:

- (a) Board administration,
- (b) Regular board meetings,
- (c) Case review procedures.

(2) Ensure that all legal questions, guidance or opinions requested by the PSAB is referred to appropriate

government attorneys. (An attorney may be present during board meetings to answer all legal questions, or provide guidance or opinions as necessary.)

2. All three PSAB members will review each case in advance of the PSAB meeting.

3. 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.

4. 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.

5. Officials from the DON CAF will neither serve as Board members nor communicate with Board members concerning the merits of an open case.

6. PSAB sitting members will not engage in exparte communications with appellants or their representatives. However, Board administrators may be involved in discussions with appellant's security managers or command officials regarding additional dispositive information requested by the PSAB.

7. Appellants will be notified of the PSAB decision by memorandum that provides the reasons for the Board's decision. The notification memorandum will be sent via the appellant's commanding officer within 5 working days of the determination.

8. The DON CAF will be notified of the PSAB decision within 5 working days of the determination and may be directed to grant or restore security clearance and or SCI access eligibility. The DON CAF will update the JPAS to reflect the PSAB decision generally within 5 working days.

9. For administrative purposes, a copy of the PSAB decision memorandum will be sent to the DON CAF, to SSO Navy or NETWARCOM (IOD) for SCI eligibility decisions, to the Naval Military Personnel Command for Navy military members, to the Commandant of the Marine Corps (ARS) for Marine Corps military members, and to the OPF for all civilian appellants.

10. The PSAB will maintain a redacted file of all decisions that will be subject to review in accordance with the Freedom of Information Act.

**EXHIBIT 8B**

**DUAL CITIZENS AND FOREIGN PASSPORTS**

1. Only U.S. citizens will be granted a personnel security clearance, assigned to sensitive duties/positions or granted access to classified.

a. Because the DON PSP relies on the verification of U.S. citizenship conducted by the Human Resource community, the accuracy and consistency of the citizenship verification process is critical to our interests.

b. For DON civilian personnel, the 5 CFR 338 outlines responsibility for verifying birth and/or citizenship for federal employment and states, "citizenship must be verified before appointment". An individual who is not a U.S. citizen or U.S. national may not compete for or be appointed to a federal government competitive service position.

c. U.S. citizens who are also dual citizens are not identified when verifying U.S. citizenship for employment purposes, and are not limited from federal government employment opportunities. Identification and resolution of dual citizenship is a function of local security officials and is specific to positions requiring an eligibility determination.

2. Dual citizenship is not, in and of itself, disqualifying for eligibility purposes.

a. Individuals who claim both U.S. and foreign citizenship and who require eligibility will be adjudicated by the DON CAF using the appendix G criteria, with due consideration of the "Foreign Influence" and "Foreign Preference" guidelines.

b. In order to mitigate concerns and facilitate adjudication, individuals who are dual citizens will normally be expected to provide a statement expressing their willingness to renounce foreign citizenship claims in favor of a sole U.S. citizenship status. The statement should be formally endorsed and forwarded by command.

c. Because dual citizenship raises foreign preference concerns, individuals who claim dual citizenship are not permitted temporary or interim access to classified information pending investigation and adjudication.

3. The use and/or possession of a foreign passport is disqualifying for security clearance (unless the use and/or possession of the foreign passport is in furtherance of the DoD mission and it has been officially approved by the appropriate agency of the U.S. government).

a. The use and/or possession of a foreign passport raises doubt as to whether the individual's allegiance to the U.S. is paramount. Possession and use of a foreign passport could also facilitate foreign travel unverifiable by the U.S.

b. In order to mitigate concerns and facilitate adjudication, individuals who possess foreign passports are REQUIRED to return the passport to the appropriate country embassy or consulate requesting a return receipt to demonstrate that the passport was surrendered; or

c. If returning the passport to the embassy is impractical due to cost, security concerns, or other associated impediments, the individual may elect to destroy the foreign passport as witnessed by a DON security official. The witnessing command security official, is normally the security manager, but it could also be an assistant security manager or other personnel delegated responsibility for resolving the commands personnel security issues.

d. To support adjudicative resolution, the command security official will provide to DON CAF either a copy of the embassy or consulate receipt, or a formal statement of witness acknowledging the destruction, along with an explanatory memorandum addressing the adjudicative concerns.

(1) Expired passports should be destroyed, as instructed above, however, there is no requirement to relinquish an expired passport to a foreign consulate or embassy. Individuals should be advised that "renewal" of an expired foreign passport or requesting a new foreign passport after it has been relinquished is reportable and will be grounds for removal of eligibility for cause.

(2) The only exception to the requirement to relinquish or destroy a foreign passport is when the use and/or possession of the foreign passport is in furtherance of the DoD mission and it has been officially approved by the appropriate agency of the U.S. government.

(a) Approving agencies are those agencies whose mission and interests are supported by an employee or affiliate maintaining a foreign government passport.

(b) Approval is bestowed, not requested. Approvals are agency driven determinations based on the needs of the agency, not the employee, therefore employee requests for approval are inapplicable.

4. Commands will report dual citizenship, or possession or use of a foreign passport to the DoN CAF whenever these issues come to light. If the issue develops or comes to light after assignment to sensitive duties (to include IT) or after authorizing access to classified information, the access or assignment must be suspended pending the DoN CAF security clearance eligibility determination.



**EXHIBIT 8C**

**SMITH AMENDMENT**

1. Section 1071 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, amended Title 10, United States Code, to preclude the initial granting or renewal of a security clearance by the DoD under four circumstances outlined below. Commonly referred to as the "Smith Amendment," this mandate applies to DoD civilians, contractors and military members nominated for initial security clearance eligibility, or after periodic reinvestigation for continued eligibility and who falls under one or more of the following four provisions:

a. Has been convicted in any U.S. court (federal or state court including courts martial) of a crime, has been sentenced to incarceration *and consequently served* imprisonment for a term exceeding one year;

b. Is an unlawful user of, or is addicted to, a controlled substance (as defined in Section 102 of the Controlled Substances Act (21 USC. 802));

c. Is mentally incompetent, as determined by a mental health professional approved by the DoD;

d. Has been discharged or dismissed from the Armed Forces under dishonorable conditions.

2. The DON CAF will determine whether the provisions of this amendment apply to Navy or Marine Corps military or civilian members after full investigation and adjudication. The provisions of this amendment apply, regardless of whether the issues were previously considered and favorably resolved. The provisions will NOT be applied to clearance transfers, reinstatements or clearances reciprocally accepted from within or from outside the DoD.

3. The SECNAV may authorize a meritorious waiver of the prohibitions. The determination to nominate an individual for meritorious waiver will be made by the individual's command and submitted to the DON PSAB as follows:

a. The individual will prepare an appeal and, if the command considers the individual to warrant meritorious waiver consideration, the command will endorse the appeal providing justification and recommendation for meritorious waiver.

b. The meritorious waiver recommendation and the individuals appeal will be forwarded via the chain of command to the DON PSAB for recommendation to the SECNAV.

c. If the individual requests a personal appearance before an AJ from the DOHA, the commands meritorious waiver recommendation will be forwarded separately via the chain of command to the PSAB.

d. The waiver recommendation may expound on the DON CAF outline of mitigating conditions, but should focus on the individual's character and actions in furtherance of the DON mission.

e. The PSAB will review the appeal and waiver recommendations to assure procedures and criteria were properly applied and will forward the request for SECNAV consideration. The PSAB will NOT forward requests that surface procedural or criteria concerns until the issues are adequately resolved through coordination with the DON CAF and command, as appropriate.

4. SECNAV approved meritorious waivers will be forwarded to DON CAF to establish eligibility accordingly. DON CAF will record the waiver in JPAS. Reciprocal acceptance of eligibility established under waiver is not required.

## CHAPTER 9

### ACCESS TO CLASSIFIED INFORMATION

#### 9-1 BASIC POLICY

1. Under U.S. Navy regulations, the commanding officer's responsibility for his or her command is absolute. The authority of the commanding officer is commensurate with his or her responsibility. Commanding officers have ultimate responsibility and authority for all determinations regarding persons who may have access to classified information under their control.
2. Commanding officers will determine those position functions under their control that require access to classified information, and may authorize access to the incumbents of such positions who have officially been determined to be eligible by the appropriate adjudicative authority.
3. Commanding officers may grant access to classified information to any individual who has an official need-to-know, established security clearance eligibility, and about whom there is no known un-adjudicated disqualifying information.
4. No one has a right to have access to classified information solely because of rank, position, or security clearance eligibility.
5. Access to classified information will be granted only if allowing access will promote the furtherance of the DON mission while preserving the interests of national security.
6. Access to classified information will be limited to the extent possible, to the minimum number of persons necessary to accomplish the mission, and will be based on need-to-know. Additionally, the level of the classification and the amount of information authorized for access will be limited to the minimum level and amount required to perform assigned duties.
7. Access to classified information will be formally terminated when it is no longer required in the performance of assigned DON duties and/or when the individual's security clearance eligibility is denied or revoked.

8. All individuals will complete a Classified Information Nondisclosure Agreement (SF 312) prior to being granted initial access to classified information and recorded in JPAS.

9. Commanding officers will ensure that personnel under their jurisdiction are briefed regarding their associated responsibilities for protecting classified information prior to being granted access.

a. It must be understood that properly limiting and controlling access to classified information is the responsibility of each authorized holder of classified information.

b. Individuals possessing or holding classified information must determine that allowing access to another individual is justified and based on the intended recipients' security clearance eligibility and need-to-know.

10. The JPAS is the system of record for all DoD access determinations. Commanding officers will ensure that all access authorizations for individuals under their control are properly and promptly recorded in JPAS.

## **9-2 NEED-TO-KNOW**

1. Access to classified information is not authorized by the favorable conclusion of a clearance eligibility determination. Access is only permitted to eligible individuals after determining that the individual has a "need-to-know."

2. Need-to-know is a determination that an individual requires access to specific classified information in the performance of (or assist in the performance of) lawful and authorized government functions and duties.

3. Need-to-know is one of two information points that must be determined by every authorized holder of classified information prior to relinquishing that classified information to a prospective recipient.

a. The authorized holder of classified information must determine that the intended recipient has security clearance eligibility established at (or above) the level of access required.

b. The authorized holder must determine that the

prospective recipient needs-to-know that information in order to perform lawful and authorized government functions.

c. These determinations must be based on reliable information, obtained formally or informally, from chain of command supervisors, security managers, or other sources in a position to know the prospective recipients security clearance eligibility and/or duties and organizational functions in relation to the specified classified information intended for release.

4. Need-to-know is a preventative measure to identify and deter unauthorized access.

a. Knowledge, possession of, or access to classified information is not provided to any individual solely by virtue of the individual's office, rank, or position.

b. Although access can only be authorized for individuals with established security clearance eligibility at or above the level of classified information required, having security clearance eligibility **DOES NOT** equate to need-to-know.

5. Classified discussions are prohibited in public areas; hallways, cafeterias, elevators, rest rooms or smoking areas because the discussion may be overheard by persons who do not have a need-to-know. (Individuals are obliged to report violations of the need-to-know principle to their security manager.)

6. Need-to-know requires a level of personal responsibility that is challenging, particularly since it conflicts with human nature and the desire to share information with co-workers and colleagues. It is therefore critical to frequently focus on need-to-know requirements during security education briefings and refresher training.

### **9-3 CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (SF 312)**

1. All personnel will execute a Classified Information Nondisclosure Agreement (NdA), Standard Form (SF) 312, as a condition of access to classified information.

a. 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.

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

2. The SF 312 NdA was revised in January 2000. The current form, provided as exhibit 4B, is available through the government supply system and must be used in place of the previous 1991 version.

3. The current SF 312, (Rev 1-00) supersedes SF 312 (Rev. 1-91), SF 312 (Rev. 9-88), SF 189, Classified Information Nondisclosure Agreement, and the SF 189-A, Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government).

4. Previously executed SF 312s remain valid and will be understood to be amended to reflect the language of the most current SF 312 (Rev 1-00). Previously executed copies of the SF 189, and the SF 189-A also remain valid and will be interpreted and enforced in a manner that is fully consistent with the interpretation and enforcement of the current SF 312. Therefore, any cleared individual who has previously signed the SF 189 or the SF 189-A does not need to execute the SF 312.

5. Once DON CAF security clearance eligibility has been granted, commands will ensure that an SF 312 is appropriately executed as a condition of allowing access to classified information.

6. When there is no evidence that a DON military or civilian employee has previously signed an SF 312, the current SF 312 must be signed before access to classified information is authorized. 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.

7. 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 via the JPAS "Report Incident" link.

8. Commanding officers will ensure personnel are provided 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.

9. The execution of the SF 312 must be witnessed and the witnessing official must sign and date the SF 312 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 U.S. 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.

10. Executed SF 312's will be maintained in personnel files for 70 years from date of signature. Execution of the SF 312 will be recorded in JPAS.

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

Navy military members:  
Commander, Naval Personnel Command  
Pers 312C  
5720 Integrity Drive  
Millington, TN 38055-3120

Marine Corps military members:  
Commandant of the Marine Corps  
Headquarters U.S. Marine Corps (MMSB-20)  
MCCDC  
2008 Elliot Road  
Quantico VA 22134-5030

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

12. 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 re-execution of another SF-312.**

#### 9-4 TEMPORARY ACCESS (INTERIM CLEARANCE)

1. In the absence of adverse information, commanding officers may grant temporary access (also referred to as interim clearance or interim access) to individuals pending completion of full investigative requirements and pending establishment of

security clearance eligibility by the DON CAF. Adverse information is identified in appendix G, paragraph 4.

2. Temporary access is an exception to the requirement for a completed investigation and eligibility determination prior to access. Temporary access is a stopgap measure taken to minimize operational impact, but it requires compensatory security measures to only consider this option if no issue information is present as follows:

a. Temporary Top Secret access requires:

(1) Established secret or confidential security clearance eligibility or a current NAC favorably adjudicated by DON CAF; and

(2) A favorable review of the completed personnel security questionnaire (PSQ) revealing no eligibility issues as outlined in exhibit 10A; and

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

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

b. Temporary secret or confidential access requires:

(1) A favorable review of the PSQ revealing no eligibility issues as outlined in exhibit 10A; and

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

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

3. Commands will record temporary access in JPAS.

4. Temporary access may only be authorized by the commanding officer or designee, and has been the subject of a favorably completed SSBI. Temporary access for SCI may be only authorized by the DONCAF.

5. It is important to ensure that the request for investigation reaches its destination, especially when temporary access is at issue. Since temporary access is a stopgap measure that anticipates a timely and favorable result, commands must be



vigilant in monitoring these requests and are strongly encouraged to use registered or certified mail to ensure receipt when mailing investigation request and other required/related documentation.

6. When the command receives a LOI (also known as Statement of Reasons) from the DON CAF to deny an individual's security clearance, the commanding officer will immediately withdraw temporary access (interim security clearance).

7. Temporary access or assignment to sensitive positions is not authorized for individuals who have received a final unfavorable eligibility determination. Requests for reinstatement may be submitted to DON CAF; however, temporary access is not authorized until eligibility is reestablished.

#### **9-5 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. Only a flag officer or general officer, a general courts-martial convening authority or equivalent senior executive service member, may grant one-time access, after coordination with command security officials.

b. The individual granted one-time access must be a U.S. citizen, have a DoD security clearance eligibility determination 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. A review of locally available records must reveal 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 PSI will be initiated.

e. The access authorization will automatically expire no later than 90 calendar days from the date access commenced. If the need for access is expected to continue for a period in excess of 90 days, the command must initiate a request for the appropriate PSI. Access will not be extended, in any case, beyond 90 days from the date access commenced unless a supporting PSI is requested.

f. Access at the higher level will only be allowed under the supervision of a properly cleared individual.

g. Access will be limited to information under the control of the official who authorized the one-time access. One-time access 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.

a. Justification for the access will be recorded, to include an explanation of the compelling reason for granting the higher-level access and, specifically, how the DON mission is being furthered;

b. 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 will also be recorded;

c. A description of the specific results of the local records review; and

d. The approving authority will be fully identified with name, rank, and position.

#### **9-6 WITHDRAWALS OR ADJUSTMENT OF ACCESS**

1. Access terminates when an individual transfers from one command to another, however eligibility will normally remain unaffected.

2. Commanding officers will administratively withdraw an individual's access authorization when a permanent change in official duties (e.g., rating/MOS changes) eliminates the DON

requirement for access. The command will debrief the individual as outlined in paragraphs 4-11 and 4-12 and file the completed Security Termination Statement in the individual's service record or Official Personnel Folder (OPF). Commands will update JPAS accordingly to indicate that the individual no longer requires access.

3. When the level of access required for an individual's official duties changes, the command will adjust the authorized access accordingly, provided the new requirement does not exceed the level allowed by the established eligibility. If the level of access required will exceed the established eligibility, commands will submit the appropriate investigation request and may consider granting temporary access, as appropriate.

4. The administrative withdrawal or downgrading of access is not authorized when prompted by developed derogatory information. In these cases, the command may **suspend** the individual's access for cause, and **must** report the suspension and/or the derogatory information to the DON CAF. (When SCI access is at issue, the command SSO will coordinate the action, reference (d) applies.)

5. A command report of suspension of access for cause will automatically result in the DON CAF suspension of the individual's security clearance eligibility.

6. Once the DON CAF removes/suspends eligibility, the individual may not be granted access unless the DON CAF reestablishes eligibility.

#### **9-7 SUSPENSION OF ACCESS FOR CAUSE**

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 DON CAF via the JPAS "Report Incident" link.

a. 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 non-sensitive duties pending a final eligibility determination by the DON CAF.

b. Once an individual's access is suspended for cause, DON CAF will remove eligibility and the command cannot reinstate

access until DON CAF adjudicates the issues and makes a favorable eligibility determination.

c. 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.

d. 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 within 10 days 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 via JPAS, providing sufficient details to support adjudicative review;

c. Remove the individual's access authorization from JPAS and remove the individual's name on all local access rosters and visit certifications, and notify all co-workers 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. Cancel or hold in abeyance any Permanent Change of Station (PCS) orders. Notify NAVPERSCOM (PERS-483) for Navy military members or HQ USMC (INTC) for Marine military members.

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

a. If the commanding officer continues to believe the individual is a risk, and that authorizing access to classified information is imprudent, the commanding officer may initiate action to reassign or adjust the individual's duties so that access to classified information or assignment to sensitive duties is no longer permitted.

b. Alternatively, the commanding officer may also elect to submit additional documentation to DON CAF that supports his/her concerns regarding the individual's disqualification. DON CAF will review and appraise the command accordingly.

#### **9-8 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 9-13.

2. As an exception to the above, an active duty flag/general officer or equivalent civilian SES may waive the investigative requirement and grant a retired flag/general officer/civilian SES 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/civilian SES 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 areas approved for storage of classified information.

c. The flag/general officer/equivalent civilian SES 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 PSI and clearance.

#### **9-9 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 9-5, may apply.

2. Reserve personnel may also be given access to COMSEC information necessary to maintain proficiency in their specialty. Details are provided in the Cryptographic Security Policy and Procedures Manual (CMS-1A), 25 February 1998 (NOTAL), and in the Electronic Key Management System (EKMS-1) Phase 4 Communications Security Material Systems (CMS) Policy and Procedures for Navy Electronic Key Management System Tiers 2&3, 5 October 2004.

#### **9-10 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 NCIS.

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

#### **9-11 ACCESS AUTHORIZATION IN LEGAL PROCEEDINGS**

1. Requests for access authorization for civilian attorneys representing DON personnel will be submitted to CNO (N09N2) via the Office of General Counsel (OGC) or Navy Office of the Judge Advocate General (OJAG). 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 representing his or her client.

2. OGC or OJAG will evaluate the request and certify that access to the specified classified information has been deemed necessary by the convening authority and will ensure the attorney requiring the access has completed the necessary PSI

request forms. OGC or OJAG 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 OPM and will authorize access, as appropriate. Prior to access, the attorney will be required to sign the Classified Information Nondisclosure Agreement (SF 312).

4. Requests for access authorization for witnesses and victims who require access to classified information in order to participate in the legal proceeding will also be processed under this section.

#### **9-12 CONTRACTOR ACCESS**

1. Commanding officers may grant access to classified information to contractor employees based on the contractors need-to-know and verification of access. 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 affected through DISCO. Action taken by a command to deny a contractor access to the command areas and information will be reported to the Cognizant Security Agency (CSA). If SCI access is an issue, a report will also be forwarded to the DON CAF. Refer to chapter 7-10.

3. As of January 2004, Contractor-granted confidential clearances will no longer be valid for access to any classified information. Additionally, restrictions on DoD contractors for access to information generated by foreign governments are described in the SECNAVINST 5510.34A of 8 October 2004, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives.

#### **9-13 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 PSI 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 that 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.

#### **9-14 HISTORICAL RESEARCHERS**

1. 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 History and Museums, United States Marine Corps, Marine Corps Education Command, Marine Corps University, History Division, CMC (Code HD) 3079 Moreell Avenue, Quantico, VA 22134.

b. Upon receipt of a request for access authorization, CNO (N09BH) or Marine Corps History Division will seek to declassify the requested records. If declassification cannot be accomplished, CNO (N09BH) or Marine Corps History Division 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), via HQMC (ARS), for Marine Corps requests, 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.

2. 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).

**9-15 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. A 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, a LAA may be considered under the following conditions:

a. Access is limited to classified information relating to a specific program or project;

b. The appropriate foreign disclosure authority documents that access to the specified classified information is releasable 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;

f. Personnel granted LAAs 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. A SSBI is completed favorably; where full investigative coverage cannot be completed, a counterintelligence-scope polygraph examination may 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 a LAA is justified, a commanding officer may submit a request to CNO (N09N2), Marine Corps commands will submit via HQMC (ARS), with the following information/supporting documentation:

a. The identity of the individual for whom the LAA is requested, including name, date and place of birth, current citizenship, social security number (if held),

b. Date and type of most recent PSI; (If a SSBI has not been completed within the past 5 years, a completed PSI request package must be enclosed for CNO (N09N2)'s review and submission;

c. A description of the position requiring access and the specific duties (delineated as precisely as possible) for which access is requested;

d. 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;

e. A full description of the specified classified information to be accessed, including classification;

f. A copy of the foreign disclosure authority determination for the specified classified or controlled unclassified information (CUI);

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 (Not to exceed 5 years).

3. CNO (N09N2) will review the LAA request to ensure it meets program requirements.

a. Requests that are incomplete or not properly justified will be promptly returned to the requester.

b. After ensuring that the LAA meets program parameters, CNO (N09N2) will forward the SSBI request to OPM. No authorization for access to classified information can be issued until favorable adjudication of the SSBI.

4. Individuals who have been granted a LAA will not be allowed to have access to any classified information other than that specifically authorized.

a. 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.

b. A Classified Information Nondisclosure Agreement (SF 312) must be executed by the individual prior to being granted access to classified information.

c. Individuals with LAAs will be placed under the general supervision of appropriately cleared U.S. citizens. 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.

5. LAAs are authorized for 5 years. If a LAA is required in excess of 5 years, a new request must be submitted following the procedures outlined in paragraph 2, including a completed SSBI-PR request package. CNO (N09N2) will review the new request and may approve continuation of the LAA, as appropriate, pending favorable adjudication of the completed SSBI-PR.

6. 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, again following paragraph 9-15 procedures. If the individual's SSBI is less than 5 years old, a new PSI may not be required.

#### **9-16 PERSONNEL EXCHANGE PROGRAM ACCESS**

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.

### **9-17 NATO ACCESS**

1. Personnel assigned to a NATO staff position requiring access to NATO COSMIC (Top Secret), NATO Secret, or NATO Confidential information shall have been the subject of a favorably adjudicated SSBI (10 year scope), or ANACI or NACLC, current within five years prior to the assignment in accordance with USSAN Instruction 1-69 and paragraph 9-17.2 below.

2. Personnel not assigned to a NATO staff position, but requiring access to NATO COSMIC or NATO Secret, or access to the NATO accredited SIPRNET terminals, must possess the equivalent final or interim U.S. security clearance based upon the appropriate personnel security investigation required in chapter six. However, access to ATOMAL information may not be granted based on an interim security clearance.

3. Access to NATO classified information based on a temporary access (interim security clearance) shall be subject to the following conditions:

a. Approval by the authority who is granting access to U.S. classified information based on the interim security clearance;

b. Written authorization, maintained as a record; temporary access held is at the Secret or Top Secret level;

c. Process for a final security clearance has been initiated; and

d. The individual has received and acknowledged a briefing on NATO security requirements.

e. Record access in JPAS.

### **9-18 SENSITIVE COMPARTMENTED INFORMATION (SCI) ACCESS**

1. SCI access eligibility is granted by the appropriate Senior Official of the Intelligence Community (SOIC), having cognizance of the individuals involved.

2. Within the DON, reference (d), contains the policies and procedures for access to and dissemination of SCI.

3. The Director, DON CAF, as delegated by the SOICs, is responsible for decisions rendered with respect to SCI access

eligibility or ineligibility. In addition, the Director, DON CAF is also delegated the responsibility to adjudicate DON contractor personnel requiring SCI access eligibility under the NISP and reference (d).

4. The PSAB has been delegated the authority to review final appeals of unfavorable SCI access eligibility determinations.

5. The following basic procedures apply to requests for DON CAF SCI access eligibility determinations:

a. If it is determined that SCI access is required and a valid (i.e., conducted within the past 5 years) SSBI does not exist, an SSBI (or SSBI-PR if an outdated SSBI exists) will be requested as directed by chapter 6.

b. If SCI access is required and a valid SSBI or SSBI-PR exists, the commanding officer will request a SCI eligibility determination from the DONCAF using the Joint Personnel Adjudication System (JPAS).

c. Commands are required to report the citizenship of immediate family members as reference (d) imposes additional procedural requirements for individuals with foreign national immediate family members.

d. Upon favorable adjudication of the completed SSBI, the DON CAF will update the JPAS to reflect a final SCI eligibility determination.

6. Requests for exceptions to DCID 6/4 for SCI access eligibility will be prepared as directed by reference (d) and forwarded to the DON CAF.

7. 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 (d).

a. Information that could potentially affect an individual's eligibility must be reported to the DON CAF in accordance with the procedures outlined in appendix G. The DON CAF will either reaffirm eligibility or will begin the unfavorable determinations process.

b. Commanding officers may suspend, or debrief for cause from SCI access in accordance with reference (d). Coordinate with command security manager.

c. A SSBI-PR is required every 5 years for individuals with SCI access.

8. The Commanding officer may debrief an individual from SCI access for administrative reasons as provided in reference (d). Coordinate with SSO.

**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 DoDD 5210.2, Access to and Dissemination of Restricted Data, 12 January 1978.

(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 DoDD 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 Directive 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 thermo-nuclear 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. LAA procedures apply.

(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 Directive 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 Directive 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 procedures and format for briefing/debriefing.

b. For additional guidance refer to DoD Directive 5210.2 or contact CNO (N09N2).

## **9-20 FACILITY ACCESS 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. The commanding officer has the prerogative of requesting a trustworthiness NAC or Facility Access NAC to ensure the individuals who are permitted access to command persons, property, facilities, are trustworthy.

2. Trustworthiness NACs will be requested using the SF 85P, and the FD-258 fingerprint card, and will be forwarded to OPM 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.

4. Contractor employees are not normally subjected to investigation unless access to classified information is required, in which case they are investigated and determined eligible under the National Industrial Security Program (NISP). Security clearance eligibility 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.

5. 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 judgment 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.

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

7. The procedures for requesting and receiving the results of a FAD NAC mirror the procedures for requesting and receiving the results of trustworthiness NAC.

a. 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 will be forwarded to OPM to conduct the NAC.

b. The completed NAC will be 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, and record in JPAS.

8. 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 OPM investigative data protected under the Privacy Act should be referred to OPM.

## 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 that may be relevant to a security clearance determination.

a. Individuals are required to report to their supervisor or appropriate security official and seek assistance for any incident or situation that could affect their continued eligibility for access to classified information. Individuals shall be initially and periodically briefed thereafter, to ensure familiarity with pertinent security regulations and the standards of conduct required of individuals holding positions of trust. The ultimate responsibility for maintaining eligibility to access classified information rests with the individual. Reporting requirements for individuals with SCI access authorization are contained in reference (d).

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 EMPLOYEE EDUCATION AND ASSISTANCE PROGRAM**

1. EO 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 employees 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 issues.

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 (OCA), security managers, security specialists and all other personnel whose duties significantly involve the creating, handling, or management of classified information, EO 12958, reference (a), 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/Office of Civilian Human Resources (ODASN(CP/OCHR) 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 shall report that information to the DON CAF, via JPAS. Commands will report all information that meets the exhibit 10A standards without attempting to apply or consider any mitigating factors what may exist.

2. When reporting unfavorable information commands are encouraged to provide full coverage and detail 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 9-7. When suspending SCI access, reference (d) 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 re-indoctrination into SCI access) until clearance eligibility has been re-established 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 investigations.

5. The DON CAF will evaluate and adjudicate all reported information and promptly notify the command 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 investigation request forms to the DON CAF in order to open an investigation at OPM to resolve outstanding or missing information.

**10-6 AUTOMATED CONTINUOUS EVALUATION SYSTEM (ACES)**

1. ACES is a DoD tool to automatically query government and commercial databases between periodic reinvestigation cycles in order to detect serious, yet unreported, issues of security concerns. ACES uses established adjudication criteria to identify issues, such as financial anomalies, criminal incidents and foreign connections. ACES then generates a detailed issue report which is forwarded via the JPAS to the DON CAF for DON personnel.

2. ACES reinforces the DON continuing evaluation program reporting requirements, it DOES NOT replace them. ACES does not require a personnel interview, a personnel security questionnaire, or an information release form prior to query.

3. Personnel and commands will not be notified before an ACES search is conducted, however DON CAF may contact command and/or personnel subsequent to an ACES query to obtain information to complete an ACES developed issue report.



**EXHIBIT 10A**

**CONTINUOUS EVALUATION CHECK SHEET**

1. When questionable or unfavorable information becomes available concerning an individual who has been granted access, or who has eligibility to classified information or assigned to sensitive duties, commands will report that information to the DON CAF, via JPAS. Commands shall 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 U.S. 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 that 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 investigation request package. OPM will conduct a RSI to gather the necessary information. The RSI results will be returned to the DON CAF for adjudication.

## CHAPTER 11

### VISITOR ACCESS TO CLASSIFIED INFORMATION

#### 11-1 BASIC POLICY

1. For the purposes of this policy manual, 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.

2. The movement of all visitors shall be controlled to ensure that access to classified information is deliberate and consistent with the purpose of the visit. If an escort is required for the visitor, a military, civilian or a cleared contractor assigned to the command being visited may be assigned escort duties.

3. 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.

4. 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, or controlled unclassified information (CUI) may be divulged to the general public). A written statement of command safeguards will

be prepared and implemented assuming the possibility of the presence of foreign agents among the visitors and ensuring proper protections are in place.

5. Visit Authorization Letters (VAL) are no longer required for visits involving civilian, military and contractor personnel whose access level and Security Management Office (SMO) affiliation are accurately reflected in JPAS.

#### **11-2 CLASSIFIED VISITS**

1. Commanding officers shall establish procedures to accommodate visits to their commands involving access to, or disclosure of, classified information. As a minimum these procedures will include verification of identity, validation of personnel security clearance eligibility, and access using JPAS, and a need-to-know determination.

2. The command sponsoring the visitor is responsible for ensuring the visitor's eligibility, access, and affiliation data are current and accurate in JPAS.

3. In addition to requirements for authorizing access to classified information, the visited command must also fulfill the local facility access and general visit control requirements. If local conditions necessitate formal visit request letters for visit/access control purposes, the command sponsoring the visitor must comply with local facility access requirements.

4. Visits involving access to and dissemination of Restricted Data, or to facilities of the DOE, are governed by the policies and procedures in DoD Dir 5210.2 of 12 January 1978 (NOTAL).

#### **11-3 VISITS BY FOREIGN NATIONALS AND REPRESENTATIVES OF FOREIGN ENTITIES**

1. Consult SECNAVINST 5510.34A concerning foreign visitors, whether or not the visitor requires access to classified, or CUI or material.

2. 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. Official requests

must be submitted by the applicable foreign government (normally its Washington, D.C. embassy), certifying the visitor's 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 may be made. Immediately thereafter, the OLA will be informed of the visit and the extent of the disclosure of information provided. In case there is a question as to whether particular classified information may be furnished to a member of congress, the commanding officer will release the information and will immediately contact the SECNAV 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 7-8.5 applies.

#### **11-5 CLASSIFIED VISITS BY REPRESENTATIVES OF THE GENERAL ACCOUNTING OFFICE**

1. Properly investigated, adjudicated 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 some exceptions.

a. 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 eligibility of each GAO representative.

b. Occasionally, GAO representatives in the Washington metropolitan area receive assignments - such as Congressional requests - which preclude the usual advance notice of visit, and verbal arrangements are made for visits. To assist the GAO in those instances, the DON commands will verify eligibility and

access requirements through Director, Audit and Cost Management Division, (NAVINSGEN 4).

c. As exceptions to the procedures described above:

(1) Commanding officers will not grant access to documents and information specified as not releasable or requiring approval of the SECNAV for release, enclosure (1) to SECNAVINST 5740.26B, Relations with the General Accounting Office (GAO) (NOTAL).

(2) Requests for classified defense information in the area of tactical operations and intelligence collection and analysis will be sent to the Comptroller of the Navy (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.

2. Questions and problems concerning clearances of individuals and release of classified information in connection with visits of the GAO will be addressed to the NAVINSGEN 4.

## **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.

#### **Account Manager**

The individual responsible for establishing local JPAS access and monitoring and controlling system access thereafter. The security manager is unusually the JPAS account manager.

#### **ACES**

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

**Active Duty/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 USC. 105, the "military departments" as defined in 5 USC. 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.

**Attestation**

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

**Authorized Investigative Agency**

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

**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 (EO) 12958, or any successor order, EO 12951, or any successor order, or the Atomic Energy Act of 1954 (42 USC. 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 eligibility standards and is thus afforded access to classified information. There are three types of clearances: Confidential, Secret, and Top Secret. A Top Secret clearance implies an individual has been determined by an authorized adjudicative authority to be eligible for access to Top Secret, and has access to the same; a Secret clearance implies an individual has been determined to be eligible for Secret, and has access to the same; and a Confidential clearance implies an individual has been determined to be eligible for access to Confidential, and has access to the same.

**Clearance Eligibility**

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

**Cleared Contractor**

Any industrial, educational, commercial, or other entity, grantee, or licensee, including an individual, that has executed an agreement with the Federal Government 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 eligibility 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 that 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)

**Continuous Evaluation**

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

**Continuous Service**

Includes honorable active duty; attendance at the military academies; membership in ROTC scholarship program; Army and Air Force National Guard membership; service in the military Ready Reserve forces (including active status); civilian employment in government service, employment with a cleared contractor or employment as a consultant with access to classified information under the National Industrial Security Program. For security clearance purposes continuous service is maintained despite changes from one of the above statuses to another as long as there is no single break in service greater than 24 months.

**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 thermo-nuclear or implosion type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive material by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test or replace.

**Defense Central Index of Investigations (DCII)**

Previously referred to as the Defense Clearance and Investigations Index, the DCII is the single, automated, central DoD repository that identifies investigations conducted by DoD investigative agencies.

**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.

**Due Process**

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

**Eligibility**

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

**Employee**

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

**Entrance National Agency Check (ENTNAC)**

An FBI fingerprint check conducted on first term military enlistees

**e-Qip**

The Electronic Questionnaires for Investigations Processing is a software system developed by OPM which allows applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to their

employing agency or security management office for review and approval of the personnel security investigation request.

**Exception**

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

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

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

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

**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 (US Coast Guard, Federal Aviation Administration, Maritime Administration), and Treasury (US Customs Service, Internal Revenue Service, US Secret Service). Among the independent establishments and government corporations are Office of Personnel Management, Central Intelligence Agency, General Services Administration, US 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.

**For Official Use Only (FOUO) information**

Unclassified sensitive Information that may be exempt from mandatory public disclosure under the Freedom of Information Act (FOIA) (see Sensitive Data).

**Foreign Government Information**

Sensitive information provided by a foreign government or governments, an international organization of governments or any element thereof, with the expectation that the information or source of the information, or both, are to be held in confidence.

**Foreign National**

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

**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.

**Incident Report**

A report of developed issue information forwarded to the CAF through JPAS.

**Information Technology (IT)**

Any equipment or interconnected system or subsystem of IT equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

**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 Access/Clearance** (See Temporary Access)

**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 that has been compromised or subjected to compromise.

**Least Privilege**

A security requirement in which users are strictly limited and contained and have access only to the information and functions to which they are specifically entitled and nothing more. Least Privilege in the IT environment is synonymous with technically prescribed Need-to-Know.

**Limited Access Authorization (LAA)**

Authorization for access to Confidential or Secret information granted by the Chief of Naval Operations (N09N2) to non-US 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.

**Limited Privileged Access**

Privileged access with limited scope, e.g., an authority to change user access to data or system resources for a single information technology system or physically isolated network.

**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/Issue 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 (NACLIC)**

The personnel security investigative requirement developed under EO 12968 for persons who will require access to Secret and Confidential classified information. A NACLIC covers the past 5 years and consists of a NAC, a financial review, certification of date and place of birth, and LACs. The NACLIC is the minimum investigative requirement for military service, and is the reinvestigative requirement for continued access to Secret and Confidential classified information (sometimes previously referred to as a Secret PR (SPR) or Confidential PR (CPR)).

**National Industrial Security Program (NISP)**

National program to safeguard classified information that is released to contractors, licensees, and grantees of the US Government. The NISP is a single, integrated, cohesive industrial security program to protect classified information and preserve US 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 US 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 US 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 non-appropriated fund instrumentalities.

**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 US 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.

**Nondisclosure Agreement (NdA)**

An agreement between an individual who will be permitted access to classified national security information and the United States government, acknowledging and agreeing to obligations for protecting national security information. All personnel must execute the Standard Form 312 Nondisclosure Agreement as a condition of access to classified information.

**Non-Privileged Access**

IT Access that provides no capability to alter the properties, behavior or control of the information system/network. Also known as "User level access," non-privileged access is typically controlled and limited to preclude intention or unintentional adverse impact to sensitive data or other resources within the IT environment.

**Non US Citizen.**

Any person who is not a US citizen or US national, usually used when referring to DON employees or affiliates who are not U.S. citizens (see United States Citizen).

**Personnel Identifying Data**

Personal information, e.g., date and place of birth, SSN, citizenship, used to identify an individual on personnel

security questionnaire and in personnel security automated systems such as JPAS.

**Personnel Security Investigation (PSI)**

Any investigation conducted for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DoD, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties or access requiring such investigation. PSIs are conducted for the purpose of making initial personnel security determinations and to resolve allegations that may arise subsequent to a favorable personnel security determination to ascertain an individual's continued eligibility for access to classified information or assignment or retention in a sensitive position.

**Privileged Access**

Authorized access that provides capability to alter the properties, behavior or control of the information system/network. It includes, but is not limited to: "Super user," "root," or equivalent access, such as access to the control functions of the information system/network, administration of user accounts, etc; access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multi-plexers, and other key information system/network equipment or software; ability and authority to control and change program files, and other users' access to data; direct access to operating system level functions (also called unmediated access) which would permit system controls to be bypassed or changed; access and authority for installing, configuring, monitoring or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operation.

**PSAB**

The Personnel Security Appeals Board (PSAB) is the appellate authority for appeals of unfavorable DON CAF eligibility determinations.

**Reciprocity**

Acceptance by one agency or program of a favorable security clearance eligibility determination, made by another. Reciprocity does not include agency access determinations or employment suitability determinations.

**Reinvestigation**

An investigation conducted for the purpose of updating a previously completed investigation of persons occupying sensitive positions, afforded access to classified information or assigned other duties requiring reinvestigation. The intervals of reinvestigation are dependent upon the sensitivity of the position or access afforded. A periodic reinvestigation of an SSBI is conducted at five-year intervals; a reinvestigation of a NACLIC for Secret or Confidential access is conducted respectfully at 10 year and 15 year intervals.

**Reimbursable Suitability Investigation (RSI)**

Required to prove or disprove allegations concerning an individual on whom a PSI has been conducted. SII requests are requested by the DON CAF, commands will obtain an SF 86 as directed by the DON CAF. DON CAF will coordinate the investigative effort.

**Scope**

The time period to be covered and the sources of information to be obtained during the prescribed course of a PSI.

**Secret Periodic Reinvestigation (SPR)**

AN OBSOLETE TERM. Replaced by the NACLIC, which is conducted at 10-year intervals for the purpose of updating a previously completed NAC, ENTNAC, NACI, ANACI, or NACLIC.

**Security**

A protected condition that prevents unauthorized persons from obtaining classified information of direct or indirect military value. This condition results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influence.

**Security Clearance Eligibility (See Clearance)**

**Security Management Office (SMO)**

For purposes of JPAS, a Security Management Office is a local entity that has personnel security management jurisdiction.

**Security Violation**

Any failure to comply with the regulations for the protection and security of classified material.

**Senior Official of the Intelligence Community (SOIC)**

The heads of organizations within the intelligence community as defined by EO 12333, or their designated representatives.

**Sensitive Compartmented Information (SCI)**

Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

**Sensitive Duties**

Duties in which an assigned military member or civilian employee could bring about, by virtue of the nature of the duties, a material adverse affect on the national security. Any duties requiring access to classified information are sensitive duties.

**Sensitive Information**

Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine DON payroll, finance, logistics, inventory, and personnel management systems. Examples include FOUO, Unclassified Technical Data, State Sensitive but Unclassified (SBU), or Foreign Government information.

**Sensitive Position**

Any position so designated, in which the occupant could bring about, by virtue of the nature of the position, a materially adverse affect on the national security. All civilian positions within the DoD are designated special-sensitive, critical-sensitive, noncritical-sensitive, or non-sensitive.

**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 individual's life 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 DSS term that is no longer used in the clearance investigative process. The current OPM term is RSI.

**State Sensitive But Unclassified (SBU)**

Sensitive information that originated from the Department of State (DoS) that has been determined to be SBU under appropriate DoS information security policies.

**Substantial Issue Information - (See Issue Information)**

**Temporary Access**

A local determination to allow temporary access to classified information based on the favorable minimum investigative requirements, pending the completion of the full investigative requirements. (Temporary access to Sensitive Compartmented Information cannot be approved locally and must be requested from the DON CAF).

**Transmission**

Any movement of classified information or material from one place to another.

**Unclassified Technical Data**

Sensitive data related to military or dual-use technology, which is subject to approval, licenses or authorization under the Arms Export Control Act.

**Unfavorable Administrative Action**

Action taken as the result of an unfavorable personnel security determination including a denial or revocation of security clearance eligibility; denial or revocation of access to classified information, denial or revocation of a SAP or SCI access authorization; non-appointment to or non-selection to a sensitive position.

**Unfavorable Personnel Security Determination**

A determination based on an assessment of available information that an individual does not meet the standards required for access to classified information or assignment to sensitive duties.

**Unauthorized Disclosure**

A communication or physical transfer of classified information to an unauthorized recipient.

**United States Citizen (to include US 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 United States citizens, and a person who has met the requirements for citizenship as determined by the Immigration and Naturalization Service and has taken the requisite oath of allegiance.

**United States National**

A United States citizen, or a person who, though not a citizen of the United States, owes permanent allegiance to the United States. NOTE: Consult 8 USC. 1401(a)(1-7) whenever there is doubt whether a person qualifies as a national of the United States.

**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/ANCI - Access National Agency Check with Inquiries  
BI - Background Investigation  
BUPERS - Bureau of Naval Personnel  
CAF - Central Adjudication Facility  
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 States  
COR - Contracting Officer's Representative (formerly Contracting Officer's Security Representative)  
CPR - Confidential Periodic Reinvestigation  
CS - Critical-Sensitive  
CSA - Cognizant Security Agency

CSO - Cognizant Security Office  
CUSR - Central U.S. Registry  
DCI - Director, Central Intelligence  
DCID - Director, Central Intelligence Directive  
DCII - Defense Central Investigations Index  
DCPDS - Defense Civilian Personnel Data System  
DAA - Designated Approval Authority  
DEERS - Defense Enrollment Eligibility Reporting System  
DFAS - Defense Finance & Accounting Service  
DIA - Defense Intelligence Agency  
DIRNCIS - Director, Naval Criminal Investigative Service  
DISCO - Defense Industrial Security Clearance Office  
DNI - Director of Naval Intelligence  
DOB - Date of birth  
DoD - Department of Defense  
DOE - Department of Energy  
DOHA - Defense Office of Hearings and Appeals  
DON - 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  
EO - Executive Order  
EOD - Explosive Ordnance Disposal  
EPSQ - Electronic Personnel Security Questionnaire  
E-QIP - Electronic Questionnaires for Investigations Processing  
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  
IA - Information Assurance  
IAM - Information Assurance Manager  
IAO - Information Assurance Officer  
IBI - Interview oriented Background Investigation  
INFOSEC - Information Security  
INS - Immigration and Naturalization Service  
IRR - Inactive Ready Reserves

ISIC - Immediate Superior in Chain of Command  
ISOO - Information Security Oversight Office  
ISP - Information Security Program  
ISSM - Information Systems Security Manager  
IT - Information Technology  
JAG - Judge Advocate General of the Navy  
JAMS - Joint Adjudication Management System  
JCAVS - Joint Clearance and Access Verification System  
JCS - Joint Chiefs of Staff  
JPAS - Joint Personnel Adjudication System  
LAA - Limited Access Authorization  
LBI - Limited Background Investigation  
LOI - Letter of Intent  
LOD - Letter of Decision  
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  
NACLK/NCL- National Agency Check with Local Agency Checks and  
Credit Check

NAF - Non-appropriated Fund

NAFI - Non-appropriated Fund Instrumentalities

NASA - National Aeronautics and Space Administration

NATO - North Atlantic Treaty Organization

Navy IPO - Navy International Programs Office

NCC - National Computer Center (within DSS)

NCIC - National Crime Information Center

NCIS - Naval Criminal Investigative Service (Formerly  
NIS/NSIC/NISCOM)

NCS - Noncritical-Sensitive

NdA - Nondisclosure Agreement

NISP - National Industrial Security Program

NISPOM - National Industrial Security Program Operating Manual

NJAG - Navy Judge Advocate General

NMCI - Navy and Marine Corps Intranet

NNPI - Naval Nuclear Propulsion Information

NRC - Nuclear Regulatory Commission

NRO - National Reconnaissance Office

NSA - National Security Agency

NSC - National Security Counsel

NSDD - National Security Decision Directive

NSG - Naval Security Group

NSI - National Security Information

OASDOCB - Operations Center, Columbus (Formerly Defense  
Investigative Service Clearance Office (DISCO))

ODCR - Officer Distribution Control Report

OGC - Office of the General Counsel

OMB - Office of Management and Budget

OMT - Office of Mission Training (Formerly Department of Defense Security Institute (DoDSI))

ONI - Office of Naval Intelligence

OPLOC - Operating Locations (formerly Cognizant Security Office)

OPF - Official Personnel Folder (civilians)

OPM - Office of Personnel Management

OPM-FISD - Office of Personnel Management - Federal Investigative Services Division

OPNAV - Staff Offices of the Chief of Naval Operations

OSD - Office of the Secretary of Defense

PCC - Policy Coordinating Committee

PCS - Permanent Change of Station

PEP - Personnel Exchange Program

PID - Personnel Identification Data

POB - Place of Birth

POC - Point of Contact

PR - Periodic Reinvestigation

PRP - Nuclear Weapon Personnel Reliability Program

PSA - Presidential Support Activities

PSAB - Personnel Security Appeals Board

PSI - Personnel Security Investigation

PSM Net - Personnel Security Management Network

PSQ - Personnel Security Questionnaire  
PSP - Personnel Security Program  
PSQ - Personnel Security Questionnaire  
RD - Restricted Data  
RRU - Request to Research/Recertify/Upgrade Eligibility  
RSI - Reimbursable Suitability Investigation  
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 (Obsolete)  
SMO - Security Management Office  
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  
STAAT - Security Training, Assistance, Assessment Team  
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  
U.S. - United States  
U.S.C. - United States Code  
USD(CI&S) - Under Secretary of Defense (Counterintelligence &  
Security  
USD(P) - Under Secretary of Defense for Policy  
USD/I - Under Secretary of Defense for Intelligence  
USIS - U.S. Investigative Service  
USO - United Service Organization  
USSAN - United States Security Authority, NATO  
WHS - Washington Headquarters Service



## APPENDIX C

### GUIDELINES FOR COMMAND SECURITY POLICY MANUAL

1. A written command security policy manual or written procedures are necessary to ensure the security requirements contained herein are established for local command operations. In composing a command security policy manual 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 policy manual; rather the procedures should supplement the DON ISP and PSP, and other directives. The guidelines that follow may be helpful in developing the PSP portions of your command security policy manual.

a. The introduction to the command security policy manual should cover the purpose of the policy manual, its applicability to all in the command and its relationship to other directives.

b. The majority of the command policy manual 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 (e.g., 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 policy manual. Identify personnel responsible for the security education program

including specific areas of responsibility (e.g., 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 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 Judge Advocate General (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 investigation requests.

(9) Establish procedures for documenting clearance and command access in JPAS.

(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 PSP, 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 (e) 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. What versions of the SECNAVINST 5510.30 (series) and SECNAV M-5510.30 does the command hold?
2. What other references applicable to its security program does the command hold and use?
3. Provide the document that establishes or announces commands security organization and demonstrates the security manager as having direct and ready access to the commanding officer.
4. Provide the security manager designation letter and the forwarding letter to demonstrate that a copy of the letter was forwarded to CNO (N09N2).
5. Provide evidence of formal security management training.
6. Provide the document or announcement that identifies the security manager by name to all command personnel.
7. Provide examples of security management functions that demonstrate overall management of the program.
8. How many persons are assigned duties and responsibilities to support the command's security program, what are their duties and how do they report to the security manager?
9. Are all program requirements sufficiently covered by assigned security personnel?
10. How do the SSO, IAM, and security manager coordinate and cooperate in the command program?
11. Provide a copy of the most current written command security procedures.
12. Provide a copy of the most current written command emergency plan.
13. Provide a copy of any written security servicing agreements.
14. Explain any security services provided by the command including inspection, evaluation, education, or assist visits.

15. Provide a copy of any written assessments or evaluations of subordinate command security programs.
16. Who conducted the evaluation or inspection of subordinate command security program and what are the inspector's qualifications?
17. Provide follow-up reports and corrective actions taken to address discrepancies noted during assessments and assist visits.
18. Provide any command generated or designed security awareness or education plans.
19. Provide evidence that security education materials were coordinated with CNO (N09N2), when required.
20. Provide the format or requirements for the indoctrination briefings.
21. Provide the format or requirements for the orientation briefings.
22. Describe on-the-job security training that is provided.
23. Provide the format or requirements for the annual refresher briefings.
24. Describe the attestation process used and provide a roster of individuals who have completed their attestation.
25. When was the last time a counterintelligence briefing was given and what is the command policy on these?
26. When was the last time a foreign travel briefing was given and what is the command policy on these?
27. Provide documentation that briefings have been accomplished for all personnel with SIPRNET, NATO, SIOP-ESI or CNWDI access.
28. Provide the commands Security Termination Statement procedures.
29. Which of the briefings include awareness training on the administrative and legal sanctions that military and civilian personnel are subject to for knowingly, willfully, or negligently committing security violations?

30. Provide copies of any 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. Explain any counterintelligence matters that have been reported to the NCIS.
32. Which briefing is used to advise all personnel 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 targets of exploitation by a foreign entity?
33. Provide any notifications made to NCIS of unauthorized absentees.
34. How many non-U.S. citizens are employed at command and what security procedures are in place to limit access?
35. How many non-U.S. citizens are assigned to sensitive duties and provide a copy of the waiver approval permitting the assignment.
36. How are non-U.S. citizens and others who are ineligible for access to classified information identified to other command personnel?
37. Provide a copy of the IT position designations for the command.
38. Provide a roster of employees assigned to sensitive positions including the date of the favorable DON CAF eligibility determination.
39. How is U.S. citizenship verified and what are the rules followed to determine U.S. citizenship prior to requesting PSI?
40. How many non-sensitive positions does the command have and do any persons in non-sensitive positions have access to a DON IT system?
41. How does the command determine if a PSI is required?
42. What type of local checks are done to assure that only trustworthy persons have access to classified information or are

assigned to sensitive duties?

43. What investigation requests have been submitted this year and what is the current status?

44. How often does the command check on the status of an investigation request?

45. How many requests have been returned due to error this year and how long did it take to correct and resubmit the request?

46. What procedures are used to prepare PSI requests?

47. Did you have any persons who transferred after a PSI was requested and what did you do about the pending PSI request?

48. How do you store and control access to investigation reports?

49. How do you record local security information and how do you use personnel records?

50. How do you determine if a prior investigation or eligibility determination exists?

51. What security criteria and adjudication guidelines are applied in your local personnel security determinations?

52. How do you handle adverse personnel security information that develops on assigned personnel?

53. Explain your continuous evaluation program.

54. How are temporary access determinations made and recorded?

55. How are routine access determinations made and recorded?

56. How are one-time access determinations made and recorded?

57. Do you have NATO billets or NATO information and how is access determined and recorded?

58. Do you have any personnel who are currently undergoing or have undergone an unfavorable determinations process and explain your role in this process?

59. How is need-to-know observed?

60. How are visitors identified and controlled?
61. How many classified visits have you had and how is eligibility verified for visitors?
62. Explain your process for completing the Classified Information Nondisclosure Agreements, Standard Form 312.
63. Do you manage special access information and how is access managed, controlled and recorded?
64. Provide any Limited Access Authorizations currently in effect at your command.
65. How many persons have JPAS access at your command and how is their access controlled and monitored?

## APPENDIX E

### JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS)

#### E-1 POLICY

1. The Joint Personnel Adjudication System (JPAS) is the automated system of record for personnel security management within the DoD, providing a means to record and document personnel security actions. JPAS facilitates PSP management for the DoD Central Adjudication Facilities (CAF's), for DoD security managers, and SCI program managers. JPAS interfaces with the DSS and the OPM to provide PSI data, and the various DoD personnel systems to include the Defense Enrollment Eligibility Reporting System (DEERS) and Defense Civilian Personnel Data System (DCPDS) to provide personnel identifying data.

2. JPAS is the system of record for documenting the personnel security adjudicative and management process, to include position sensitivity determinations, PSI history and current status, adjudicative eligibility determinations history and current status, exceptions (if the eligibility determination was based on a condition, deviation from prescribed investigative standards or waiver of adjudication guidelines), access history and current status, reports of security-related incidents including issue files, suspension of access, denial or revocation of eligibility, eligibility recommendations or decisions made by an appellate authority, nondisclosure execution dates, indoctrination date(s), security briefing and debriefing date(s) and rationale.

#### E-2 APPLICATIONS

1. JPAS has two applications. The Joint Adjudication Management System (JAMS) and the Joint Clearance and Access Verification System (JCAVS).

a. JPAS is the application that supports the central adjudication facilities in recording and maintaining security eligibility determinations and provides the capability to communicate with command security personnel.

b. JCAVS is the application that supports command security personnel providing capabilities such as communication links with the CAFs, e-QIP links to submit investigation requests, and records keeping capabilities. JCAVS provides data such as civilian position sensitivity levels, PSI history, status of



current adjudicative actions, security clearance eligibility and access determinations, non-disclosure execution dates, indoctrinate dates, to assist in local command program management.

2. JPAS is linked to other systems such as Defense Central Index of Investigations (DCII) and the Automated Data Warehouse and DSS' internal management systems to comprise "System X," DoD's automated tool supporting the reengineered DoD PSP.

3. JPAS provides program management reports to JCAVS and JAMS users and to DSS program managers, as required, using pre-programmed formats supported by system data.

### **E-3 COMMAND LEVEL SYSTEM USE**

1. DON commands must use JCAVS exclusively to document local access determinations (temporary access/interim clearance, access upgrades and downgrades, suspensions and withdrawals). Commands must document execution of nondisclosure agreements and verbal attestation. JCAVS will be used to communicate with the DON CAF, to submit continuous evaluation reports, to pass/receive visit requests, to determine security clearance and SCI access eligibility, to determine status of requested PSI, to record PSI submission dates and request DON CAF determinations.

2. JCAVS replaces all records keeping requirements associated with PSP management activities.

### **E-4 SYSTEM ACCESS**

1. JCAVS accounts may be provided to personnel determined by the command JCAVS manager (normally the security manager) to require access to perform assigned duties.

2. Personnel requiring system access must be the subject of a favorably adjudicated NACLIC (ANACI for civilians) with Secret security clearance eligibility established by a DoD CAF. Personnel with Secret security clearance eligibility established using other investigations, which were valid prior to 1999, will be permitted access to JCAVS provided a NACLIC or an ANACI has been requested, as appropriate, and JPAS reflects that the investigation request is open.

3. Prior to authorizing JCAVS account access, personnel must download, complete and sign the JCAVS System Access Request (SAR) form found on the JPAS gateway at <https://JPAS.dsis.dod.mil>.

Security managers will function as account managers for their command, and will approve, register and monitor command staff accounts, as appropriate.

4. To initialize a security manager/account manager account for a command, the account approval and registration will be hierarchically processed by the security manager/account manager of the Immediate Senior Activity in the Chain of Command (ISIC). All second echelon command account managers will approve and register their subordinate third echelon commands; third echelon command account managers will approve and register their subordinate fourth commands, etc.

5. The completed and signed JCAVS SAR is an official record authorizing system access. Account managers will maintain the form on file for all approved accounts for the duration of account assignment and for an additional one year after transfer of the individual and/or removal of the account.

6. JCAVS accounts may not be transferred from one command to another. The account must be removed prior to transfer or separation of the individual.

7. Security manager/account managers are responsible for ensuring proper and secure system use. Noncompliance with rules, procedures, guidelines or regulations pertaining to the security of the JPAS system, use of accounts or account passwords, or the integrity of the JPAS data, will be reported to the appropriate CAF as a personnel security issue requiring adjudication. Security managers/account Managers will take appropriate steps to see that JPAS access is removed and accounts are terminated, as appropriate.

8. The DON JCAVS User's Manual may be accessed on the CNO(N09N2) web page at [www.navysecurity.navy.mil](http://www.navysecurity.navy.mil) (click on JPAS/JCAVS). Notices of JCAVS training can also be found on the web page at [www.dss.mil/training/index](http://www.dss.mil/training/index), which provides notices of training presented by DSS.

## APPENDIX F

### CITIZENSHIP REQUIREMENTS

#### F-1 POLICY

1. Only U.S. citizens are eligible for a security clearance, assignment to sensitive duties, national security positions 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 LAA (see chapter 9) under special procedures.
2. When this policy manual refers to U.S. citizens, it makes no distinction between those who are U.S. citizens by birth, those who have derived U.S. citizenship or those who acquired it through naturalization.

#### F-2 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 verified before processing a PSI request. 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 documentation verifying U.S. citizenship status prior to commissioning. Likewise, enlistees are required to submit documentation verifying U.S. citizenship status during enlistment processing. Evidence of source documents sighted as proof of citizenship is maintained in service records for two years and, if available, can be used by security officials to verify citizenship for future requirements.
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 an appointment can be effected. Previously hired employees were not required to submit proof of U.S. citizenship. The document used by personnel offices as verification 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 4 below.

4. All documents submitted as evidence of U. S. citizenship **must be original documents or certified copies**. Uncertified copies are not acceptable. The following documents are acceptable proof of citizenship:

a. The original U. S. birth certificate with a raised seal issued at the time of birth from one of the 50 states, or outlying territories or possessions.

b. A hospital birth certification (clinic and commercial birth center certification is not permitted) with an authenticating raised seal or signature provided all vital information is given.

c. A delayed birth certificate provided it shows the birth record was filed within one year after birth, it bears the registrar's seal and signature, and cites secondary evidence such as a baptismal certificate, certificate of circumcision, affidavits of persons having personal knowledge of the facts of the birth or other official records such as early census, school or insurance.

d. U.S. Passport (current or expired) or U.S. passport issued to individual's parent in which the individual is included.

e. FS-240 Report of Birth Abroad of a Citizen of the United States of America/Consular Report of Birth.

f. FS-545 Certification of Birth issued by a U.S. Consulate or DS-1350 the Department of State Certification.

g. INS N-550/570 U.S. Immigration and Naturalization Service Naturalization Certificate.

h. INS N-560/561 U.S. Immigration and Naturalization Service Certificate of Citizenship. If the individual does not have a Certificate of Citizenship, the original 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 October 1978) and residing permanently in the U.S.

i. Certificate of birth issued by the Canal Zone government indicating U.S citizenship is only acceptable if verified by direct government inquiry to: Vital Records Section, Passport Services, 1111 19th Street NW, Suite 510, Washington, D.C. 20522-1705.

j. DD 372, Verification of Birth is acceptable for military members (officer and enlisted) provided the birth data is listed and verified by the Department of Vital Statistics.

k. DD 1966, Application for Enlistment into the Armed Forces of the United States are acceptable provided the documents sighted are listed and attested to by a recruiting official.

5. If none of the above forms of evidence are obtainable, a notice from the registrar issued by the state with the individual's name, date of birth, which years were searched for a birth record and that there is no birth certificate on file for the applicant should be presented. \*The registrar's notice must be accompanied by the best combination of the following secondary evidence:

- a. Baptismal certificate
- b. Census record
- c. Certificate of circumcision
- d. Early school record
- e. Family Bible record
- f. Doctor's record of post-natal care
- g. Newspaper files and insurance papers

*\* NOTE: These documents must be early public records showing the date and place of birth, created within the first five years of life. The individual may also submit an Affidavit of Birth, Form DSP-10A, from an older blood relative, i.e., a parent, aunt, uncle, sibling, who has personal knowledge of the birth. It must be notarized or have the seal and signature of the acceptance agent.*

### F-3 LIMITATIONS ON NON-US CITIZENS

1. **"Non-US 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 foreign liaison officers, exchange personnel, cooperative program personnel, 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 5510.34A, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations and Foreign Representatives, 8 October 2004 (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) that 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 5-6 for processing non-U.S. citizens in sensitive positions.

## APPENDIX G

### ADJUDICATION GUIDELINES

1. The following adjudication guidelines are established for all U.S. government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information and/or assignment to sensitive national security positions. They apply to persons being considered for initial or continued eligibility for assignment to sensitive positions and/or access to classified information, to include SCI and SAPs and are to be used by government departments and agencies in all final clearance determinations.

2. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

- a. The nature, extent, and seriousness of the conduct,
- b. The circumstances surrounding the conduct, to include knowledgeable participation,
- c. The frequency and recency of the conduct,
- d. The individual's age and maturity at the time of the conduct,
- e. The voluntariness of participation,
- f. The presence or absence of rehabilitation and other pertinent behavioral changes,
- g. The motivation for the conduct,

h. The potential for pressure, coercion, exploitation, or duress, and

i. The likelihood of continuation or recurrence.

3. Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

4. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

- a. Allegiance to the United States,
- b. Foreign influence,
- c. Foreign preference,
- d. Sexual behavior,
- e. Personal conduct,
- f. Financial considerations,
- g. Alcohol consumption,
- h. Drug involvement,
- i. Emotional, mental, and personality disorders,
- j. Criminal conduct,
- k. Security violations,
- l. Outside activities, and
- m. Misuse of Information Technology

5. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment,



irresponsibility, or emotionally unstable behavior. Notwithstanding, the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

6. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

- a. Voluntarily reported the information,
- b. Was truthful and complete in responding to questions,
- c. Sought assistance and followed professional guidance, where appropriate,
- d. Resolved or appears likely to favorably resolve the security concern,
- e. Has demonstrated positive changes in behavior and employment, or
- f. Should have his or her access temporarily suspended pending final adjudication of the information.

7. If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

### 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; or

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 person 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 that 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; or
- 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. Contact with foreign citizens is 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, or

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. Exercising dual citizenship,
- b. Possessing and/or using 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, or
- 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; or
- 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, including violation of any written or recorded agreement made between the individual and the agency; or

f. Association with persons involved in criminal activity.

**Conditions that could mitigate security concerns include:**

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; or

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, or
- 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; or
- 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; or
- 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, or
- 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); or

(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, or

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; or
- 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.

*\* Under the provisions of 10 U.S.C. 986, any person who is an unlawful user of, or is addicted to, a controlled substance as defined in section 102 of the Controlled Substances Act (21 U.S.C. 802), may not be granted or have renewed their access to classified information.*

## **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. An 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; or
- 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; or
- 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.

***\* Under the provision of 10 U.S.C. 986, any person who is mentally incompetent, as determined by a credentialed mental health professional approved by the Department of Defense, may not be granted or have renewed their access to classified information.***

## 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;
- c. Conviction in a Federal or State court, including a court martial of a crime, sentenced to imprisonment for a term exceeding one year and incarcerated as a result of that sentence for not less than a year; or \*1
- d. Discharge or dismissal from the Armed Forces under dishonorable condition. \*2

**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; or
- f. There is clear evidence of successful rehabilitation.
- g. Potentially disqualifying conditions c and d, above, may not be mitigated unless, where meritorious circumstances exist, the officials designated by the Secretary of Defense or the Secretary of the Military Department concerned or as delegated has granted a waiver.

***\*1 Under the provision of 10 U.S.C. 986, a person who has been convicted in Federal or State court, including courts martial, sentenced to imprisonment for a term exceeding one year and incarcerated for not less than one year, may not be granted or have***

*renewed their access to classified information. In a meritorious case the officials designated by the Secretary of Defense, or the Secretary of the Military Department concerned, or as delegated, may authorize a waiver of this prohibition.*

*\*2 Under the above mentioned statute, a person who has received a dishonorable discharge or has been dismissed from the Armed Forces may not be granted or have renewed their access to classified information. The same waiver provision also applies.*

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 or
- 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; or
- 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; or
- 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 or
- b. The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

**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; and
- 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; and
- e. The misuse was followed by a prompt, good faith effort to correct the situation.

**INDEX**

**PARAGRAPH**

**A**

Acronyms.....	App B
Absentee, unauthorized.....	3-5
Access (see also Clearance)	
Access for persons outside of the Executive Branch.....	9-13
Adjustment of	
access.....	9-6
Attorneys/legal procedures.....	9-11
Basic policy.....	9-1
Contractor access.....	9-12
CNWDI.....	9-19
Congressional staffs.....	11-4
Eligibility.....	9-2
Continuous evaluation of eligibility.....	10-1
Facility Access Determinations.....	9-20
Personnel Exchange Program Access.....	9-16
Granting access.....	9-2
Reciprocity and Granting access to personnel.....	6-10
Historical researchers .....	9-14
Investigative and law enforcement agents .....	9-10
Limited Access Authorization (LAA).....	9-15
Members of Congress.....	8-3
NATO.....	9-17
Non-Disclosure agreement (SF-312).....	9-3
Need to know.....	9-2
Access by Reserve personnel.....	9-9
Restricted Data (RD)/CNWDI.....	9-9
Retired personnel.....	9-8
SCI (Sensitive Compartmented Information).....	6-9, 9-18
SIOP-ESI.....	6-9
Suspension of access for cause.....	9-7
Temporary access (Interim clearance).....	9-4
Withdrawals/adjusting access.....	9-6
Visitor access.....	11-1
Adjudication	
Standards for adjudication review.....	7-5
Unfavorable determinations process.....	8-4
Sensitive duty assignment.....	7-5
Personnel security determination authorities.....	7-2
Adjudication Criteria/Mitigation.....	App G
Allegiance to the United States.....	App G-5
Foreign Influence.....	App G-6
Foreign Preference .....	App G-7
Sexual Behavior.....	App G-9
Personal Conduct .....	App G-10

Financial Consideration.....	App G-1
Alcohol Consumption.....	App G-13
Drug Involvement.....	App G-5
Emotional, Mental, and Personality Disorders.....	App G-17
Criminal Conduct.....	App G-18
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
National authorities for security matters.....	1-3

**B**

Briefings (See security briefings).....	4-3, 4-10
---	-----------

**C**

Cancellation of personnel security investigation.....	6-17
Central Adjudication Facility.....	7-2
Chief of Naval Operations (N09N).....	1-5
Citizenship.....	App F
Foreign nationals.....	App A, 9-15
Immigrant aliens.....	App A
Non-U.S. citizens.....	9-15
Security requirements.....	8-3
Verification of U.S. citizenship.....	App F
Classified visits.....	11-2
Clearance.....	7-3
Authorities and responsibilities.....	7-2
Citizenship verification.....	App F
Commanding officer's clearance.....	7-9
Consultants to User Agency.....	7-9
Cryptographic Duties.....	7-9
Definition.....	App A
Denial or revocation of clearance for cause.....	8-4
Investigation requirements.....	6-4, 6-5, 6-6, 6-7
Sensitive Assignment Eligibility Determinations.....	6-9
General Accounting Office personnel.....	11-5
Granting .....	7-2, 7-3, 8-6
Individual Ready Reserve (IRR).....	7-15
Interim.....	9-4
Investigative request types.....	6-2
National Industrial Security Program (NISP).....	8-8
NATO security clearances.....	6-9
Prohibitions.....	8-3
Rating/MOS Requirement.....	8-7
Reciprocal acceptance of.....	8-2
Recording Determinations.....	8-4

Reestablishing after a denial or revocation.....8-6  
Security Manager.....2-3  
Security Termination Statement.....4-12, Exh 4A  
Temporary access.....9-4  
Unfavorable Determination process.....8-4  
Combat Operations.....1-9  
Commanding Officer.....1-1, 1-8, 1-11, 2-2  
  Authority to grant access.....9-2  
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  
Contracting Officer Representative.....2-7  
Contact Reporting.....3-3  
Controlled PRP positions.....6-8  
Counterintelligence Matters.....3-1  
  Counterintelligence briefings.....4-9  
  Counterintelligence matters to be reported to NCIS.....3-2  
Critical Nuclear Weapon Design Information (CNWDI)  
  Access controls.....9-19  
Critical PRP position.....6-8  
Critical-sensitive position.....5-2, 5-3  
Cryptologic Duties.....6-8

**D**

Death or Desertion.....3-6  
Debriefings.....4-11  
Defense Intelligence Agency (DIA).....1-4  
Defense Security Service (DSS).....1-4  
Definitions.....App A  
Department of Defense.....1-4  
  Under Secretary of Defense for Policy.....1-4  
  DoD Personnel Security Program Regulation (DOD 5200.2-R)...1-4  
Department of the Navy.....1-5  
  Chief Information Officer (DON CIO).....1-5  
  Chief of Naval Personnel.....1-5  
  Commander, Naval Network Warfare Command (NETWARCOM)  
  Deputy Assistant Secretary of the Navy (Civilian Human  
  Resources).....1-5  
  Secretary of the Navy (SECNAV).....1-3, 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, 7-4  
Director of Naval Intelligence (CNO (N2)).....1-3  
Director Security Directorate.....1-5  
Deputy Chief of Naval Operations (N7SP), Special Programs  
Division (SAP).....1-5  
Director, Navy International Programs Office.....1-5  
Duties of the Security Manager.....2-4

**E**

Education (See security briefings).....4-1, 4-4, 10-2  
Emergency access to classified information (see  
one-time access).....9-5  
Electronic Questionnaires for Investigative Processing  
(e-QIP) .....6-13  
Eligibility  
National Industrial Security Program.....7-10  
Prohibitions.....7-8  
Unique requirements.....7-9  
Requesting determinations.....7-6  
Emergency Action Plan.....2-13  
Emergency appointment of civilians.....6-6  
Employee Education and Assistance Programs.....10-3  
Espionage.....3-2  
NCIS liaison with FBI U.S. Intelligence Comm.....3-2  
Executive Branch of Government, access by persons outside...9-13

**F**

Federal Bureau of Investigation (FBI).....1-3  
Federal employees, investigative requirements.....5-2  
Eligibility for Clearance.....8-1  
Follow-up actions on investigation request .....6-11  
Foreign Nationals  
Classified visits.....11-3  
Foreign connections.....3-8  
Foreign Travel Requirements.....3-7  
Forms procurement.....Exh 6B

**G**

General Accounting Office, access by .....11-5  
Granting access.....9-2  
Guidance.....1-12

**I**

Inactive Status  
Reserve personnel, access.....9-9

Indoctrination .....4-5

Industrial Security

- Access to classified information.....8-8, 9-12
- Adverse information.....8-2
- Facility Access Determination Program.....9-20
- National Industrial Security Program.....8-3

Information Assurance Manager.....2-8

Information Security Oversight Office (ISOO).....1-3

Inspections

- Inspections and review.....2-2, 2-10
- Security Inspection checklist.....App D

Policy manual, command guidelines.....App C,  
2-2

Investigation types, personnel security.....6-2

- Access to classified information by non-U.S. Citizens.....9-15
- Access to NATO .....6-9
- Access to SCI.....6-9
- Access to SIOP.....6-9
- Agencies authorized to conduct.....6-1
- Cancellation.....6-17
- Civilian employment in sensitive positions & employees in  
IT positions.....5-4
- Entrance National Agency Check (ENTNAC).....6-2
- NACLCL Follow-up actions.....6-17
- Limitations on requests for investigations .....6-11
- Local records 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 (NACLCL).....6-2
- National Security Council.....1-3
- Nuclear weapon PRP.....6-8
- Pre-nomination interview.....6-2
- Personnel security investigation.....6-1, 6-2, 8-1
- Persons outside of the Executive Branch of Government.....9-13
- Presidential support activities.....6-9
- Preparation and submission of.....6-12,6-13,6-14
- Reinvestigations.....6-2
- Rejection.....6-17
- Request forms.....6-13
- Retention or Transfer of subject of investigation.....6-13

Investigative Requirements

- Access to chemical agents.....6-8
- Access to NATO.....6-9
- Access to SCI.....6-9
- Access to SIOP-ESI.....6-9
- American Red Cross or USO.....6-9
- Appellate Authorities .....6-9
- Arms, Ammunition and Explosives.....6-9



Cancellations.....6-8  
Chemical agent access.....6-17  
Commissioning.....6-8  
Confidential.....6-4  
Consultants, Navy-hire.....6-7  
Contract guard functions.....6-8  
Contractor personnel.....6-7  
Controlled PRP position.....6-8  
Critical PRP position.....6-8  
Cryptographic duties.....6-8  
Education personnel.....6-9  
Emergency appointment.....6-8  
Follow-up actions on investigation..... 6-17  
Foreign Nationals hired/employed Overseas.....6-8  
Investigative duties.....6-8  
Information Technology positions.....5-2,5-3,6-6  
Limitations on requesting PSIs.....6-11  
Limited Access Authorization.....9-15  
Military members.....6-5  
Mobilization.....6-6  
Non-Appropriated Fund (NAF) personnel.....6-8  
Prenomination interview.....6-2  
Persons outside of the Executive Branch of Government.....9-14  
Personnel Security Clearance Adjudication Officials.....5-6  
Preparation and submission of investigative forms.....6-12,6-13  
Presidential Support Activities.....6-9  
PRP.....6-8  
Safeguarding investigative reports.....6-13  
Secret access.....6-4  
Security Manager.....2-3, 6-8  
Sensitive Compartmented Information (SCI).....6-9, 9-18  
Specific duty or assignment.....6-8  
Specific program .....6-9  
Summer hires (temporary employment) .....6-6  
Temporary employment.....6-6  
Top Secret access.....6-4  
Training professionals/personnel.....6-8  
Types of personnel security investigations.....6-2  
Validity of prior personnel security investigations.....6-4  
Verification of prior investigations.....6-4  
Information Assurance Manager.....2-8

**J**

JPAS.....App E

**L**

Limited Access Authorization (LAA).....9-15  
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 (NACLIC).....6-2  
National Security Agency (NSA).....1-4  
National Security Council (NSC).....1-3  
NATO, Investigative requirements for access to.....6-9  
Noncritical-sensitive positions.....5-2, 5-3  
Nonsensitive position.....5-2, 5-3  
Nuclear Weapon Personnel Reliability Program (PRP).....6-8

**O**

Office of Personnel Management (OPM)  
    Investigations.....6-1, 6-2  
    Responsibilities.....1-3  
On-the-job training.....4-7  
One-time access  
    Authorization for one-time access.....9-5  
Orientation Briefing.....4-6, 10-2  
Other investigative requests for specific performance  
of duty.....6-8  
Record of temporary/interim clearance.....9-4  
Report issues.....10-5  
    Request clearance certification.....7-2, 9-4  
    Request SCI access.....9-18

**P**

Performance Evaluation System.....10-4  
Personnel Security  
Investigations.....6-2  
Personnel Security Appeals Board.....1-5, 7-8  
Personnel Security Determinations  
    Acceptance of personnel security determinations.....7-1  
    Adjudication guidelines.....App G  
    Appeals of.....8-5  
    Authorities.....8-2  
    Continuous evaluation.....10-1  
    Recording.....7-2  
    Reciprocal Acceptance.....7-7  
Personnel Security Investigation (see Investigation)  
Personnel Security Investigative Requirements  
    Appellate Authorities.....6-8

Information Technology personnel.....	5-2,5-3,6-7,6-8
Chemical agent access.....	6-8
Citizenship Requirements.....	5-6
Civilian employment.....	6-6
Commissioned Officer/ military members.....	6-5
Consultants, Navy-hire.....	6-7
Education personnel.....	6-9
Enlisted Personnel/military members.....	6-6
Intermittent/temporary appointees.....	6-6
Investigative agents/duties.....	6-8
Limitations on requesting PSIs.....	6-11
Limited Access Authorizations.....	9-15
Local Record Checks.....	6-12
NATO.....	6-9
Non-appropriated fund personnel.....	6-8
Non-U.S. citizens\.....	9-15
Personnel Reliability Program.....	6-8
Presidential Support duties.....	6-9
Red Cross Personnel.....	6-8
Seasonal/temporary appointees.....	6-7
Secret access.....	6-2
Security Manager.....	6-8
Sensitive Compartmented Information (SCI).....	6-8
SIOP-ESI.....	6-2
Summer/temporary hires.....	6-7
Temporary employment.....	6-7
Top Secret access.....	6-4
Unescorted entry to Restricted areas.....	9-20
Personnel Security Program	
Applicability.....	1-8
Authority.....	1-2
Citizenship.....	App F
Commanding Officer Responsibilities.....	1-11
Polygraph examination.....	9-15
Presidential Support duties.....	6-9
PRP	
Initial assignment in the PRP.....	6-8
Controlled position.....	6-8
Critical position.....	6-8
PSAB procedures.....	8-5

**R**

Reciprocity and acceptability of previously conducted investigations.....	6-10
Reciprocal acceptance of eligibility determinations.....	7-7
Red Cross, investigative requirements for.....	6-9
Refresher briefing.....	4-8
Release of investigative reports to subject.....	6-13
Reinvestigation requirements.....	6-2
Access to Confidential.....	6-2

Access to SCI.....	6-2, 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.....	6-2
Assignment to Presidential Support activities.....	6-2
Continuation of Limited Access Authorization.....	9-15
Review of prior investigations.....	6-4
Reports of investigation, safeguarding.....	6-13
Maintaining Questionable Information .....	6-10
Reserve Personnel	
Access.....	9-9
Clearance.....	7-9
Retired, access.....	9-8
Restricted Data, access.....	9-19
Retired personnel (military), access.....	9-8
Revocation/Denial of Clearance procedures.....	7-8, 8-4, 8-5

**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 Policy manual Requirements.....	2-12
Security Awareness.....	4-14
Security Training.....	4-13
Sensitive Position Investigative Requirements.....	5-4
Civilians.....	5-2, 5-3, 5-4
Critical-Sensitive /IT-I.....	5-2, 5-3
Non-Critical Sensitive/IT-II.....	5-2, 5-3
Non-Sensitive/IT-III.....	5-2, 5-3
Single Scope Background Investigation (SSBI).....	6-2
Sensitive Compartmented Information (SCI)	
Access requirements.....	9-18
Investigative requirements for access to.....	6-2
Responsibility for.....	1-5, 2-9
SIOP-ESI	
Investigative requirements.....	5-2, 6-2
Special programs.....	1-6

Special Access Programs.....	5-7
Authority for.....	1-7
Investigative requirements.....	6-2
Special Investigative Inquiry (SII).....	6-4
Special Security Officer.....	2-9
Duties.....	2-9
Grade requirement.....	2-9
Storage of Investigative reports.....	6-13
Sabotage, Espionage, International Terrorism, Subversion or Deliberate Compromise.....	3-2
Suicide or attempted suicide.....	3-4
Suspension of access.....	9-7, 10-5

**T**

Temporary access (Interim clearance).....	9-4
Top Secret Control Officer (TSCO).....	2-5
Designation of.....	2-5
Grade requirement.....	2-5
Training for security professionals.....	4-13
Transferring personnel	
Debrief.....	4-11
Pending investigation.....	6-13

**U**

Unauthorized Absentee.....	3-5
Unfavorable Personnel Security Determinations.....	8-1
Determination process.....	8-4, 8-5
Appeal Process.....	8-5
Command Responsibilities.....	7-7, 8-4, 8-5
Letters of Intent.....	8-2
USO Personnel Investigative requirements for.....	6-9

**V**

Validity of prior personnel security investigations.....	6-10
Validity and reciprocal acceptance of personnel security determinations.....	6-10
Verification of citizenship.....	App F
Visits.....	11-1
Access restrictions.....	11-1
Foreign nationals.....	11-3
"Need to know".....	11-3
Classified visit requests to DON commands.....	11-2
Violations of this policy manual.....	1-13

**W**

Waivers.....	1-10
--------------	------

Security Manager SSBI requirement.....2-3  
Security Manager Grade requirement.....2-3



**BRIEF OF REVISIONS/CHANGES**

The following are major changes in policy and procedures incorporated in the last revision to this SECNAV Manual. A revised Foreword and Table of Contents will be issued with each change.

1. Chapter\_\_\_\_\_, Page\_\_\_\_\_, Paragraph\_\_\_\_\_:
2. Chapter\_\_\_\_\_, Page\_\_\_\_\_, Paragraph\_\_\_\_\_:
3. Chapter\_\_\_\_\_, Page\_\_\_\_\_, Paragraph\_\_\_\_\_:
4. Chapter\_\_\_\_\_, Page\_\_\_\_\_, Paragraph\_\_\_\_\_:
5. Chapter\_\_\_\_\_, Page\_\_\_\_\_, Paragraph\_\_\_\_\_:
6. Chapter\_\_\_\_\_, Page\_\_\_\_\_, Paragraph\_\_\_\_\_:
7. Chapter\_\_\_\_\_, Page\_\_\_\_\_, Paragraph\_\_\_\_\_:
8. Chapter\_\_\_\_\_, Page\_\_\_\_\_, Paragraph\_\_\_\_\_:
9. Chapter\_\_\_\_\_, Page\_\_\_\_\_, Paragraph\_\_\_\_\_:
10. Chapter\_\_\_\_\_, Page\_\_\_\_\_, Paragraph\_\_\_\_\_:



SECNAV M-5510.30

STOCK NUMBER  
0516LP1055278