DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH, VA 22042

IN REPLY REFER TO
BUMEDINST 5510.11
BUMED-M4
6 Apr 2016

BUMED INSTRUCTION 5510.11

From: Chief, Bureau of Medicine and Surgery

Subj: PERSONNEL SECURITY PROGRAM

Ref: See Appendix B of enclosure (1)

Encl: (1) Personnel Security Program Manual

1. Purpose. This instruction establishes the Bureau of Medicine and Surgery's (BUMED) Personnel Security Program (PSP). Enclosure (1) is the BUMED PSP.

a. References (a) through (x), establish procedural guidance to effectively protect personnel, technology, and equipment within the BUMED enterprise.

b. The PSP provides guidance under the Department of the Navy (DON) PSP, which implements reference (n) and updates all command level relevant security policies in compliance with the higher authority associated policies and procedures.

c. This instruction ensures the effectiveness and uniformity in the application of the PSP policies throughout the enterprise. PSP applies to all personnel employed and/or assigned to BUMED including military, civilian, and on-site contractor personnel.

d. The PSP is in compliance with reference (a). Questions regarding command implementation must be referred to the BUMED PSP Manager via the Navy Medicine Echelon 3 Security Managers.

2. Scope and Applicability. This instruction applies to all personnel, assigned to all Budget Submitting Office (BSO) 18 and activities. Nothing in this instruction must be construed as authority to implement security policies that are contrary to higher authority. Commanders at all levels are responsible for compliance and implementation of the PSP within their area of responsibility. The effectiveness of the security programs depends on the importance given to the program by leadership at all levels.

3. Responsibilities

a. Chief, Bureau of Medicine and Surgery must:

(1) Have overall responsibility for the formulation and dissemination of Navy Medicine's personnel security policies per references (a) through (x).

(2) Ensure the BUMED PSP Manager is appointed and designated in writing and has been provided the core training, and received additional training as needed to remain proficient for the position.

(3) Ensure the PSP Manager has the sufficient authority to effectively manage and provide oversight within the enterprise hierarchy.

(4) Conduct, at a minimum, an assessment of the PSP at Navy Medicine Echelon 3 commands annually, and at selected BUMED commands as needed.

(5) Ensure PSP policy has been written and disseminated to all subordinate commands.

b. Navy Medicine Echelon 3 activities must:

(1) Administer and execute Navy Medicine's Personnel Security Management Program per references (a) through (x) and align their program with Fleet Support and Logistics (BUMED-M4).

(2) Designate in writing an Echelon 3 Security Manager. The Echelon 3 Security Manager will be a Commissioned Officer or civilian (GS-11 or above) and a United States (U.S.) citizen. This position will not be a collateral duty.

(3) Ensure the Echelon 3 Security Manager has been properly trained per reference (a).

(4) Ensure the Echelon 3 Security Manager has sufficient authority to effectively manage and to provide oversight of the PSP within the area of responsibility.

(5) Ensure the assigned Echelon 3 Security Manager has had a successfully adjudicated Single Scope Background Investigation (SSBI) within the past 5 years.

(6) Implement policies and guidance consistent with this instruction and references (a) through (x) to provide subordinate commands the information needed for a successful PSP.

(7) Ensure subordinate commands develop and implement effective PSP.

(8) Ensure a qualified Echelon 3 Assistant Security Manager has been appointed in writing. The Echelon 3 Assistant Security Manager will be a U.S. citizen, an officer, or enlisted person (E-6 or above), or a civilian (GS-6 or above) with a successfully adjudicated SSBI.

(9) Aggressively work in meeting the goals and objectives of the DON, BUMED, Echelon 3, and Command Security Managers (CSM) per references (a) through (p).

(10) Ensure adherence to established standards for the security management program, rely on the expertise of the CSM, and provide them the support needed to discharge their duties.

c. COs of BSO-18 activities must:

(1) Administer and execute Navy Medicine's PSPs per references (a) through (x) and this instruction.

(2) Designate a CSM in writing. The CSM will be a Commissioned Officer, or a civilian, (GS-11or above) and a U.S. citizen. For medical treatment facilities (MTF) and larger non-MTF commands, this position must not be a collateral duty. At smaller commands with limited human assets, the position may be a collateral duty, but caution will be taken to ensure the assigned security manager will have the time to effectively perform the CSM duties. To ensure continuity, CSM appointments must be at a minimum 24 months.

(3) Ensure the CSM has been properly trained per reference (a).

(4) Ensure the CSM has the sufficient authority to ensure personnel adhere to program requirements, their position within the organizational hierarchy must ensure their credibility, and enable them to raise security issues directly to the CO.

(5) Ensure that the CSM reports directly to the CO for functional security matters and report to the XO for administrative matters, per reference (p).

(6) Provide CSM with formal and recurring training. The Naval Security Manager Course is offered by the Naval Criminal Investigative Service (NCIS) Security, Training, Assistance, and Assessment Team (STAAT), which will satisfy this requirement.

(7) Ensure a PSP self-assessment is completed annually per reference (a). The results of the self-assessment will be reported to the CO as well as the Echelon 3 Security Manager. This requirement will be negated for the years that a higher headquarters assessment is being conducted.

(8) Ensure a qualified Assistant Command Security Manager (ACSM) has been appointed. Additional Security Assistants may be assigned as needed and will be designated in writing. The ACSM where applicable, will be at a minimum a U.S. citizen, an officer or enlisted person (E-6 or above), or civilian (GS-6 or above) with a successfully adjudicated SSBI.

(9) Aggressively work in meeting the goals and objectives of the DON, BUMED, Echelon 3, and CSM per references (a) through (p).

(10) Coordinate PSP issues with the BUMED PSP Manager via their Echelon 3 Security Manager.

d. Navy Medicine PSP Manager must:

(1) Be the PSP subject matter expert for BSO-18 and be familiar with all references contained in this instruction. The PSP Manager will be appointed in writing and attend the Navy Security Manager course of instruction.

(2) Maintain up to date knowledge of the PSP. This may be accomplished by attending seminars, symposiums, webinars, and online courses.

(3) Maintain a successfully adjudicated SSBI.

(4) Provide PSP program management and coordination with the Deputy Under Secretary of the Navy Plans, Policy, Oversight, and Integration (DUSN (Policy)) as well as Navy Medicine Echelon 3 activities.

(5) Conduct, at a minimum, an assessment of the PSP at Navy Medicine Echelon 3 activities and selected BUMED commands at a minimum every 3 years.

(6) Develop policy and disseminate to all subordinate commands. Conduct an annual review of all personnel security policy directives.

(7) Ensure security awareness training and education programs are implemented at all BSO-18 commands via the Echelon 3 Security Manager.

(8) Ensure all Echelon 3 Security Managers and CSMs are knowledgeable in their positions and have the ability and support needed to maintain a successful program per references (a) through (o).

(9) Review and incorporate changes to this instruction annually.

e. Echelon 3 Security Managers must:

(1) Be the subject matter expert for all assigned subordinate commands within their area of responsibility and be familiar with references (a) through (x) contained in this instruction.

(2) Administer and execute Navy Medicine's PSP per references (a) through (x) and have the authority to effectively manage this program throughout the area of responsibility.

(3) Be designated in writing and be a Commissioned Officer or civilian (GS-11 or above), and be a U.S. citizen. This position shall not be a collateral duty.

(4) Have a successfully adjudicated SSBI within the past 5 years.

(5) Manage and provide oversight to subordinate commands, ensuring fully developed and effective personnel security management programs are in effect.

(6) Implement policies and guidance consistent with this instruction and references (a) through (o) to provide subordinate commands the information needed for a successful PSP.

(7) Ensure subordinate commands develop and implement effective PSP in their respective commands.

(8) Conduct PSP assessments at a minimum of every 2 years at all subordinate commands.

(9) Have completed the Navy Security Manager course of instruction. Additionally, the Echelon 3 Security Managers will attend seminars, symposiums, webinars, and online courses to maintain up to date knowledge of the PSP.

f. CSMs must:

(1) Administer and execute Navy Medicine's personnel programs per references (a) through (h) and this instruction.

(2) Be designated in writing and be a U.S. citizen, Commissioned Officer or civilian (GS-11 or above) and be a U.S. citizen. Ensure they have the proper training per reference (a). For MTFs and larger non-MTF commands, this position must not be a collateral duty. Smaller commands with limited human assets may assign the CSM role as a collateral duty, but caution will be taken to ensure the assigned Security Manager will have the time to effectively perform the Security Manager duties.

(3) Must have direct access to the CO to ensure effective management of the command's security program.

(4) Report to the CO for functional security matters and report to the XO for administrative matters, per reference (p).

(5) Complete the Navy Security Manager course of instruction. Additionally, the CSM will attend seminars, symposiums, webinars, and online courses to maintain up to date knowledge of the PSP.

(6) Conduct a self-assessment annually. The results of the self-assessment will be reported to the CO as well as the Echelon 3 Security Manager. This requirement will be negated for the years that a higher headquarters assessment is being completed.

(7) Ensure that all personnel who handle classified information or will be assigned to sensitive duties are appropriately vetted through the appropriate channels and organizations. Request for background investigations are properly prepared, submitted, and monitored.

(8) Ensure that access to classified information is limited to those who are eligible and have the need to know.

(9) Ensure that security investigations on staff members are properly recorded in the Joint Clearance and Access Verification System (JCAVS).

(10) Coordinate command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

(11) Ensure that all personnel who have had access to classified information who are separating or retiring have completed an OPNAV 5511/14, Security Termination Statement. The Personnel Support Detachment performs this action to ensure it is included in the member's closing paperwork.

(12) Provide formal initial and reoccurring Security Manager training.

g. Assistant Security Managers to include Assistant Echelon 3 Security Managers must:

(1) Be a Commissioned Officer or Enlisted (E-6 or above), or a civilian (GS-6 and above), and a U.S. citizen. The Assistant Security Managers will be under the supervision of the CSM who will provide direction and support as needed.

(2) Meet background requirements as the CSM and will be designated in writing.

h. Security Assistant will:

(1) Be a civilian or military member that is a U.S. citizen and must be designated in writing.

(2) Must have the clearance level sufficient to access all required programs.

(3) Be under the supervision of the CSM who will provide direction and support.

i. Top Secret Control Officer must:

(1) Be designated in writing for commands that handle top secret material.

(2) Be an officer, senior non-commissioned officer (E-7 or above), or a civilian, (GS 7 or above). The Top Secret Control Officer will be a U.S. citizen and have completed a favorably adjudicated SSBI within the past 5 years.

j. Contracting Officer Representatives (COR) must:

(1) Be appointed in writing and have the prerequisite training.

(2) Be responsible to the CSM when coordinating with program managers and technical and procurement officials.

(3) Ensure that personnel and information security requirements are met and properly recorded when sensitive information, controlled unclassified information, personally identifiable information, protected health information, Health Insurance Portability and Accountability Act is provided to industry in a contract.

(4) Ensure that personnel security requirements are met when access to DON Information Technology systems is required.

k. Information Assurance Manager (IAM) must:

(1) Ensure each command involved in processing data in information technology (IT) systems, including access to local area networks and/or the intranet/internet designated in writing and to perform the duties as an IAM.

(2) Be a U.S. citizen.

(3) Be responsible for establishing, implementing, and maintaining the DON information system and information assurance program.

l. Inspections, Assist Visits, and Reviews

(1) Per reference (a), COs are responsible for evaluating the security posture of their subordinate commands.

(2) BUMED PSP Manager will conduct assessments on the Echelon 3 commands annually, and select commands as needed. Echelon 3 Security Manager will conduct assessments a minimum of every 2 years. CSMs will conduct annual self-assessments utilizing the CSM self-assessment guide, and forward this self-assessment to the BUMED PSP Manager via the Echelon 3 Security Manager.

m. Standard Program Requirements

(1) All commands within BSO-18 that handle classified information are required to prepare and keep current a written command security policy specifying how security procedures and requirements will be conducted within the command.

(2) Maintain the continuous evaluation program on all members attached to their command.

n. All BSO-18 commands will develop an emergency destruction plan for classified material per reference (a).

4. Records. Records created as a result of this instruction, regardless of media and format, must be managed per SECNAV M-5210.1 of January 2012.

5. Reports. The reports required in this instruction, are exempt from reports control per SECNAV M-5214.1 of December 2005, part IV, paragraph 7p.

6. Forms

a. OPNAV 5511/14 (Rev 9-05), Security Termination Statement is available at: http://www.secnav.navy.mil/dusnp/Security/Forms/opnav5511-14.pdf.

b. SF Forms

(1) SF 86 (Revised December 2010), Questionnaire for National Security is available at: https://www.opm.gov/forms/pdf_fill/sf86.pdf.

(2) SF 312 (Rev. 7-2013), Classified Information Nondisclosure Agreement is available at: http://www.gsa.gov/portal/forms/download/116218 .

c. FD 258 (Rev. 9-9-13), Applicant Fingerprint Card is available through the Navy Supply System. The stock number is 0104-LF-006-9600.

C. FORREST FAISON III

Distribution is electronic only via the Navy Medicine Web site at:
http://www.med.navy.mil/directives/Pages/default.aspx

PERSONNEL SECURITY PROGRAM MANUAL

TABLE OF CONTENTS

CHAPTER 1

COUNTERINTELLIGENCE MATTERS

1. Policy. Certain matters affecting national security must be reported to Naval Criminal Investigative Service (NCIS) so appropriate action may be taken. All Budget Submitting Office (BSO) 18 military and civilian personnel, whether they have access to classified information or not, will report to their security managers, commanding officers (COs), or to the nearest Command Security Manager (CSM) any activities described below involving themselves, their dependents, co-workers, or others. COs will immediately notify the nearest NCIS field office.

2. Sabotage, Espionage, Terrorism, Subversion, or Deliberate Compromise

a. Individuals becoming aware of sabotage, terrorism, deliberate compromise, or other subversive acts will report all available information concerning these activities to the security manager or CO at their command or at the most readily available command. The command receiving the report must promptly notify the nearest NCIS field office. If the NCIS office cannot be contacted immediately and the report concerns sabotage, terrorism, espionage, or imminent flight of defection of an individual, the command will immediately contact the Director, NCIS (DIRNAVCRIMINVSERV WASHINGTON DC) via classified IMMEDIATE message, with Deputy Under Secretary of the Navy Plans, Policy, Oversight, and Integration (DUSN (Policy)) and Navy Judge Advocate General (NAVY JAG WASHINGTON DC) as information addressees.

b. NCIS will advise what additional action is to be taken and conduct liaison and coordination with appropriate members of the United States intelligence community.

3. Contact Reporting

a. All personnel possessing a security clearance, to include eligible determinations, must report to their COs, activity head, or designee contacts with any individual 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.

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

4. Suicide or Attempted Suicide

a. When personnel who have access to classified information commit or attempt to commit suicide, the individual's CO will immediately forward all available information to the nearest NCIS field office for action, with an information copy to the Department of

Defense Central Adjudication Facility (DoD CAF). The report will, at 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.

b. Investigative actions will be coordinated with the CO by the NCIS Special Agent. If NCIS assumes cognizance of the investigation, no independent questioning of witnesses will be conducted without prior approval of NCIS.

5. Unauthorized Absentees (UA)

a. Personnel in a UA status who have access to classified information will be assessed for indications that the UA may be contradictory to the interests of national security. COs will conduct an inquiry to determine if there are any indications of intent from the individual's activities, behavior, or associations. Any identified concerns will be reported to the nearest NCIS field office by the quickest means available.

b. NCIS will advise the command whether or not they will launch an investigation.

6. Death or Desertion. When a Service member or employee of the DON with access to classified information dies or deserts, the CO must determine if any indicators or unusual circumstances may exist to cause a security concern. The CO will report any concerns and pertinent information to the nearest NCIS field office by the most expedient means available.

7. Foreign Travel

a. Commands will advise personnel of the particular vulnerabilities associated with foreign travel during orientation and annual refresher briefs.

b. All personnel possessing security clearance eligibility are required to list all 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.

8. Foreign Connections

a. A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom the member 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.

b. The personnel security adjudication process requires examination of a sufficient amount of an individual's information to determine whether the individual is an acceptable security risk. The assessment of risk due to association with foreign nationals and foreign entities is a part of the adjudicative process.

c. 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 DoD CAF as appropriate.

CHAPTER 2

SECURITY EDUCATION

1. Policy

a. 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.

b. The purpose of the security education programs is to ensure that all personnel understand the need for protecting classified information and the proper procedures for handling and destruction.

2. Responsibility. COs are responsible for security training and awareness within their command. Supervisors, in coordination with the CSM, 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.

3. Scope

a. Security education must be provided to all personnel and must be tailored to meet the needs of the command and different groups within the command.

b. When developing a command security education program, the security manager must provide the minimum briefing requirements. Security managers must guard against the program becoming stagnant or simply complying with requirements without achieving the desired goals.

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

(1) Advise personnel of the adverse effects to 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.

(2) 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.

(3) Advise personnel of their obligation to notify their supervisor or CSM when they become aware of information with potentially serious security significance regarding someone with access to classified information or assigned to sensitive duties.

(4) Advise supervisors of the requirement for continuous evaluation of personnel eligibility for access to classified information or assignment to sensitive duties.

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

(6) Familiarize personnel with procedures for challenging classification decisions believed to be inappropriate.

(7) Familiarize personnel with the security requirements and restrictions for their particular assignments.

(8) Instruct personnel having knowledge, possession, or control of classified information how to determine a recipient's suitability prior to disseminating the information. This determination includes whether the prospective recipient has been authorized access, needs the information to perform his/her official duties, and can properly protect and store the information.

(9) 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.

(10) Inform personnel of the techniques employed by foreign intelligence activities to obtain classified information.

(11) Inform personnel of their vulnerability to compromise classified information during foreign travel.

(12) Advise personnel that they are to report to their CO, activity head, or designee, any personal or official contact with individuals regardless of nationality in which:

(a) Illegal or unauthorized access is sought to classified or other sensitive information.

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

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

4. Minimum Requirements. The following are the minimum requirements for security education:

a. Indoctrination of personnel upon employment by all BSO-18 commands in the basic principles of security.

b. Training on command security requirements for personnel who will have access to classified information or assignment to sensitive duties (including IT duties) at the time of assignment.

c. On-the-job training on specific security requirements for duties assigned.

d. Annual refresher briefings for personnel who have access to classified and non-critical sensitive (NCS) information.

e. Counterintelligence briefings held annually for personnel who have access to information classified secret and above or have access to NCS information.

f. Special briefings as circumstances dictate.

g. Debriefing upon termination of access.

5. Indoctrination/Orientation

a. All personnel entering employment with any BSO-18 commands will have a basic understanding of classified information, reasons for its protection, and how to protect it.

b. Personnel who will have access to classified information or assignment of 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.

c. 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.

d. 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.

6. Refresher Briefings

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

b. Refresher briefings should cover:

(1) New security policies and procedures.

(2) Counterintelligence requirement to report contacts, exploitation attempts, and foreign travel issues.

(3) Continuous evaluation.

(4) Command specific security concerns or problem areas.

(5) Insider threat concerns.

7. Special Briefings

a. Foreign Travel Briefing. Although foreign travel (personal or official) may be briefly discussed during annual refresher briefings, it may also be appropriate to require specific foreign travel briefings for personnel 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 foreign travel may present. All military, civilian, and contractor personnel traveling outside of the continental United States will require an area specific briefing by the Command Antiterrorism Officer/Antiterrorism Representative.

b. North Atlantic Treaty Organization (NATO) Security Briefing. All personnel who have access to a Secret Internet Protocol Router Network terminal accredited to receive and process NATO information must receive a NATO security briefing. This briefing will be recorded in Joint Personal Adjudication System (JPAS) as functionality permits. Records may be maintained locally in the form of rosters or another automated format, if JPAS record keeping functionality is intermittently unavailable.

c. Command Debriefings

(1) Command Debriefings will be given to:

(a) Individuals who no longer require access to classified information as a result of a transfer to another command or termination of military service or civilian employment.

(b) Individuals with a temporary separation of a period of 60 days or more to include sabbaticals, leave without pay, or transfer to the Inactive Ready Reserves.

(c) Individuals with an expired Limited Access Authorization (LAA).

(d) Individuals with revoked security clearance eligibility.

(e) Individuals undergoing administrative withdrawal or suspension of security clearance and sensitive compartment information (SCI) access eligibility for cause.

(2) Debriefings will include the following:

(a) Return of all classified materials within the individual's possession.

(b) Individual is no longer eligible for access to classified information.

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

(d) The individual must report to the NCIS (or to the Federal Bureau of Investigation (FBI) or nearest DoD component if no longer affiliated with the DON) without delay.

(3) As part of the 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.

(4) As part of every debriefing (except when individuals transfer from one command to another command) a OPNAV 5511/14 Security Termination Statement is required (paragraph 8 applies).

8. Security Termination Statement

a. Individuals must read and execute a OPNAV 5511/14 at the time of the 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.

b. A witness to the individual's signature must sign the OPNAV 5511/14.

c. The command, agency, or activity's name and mailing address will be annotated on the three lines at the top of the OPNAV 5511/14.

d. The original signed and witnessed OPNAV 5511/14 will be placed in the individual's official service record or the official personnel folder for permanent retention.

e. If an individual refuses to execute the OPNAV 5511/14 the individual will be debriefed before a witness if possible. It must be stressed that refusal to sign the OPNAV 5511/14 does not change the individual's obligation to protect classified information from unauthorized disclosure as stated on the SF 312.

The OPNAV 5511/14 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 OPNAV 5511/14. Only send a copy of refusals to DUSN (Policy).

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

9. Training for Security Manager Personnel

a. The NCIS Security Training Assistance Assessment Team (STAAT) offers the Naval Security Manager Course. A DON unique core training developed to train security managers is also available to security specialists and assistants. For more information on this course, contact the following:

(1) Atlantic STAAT
Joint Expeditionary Base Little Creek-Fort Story (JEB LC-FS)
Phone: (757) 462-283
DSN 253-2834

(2) Pacific STAAT
Naval Air Station (NAS) North Island
Phone: (619) 545-8934
DSN 735-8934

(3) DUSN (Policy) Web site:
www.secnav.navy.mil/dusnp/security

b. For other security training available and posted on the SECNAV PPOI Web site at: www.secnav.navy.mil/dusnp/security.

10. 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 examples of media that should be used to promote security awareness.

CHAPTER 3

SENSITIVE AND INFORMATION TECHNOLOGY POSITIONS

1. Policy

a. 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 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.

b. 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). Reference (q), section 730 mandates, OPM provide the requirements for public trust position suitability determinations. Per reference (q), OPM provides the requirements for national security position suitability determinations.

c. Public trust positions include Federal Government positions that meet the high and moderate risk levels identified per reference (q). Public trust positions do not include national security positions. Public trust position determinations are under the purview of Deputy Assistant Secretary of the Navy (Civilian Personnel).

d. National Security Positions include: (1) those positions involving activities of the Government 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 positions are sensitive national security positions. DON national security position suitability determinations are under DUSN (Policy) purview and are governed by this policy manual.

e. 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.

2. Position Designation

a. In order to provide the appropriate level of background investigation and suitability adjudication, positions are designated according to potential risk. Reference (q) 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:

(1) Special Sensitive (SS)	Potential for inestimable impact and or damage
(2) Critical Sensitive (CS)	Potential for grave to exceptionally grave impact and/or damage
(3) NCS	Potential for some to serious impact and/or damage
(4) Non-Sensitive (NS)	Potential for no impact and/or damage as duties have limited relation to the agency and/or mission

b. Reference (v) 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:

(1) IT - Designated Approving Authority (DAA) – Exceptional privilege with exceptional control

(2) IT-I – Privileged access

(3) IT-II – Limited Privilege, sensitive information access

(4) IT – III – No Privilege, no sensitive information access

c. 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 SECNAV to efficiently and consistently manage national security requirements.

d. 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 CO may establish standard operating procedures to delegate this responsibility.

e. 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.

f. Sensitivity and IT position determinations will be recorded in JPAS.

(1) 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.

(2) 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.

(3) CSM 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.

3. Criteria for Designating Sensitive Positions

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

(1) SS: Any position which the head of the agency determines to be at a level higher than critical sensitive:

(a) Due to the greater degree of damage to the national security that an individual could effect by virtue of his/her position, or special requirement concerning the position under authority other than reference (t), such as designations applied under Special Security Officer (SSO) cognizance requiring as SSBI clearance and a determination that an individual is eligible for access to SCI.

(b) DAAs must be designated as SS, due to the degree of damage an individual could effect by virtue of his/her position, including these IT duties in which the incumbent has.

(2) CS: Any position that includes:

(a) Access to Top Secret national security information.

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

(c) 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.

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

(e) 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.

(f) 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:

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

2. Been designated as IAM or Information Assurance Officer (IAO).

3. Significant involvement in life-critical or mission critical systems.

4. 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.

5. 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.

6. Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.

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

(g) Any other position so designated by SECNAV and/or his or her designee.

(3) NCS: Any position that involves:

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

(b) 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).

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

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

(e) 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.

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

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

(h) 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:

1. 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.

2. Access to and/or processing of proprietary data, information requiring protection per reference (w), 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.

3. 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.

4. 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.

(4) NS: Only those positions with limited relation to the DON mission, devoid of reference (q) and (u) public trust risk criteria will be designated as NS. IT-III positions are designated as NS, and are dependent upon very rigorous IT controls to remain NS 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 per reference (w), 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. 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 designated requirements.

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

4. Suitability and Security Investigation and Adjudication

a. 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.

b. After determining the position sensitivity level, the appropriate investigation can be requested.

c. 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 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.

d. OPM forwards all completed PSIs for DON personnel to the DoD CAF. The DoD 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 DoD CAF security determination can be made. The following workflow procedures have been established to accomplish this requirement:

(1) Investigations for NS or public trust positions will be forwarded to the command for the suitability determination. There is no adjudicative action by the DoD CAF.

(2) Investigations for sensitive positions:

(a) When the Office of Federal Investigations (OFI) Form 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations, indicates "No Actionable Issue," the investigation will not 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 DoD CAF will favorably adjudicate the investigation, as appropriate, and enter the favorable determination in JPAS, thus notifying the command of the favorable determination. The DoD CAF will complete the OFI 79A accordingly and forward it to OPM Federal Investigative Services Division.

(b) 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 DoD 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 DoD CAF action is required.

5. Security Adjudication Criteria

a. The national security adjudication criteria used to determine security clearance eligibility will likewise be applied by DoD 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 DoD CAF re-establishes the eligibility.

b. Since 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 DoD 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 DoD 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.

c. 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 are contained in reference (a), paragraph 6-6.7.

6. Citizenship Requirements

a. Reference (r) requires 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.

b. U.S. citizenship is a basic condition for access to classified information and assignment to 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 counterintelligence 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, DUSN (Policy) prior to assignment. U.S. citizenship waiver procedures for appointment to sensitive positions are provided in exhibit 3B.

c. 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.

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

(2) 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 IAMs, or IAOs. 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 DUSN (Policy). U.S. citizenship requirements apply to DON employees and contractors assigned to designated IT positions. Waiver procedures are provided in exhibit 3B.

(3) IT-II: Effective the date of this policy manual, DON non-U.S. citizen employee will NOT be permitted to be assigned to NCS, IT-II positions.

(4) 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 systems. 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.

d. 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 to base a favorable personnel security determination.

e. 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.

f. Foreign representatives are governed by foreign disclosure policies and procedures per reference (w).

EXHIBIT 3A

INVESTIGATIVE EQUIVALENCY TABLE

If position is Sensitive, IT designation, or access requirement is:	**…and the individual has had the following investigation(with no break in service >2yrs):**	**…and the age of the investigation is:**	**...then the investigation request required to support the requirement is:**
SS	SSBI, SSBI-PR, FFI	<5 years	None
CS	SSBI, SSBI-PR, FFI	>5 years	SSBI-PR
IT-DAA IT-I	SBI, BI, LBI, MBI, NACLC, ANACI, NACI, MAC, NACIC	Regardless of the age of the investigation	SSBI
SCI Access Top Secret	No previous investigation	N/A	SSBI
NCS	SSBI, SSBI-PR, FFI, BI, LBI, MBI, NACLC, ANACI	<10 years	None (* See Note)
IT-II	SSBI, SSBI-PR, FFI, BI, LBI, MBI, NACLC, ANACI, NACI, NACIC, NAC, ENTANC	>10 Years	NACLC (*ANACI for initial hire civilian)
Secret Access	No previous investigation	N/A	NACLC (*ANACI for initial hire civilian)
Confidential Access	SSBI, SSBI-PR, FFI, BI, LBI, MBI, NACLC, ANACI No previous investigation	<15 years N/A	None NACLC (*ANACI for initial hire civilian)
NS IT-III No Access	Any investigation which substantially meets or exceeds the scope of the NACI is acceptable for assignment including, SSBI, SSBI-PR, FFI, MBI, NACLC, ANACI, NACIC, NACI No previous investigation	N/A N/A	None NACI

* Reference (t) requires written inquiries for all background investigations for initial suitability determinations for Federal Government civilian employees. The SSBI, SSBI - PR, limited background investigation (LBI), minimum background investigation (MBI), National Agency Check with Written Inquiries (NACI) and ANACI all include written inquiries, but the National Agency Check with Local Agency Check and Credit Check (NACLC) does not. Although the basis requirement for assignment to IT-II and IT-III positions is the NACLC, 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 NACLC and also includes written inquiries.

EXHIBIT 3B

U.S. Citizenship Requirement Waiver Procedures for Persons Nominated to Occupy DON Sensitive and IT Positions

1. 5B1 Sensitive Positions without IT Duties

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

(1) The full identity of the applicant and the applicant's country of origin.

(2) The original completed investigation request SF 86, Questionnaire for National Security will review and forward to OPM, as appropriate.

(3) 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 documentation identifying the applicant's immigration status, alien residency and/or other visa status.

(4) A detailed justification of the compelling reasons requiring assignment (to include special expertise) signed by the CO.

(5) A detailed description of the sensitive duties to be performed or sensitive information to be accessed, including all required IT system access.

(6) A detailed description of the security measures and mechanisms in place to preclude the individual from having access to classified information and/or 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.

b. DUSN (Policy) will review and coordinate the request with the appropriate authorities to determine if the 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 DUSN (Policy) for the required personnel security determination. The command will be advised of the adjudicative results accordingly.

2. 5B2 Sensitive IT positions

a. In general, assignment to a designated IT position requires U.S. citizenship. Waivers may be requested however, they are not always granted. Waivers may be requested per the following:

Position Sensitivity Designation	**Position IT Designation**	**US Citizenship Required**	**Waivers Permitted**
SS	DAA	Yes	No
CS	IT-I	Yes	For incumbents only – DUSN (Policy) approval required
NCS	IT-II	Yes	Infrequent – DUSN (Policy) approval required
NS	IT-III	No	Not necessary, technical limitations and protections negate the ability to access sensitive information, and render the positions NS

b. 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.

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

(2) IT I: Non-U.S. citizen employees will NOT be assigned to designated IT-I positions, and will NOT be permitted to function as IAMs, or IAOs. Non-U.S. citizen employees encumbering designated IT-I positions will NOT be permitted to continue assignment. If at all possible, fill the position with a U.S. citizen. If the position is critical and mission failure will result, a waiver package will be submitted to DUSN (Policy) and will include:

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

(b) 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.

(c) An explanation of the intended transition plan to replace the non-U.S. citizen within 5 years, with a qualified U.S. citizen employee.

(d) If an SSBI has not been recently performed on the incumbent, a SSBI/SSBI-PR request will be prepared using an SF 86, including a FD 258, Applicant Fingerprint Card, which will be forwarded to DUSN (Policy) as part of the waiver request package. DUSN (Policy) will review and submit the investigation request to OPM, as appropriate.

(e) DUSN (Policy) waiver approvals will expire 5 years from date of issuance and will not be renewed.

(3) IT-II: Requests to waive the U.S. citizenship requirement for designated IT-II positions may be submitted to DUSN (Policy) and must include the following:

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

(b) A detailed justification for the waiver request, including compelling need in the furtherance of the DON mission. Compelling reasons may exist to grant 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.

(c) 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 (i.e., how the command plans to control and limit the access).

(d) If an SSBI has not been recently performed on the incumbent, an SSBI/SSBI-PR request will be prepared using an SF 86, including a FD 258, which will be forwarded to DUSN (Policy) as part of the waiver request package. PPOI 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.

(e) After ensuring that the waiver request meets program parameters, DUSN (Policy) will forward the SSBI request to OPM. No waiver approval authorizations can be issued until favorable adjudication of the SSBI. DUSN (Policy) waiver approvals are valid for 5 years and will NOT be renewed.

(f) 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 their access and that physical custody of classified information by the non-U.S. citizen employee is not authorized.

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

CHAPTER 4

PERSONNEL SECURITY INVESTIGATION

1. Policy

a. The only personnel authorized to initiate PSI are the BUMED PSP Manager, Echelon 3 Security Managers, and CSMs or their assistants.

b. Requests for PSIs are kept to the absolute minimum and are limited to the minimum investigation needed to satisfy the billet requirement. It is the responsibility of the hiring manager in coordination with their Human Resources Office representative to verify that each employee's personnel description supports the level of access required for the investigation requested.

c. PSIs are not requested to resolve allegations of a suitability nature for the purpose of supporting human resource administrative decision or disciplinary procedures independent of a personnel security determination.

d. PSIs will not normally be requested for any civilian or military personnel who will be retired, resigned, or separated within one remaining service year.

2. Types of PSI

a. The term PSI describes an inquiry by an investigative agency into an individual's activities for the specific purpose of making an eligibility determination.

b. Reference (a), will assist in making the determination of the type of investigation necessary for appointment, reappointment, or assignment to a sensitive position and level of security clearance needed.

c. The types of PSIs are:

(1) National Agency Check (NAC). The NAC includes a search of DoD's Defense Clearance and Investigations Index, OPM's Reimbursable Suitability 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, OPM, Central Intelligence Agency, etc.). A NAC is an integral part of each SSBI, SSBI-PR, NACLC, NACI, and ANACI. A technical fingerprint search of the FBI files is conducted as part of a NAC, except during an SSBI-PR. The NAC is used as the basis for trustworthiness determinations.

(2) NACI. Per reference (t) the NACI is the basic 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 5 years. NACIs are insufficient for personnel security eligibility determination purposes or assignment to sensitive duties.

(3) ANACI. The ANACI is an OPM product that combines the NACI (per reference (t) to determine suitability of civilian employees within the Federal Government) and the NACLC (directed by reference (x) to determine security clearance eligibility). The ANACI meets the investigative requirements for appointment to NCS 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 5 years to law enforcement agencies, to former employers and supervisors, to references, and to schools. OPM also conducts a MBI and a LBI for public trust purposes that are acceptable equivalents to the ANACI.

(4) NACLC. The NACLC is the basic standard for determinations of eligibility to access Confidential and Secret classified national security information and is conducted at 10-year and 15-year intervals per reference (x). The NACLC also provides the basis for military suitability determinations for Navy and Marine Corps enlisted members and officers. The NACLC includes a NAC, credit bureau checks covering all locations where the subject has resided, been employed, or attended school for 6 months or more for the past 7 years, and checks of law enforcement agencies having jurisdiction where the subject has resided, been employed, or attended school within the last 5 years. In the past, the NACLC reinvestigation was referred to as a Secret PR or Confidential PR by DSS, but it always included all the elements of the NACLC.

(5) SSBI. The SSBI is the investigative standard for determinations of eligibility to access Top Secret classified national security information and SCI access eligibility determinations per reference (x). The SSBI is also the basis for determinations of eligibility to occupy a CS or SS 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, and 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 conducted by the FBI, State Department, or U.S. Secret Service is usually equivalent to an SSBI.

(6) SSBI-PR: SSBI-PRs are conducted on personnel whose clearance/access to SCI or Top Secret information is based on an investigation that is 5 years old or more. The 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 critical positions, CS, and SS positions, IT-DAA and IT-I positions, Presidential Support Activities, access to Single Integrated Operational Plan-Extremely Sensitive Information, and for 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.

(7) Phased PR: 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 PR, OPM will automatically expand the investigation coverage to full SSBI-PR coverage.

(8) Reinvestigations. A reinvestigation, updates a previous investigation, is part of the Continuous Evaluation Programs, and is only authorized for specific duties and access. While eligibility does not expire, it only remains active for access to classified information and/or assignment to a sensitive position; as long as investigations are current as specified per reference (a).

d. All PSIs will be initiated through the Electronic Questionnaires for Investigations Processing (eQIP). This system will enable CSM’s to monitor and track PSI’s from cradle to grave. Below is a listing of the roles the CSM will serve utilizing this system:

(1) Initiator: The e-QIP Initiator serves as the applicant's main point of contact during the investigation request process. The initiator is responsible for initiating the applicant's investigation request, selecting the appropriate form, completing the Agency Use Block section, and monitoring the applicant's timely completion of the SF 86. There may be a need to cancel investigation requests if, for example, the applicant takes a job elsewhere.

(2) Reviewer: The e-QIP Reviewer examines the investigation request and forwards it to the Approver, if applicable. The reviewer is responsible for conducting a thorough review of the applicant's investigation, adding appropriate attachments or confirming the presence of applicant-uploaded attachments, and indicating fingerprint submission. If no issues are found in the review, the investigation will be forwarded to the Approver, if that role is filled by another person. If there are discrepancies, the investigation will be rejected to the applicant to mitigate and correct the issues found.

(3) Approver: The approver conducts a final review of the investigation and forwards the request to the Investigation Service Provider (ISP). The approver is responsible for reviewing an applicant's investigation request to confirm there are no issues to address and will add and/or verify that appropriate attachments are present before releasing the request from your agency to the ISP. The approver's role is very similar to the reviewer's role. Depending upon your agency's structure, the role of Reviewer and Approver may be performed by the same person.

3. Restrictions during subject interview. Refer to reference (a).

4. Investigative requirements for clearance eligibility. Refer to reference (a).

5. Investigative requirements for military personnel. Refer to reference (a).

6. Investigative requirements for civilians in sensitive position and all DON Employees in DON IT positons. Refer to reference (a).

7. Investigative requirements for DON Contractor personnel. Refer to reference (a).

8. Specific duty or assignment requirements. Refer to reference (a).

9. Specific Program Requirements. Refer to reference (a).

10. Reciprocity and acceptability of previously conducted investigations. Refer to reference (a).

11. Limitations on request for investigation. Refer to reference (a).

12. Command responsibilities in PSI Requests. Refer to reference (a).

13. Personnel security investigations request forms. Refer to reference (a).

14. Preparation and submission of investigations requests. Refer to reference (a).

15. Maintaining questionnaire information. Refer to reference (a).

16. Follow up actions on investigation requests. Refer to reference (a).

17. Processing completed reports of investigations. Refer to reference (a).

18. Safeguarding reports of investigations. Refer to reference (a).

CHAPTER 5

CLEARANCE AND SENSITIVE ASSIGNMENT ELIGIBILITY DETERMINATIONS

1. Policy

a. No individual will be given access to classified information or assigned to sensitive duties unless a favorable eligibility determination has been made regarding his or her loyalty, reliability, and trustworthiness.

b. No individual will be granted an eligibility determination, security clearance, access to classified information, or assigned sensitive duties under the following conditions:

(1) They are not U.S. citizens.

(2) They hold a foreign passport.

(3) They are disqualified by per reference (s).

(a) The individual has been convicted in any court of the United States (Federal or state court including courts martial) of a crime for which they were sentenced to incarceration and consequently served imprisonment of a term exceeding 1 year.

(b) The individual is determined by an authorized mental health professional to be mentally incompetent.

(c) The individual is an unlawful user of, or is addicted to, a controlled substance.

(4) The individual has been discharged or dismissed for the Armed Forces under dishonorable conditions.

c. An individual's security clearances will be administratively withdrawn when the requirement for access to classified information is no longer needed.

d. An individual's eligibility determination will be continuously evaluated per reference (a). Upon discovery of potentially disqualifying information, the CSM must take action to review the individual's eligibility for access to classified information and assignment to a sensitive position and eligibility to occupy a public trust or DON IT position, and report all pertinent information to the DoD CAF.

(1) To maintain a continuous evaluation per reference (a), communication with the command's legal department is critical. The sharing of information is needed to maintain the level of evaluation needed.

(2) Supervisors must report potentially disqualifying information on their members to the CSM as well as the command legal department.

e. An individual's eligibility determination will be continuously evaluated per reference (a). Upon discovery of potentially disqualifying information, the CSM must take action to review the individual's eligibility for access to classified information and assignment to a sensitive position and eligibility to occupy a public trust or DON IT position, and report all pertinent information to the DoD CAF.

2. Security Clearance and Sensitive Duty Assignments

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

b. When making personnel security eligibility determinations, all information, favorable and unfavorable, is considered and assessed for accuracy, completeness, relevance, importance, and overall significance.

c. The eligibility determination is the result of overall common sense "whole person" adjudication, reached by application of the evaluation criteria set forth in Appendix (G) of reference (a).

d. Once established, eligibility remains valid provided the individual continues compliance with personnel security standards and has no break in service exceeding 24 months.

e. While eligibility does not expire, it only remains active for access to classified information and/or assignment to a sensitive position; as long as investigations are current or within the timeframes outlined in Chapter 4, paragraph 6 of this manual.

f. 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.

g. Unless there is a reasonable basis for doubting a person's loyalty to the U.S. Government, 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 instruction.

3. DoD CAF Determination Process

a. The DoD CAF, at the direction of SECNAV, is responsible for making all eligibility determinations for all military and civilian personnel within the DON. The DoD CAF is the final authority for granting, denying, and revoking all security clearances and determining eligibility for sensitive positions. The CSMs have the authority to temporarily suspend access to classified information and/or assignment to a sensitive position when derogatory information warrants such action. Criteria for such actions are located in reference (a), appendix g.

b. DoD 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.

c. In determining eligibility, DoD 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.

CHAPTER 6

UNFAVORABLE ELIGIBILITY DETERMINATIONS

1. Policy. 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.

2. Authorities and Responsibilities. DoD CAF is the single authority for making final favorable and unfavorable eligibility determinations. Supervisors are responsible for making the basic employment suitability determinations; however, only the DoD CAF can make a final determination that an employee is ineligible to occupy a sensitive national security position.

3. Restriction on the Granting or Renewal of Security Clearances. Refer to reference (a), Chapter 8, Paragraph 8-3; Page 8-5.

4. Unfavorable Determination Process

a. If locally developed derogatory information is received on an individual who has access to classified information, the command will request the employee to provide documentation to address the derogatory information.

b. When an unfavorable personnel security eligibility determination is being considered by the DoD CAF, the DoD CAF will issue to the individual concerned (via the CSM) a Letter of Intent (LOI) to revoke or deny security clearance eligibility or sensitive position eligibility.

c. The CSM 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. If suspension is warranted, the CSM will follow up pursuant to established procedures.

d. When unfavorable information is discovered regarding individuals with temporary or interim access, their access will be removed immediately.

e. Procedures

(1) Upon receipt the BUMED PSP Manager, Echelon 3 Security Manager, or CSMs will immediately present the LOI to the individual and assume a direct role in facilitating the process.

(2) The CSM will determine the individual's intent regarding a response to the LOI and immediately complete and return the Acknowledgement of Receipt of the LOI.

(3) The CSM will advise DoD CAF of any extension of time granted for submission of a response. The individual will be advised that in the absence of an approved extension or if the response is untimely, they may forfeit their right to appeal.

(a) The CSM has the authority to grant extensions up to 45 days (for a total of 60 days) for the preparation of a response.

(b) Extensions are appropriate to enable the individual to obtain a copy of the investigation or information based upon the DoD CAF's intended action, medical, or mental evaluation, personal reference letters that will mitigate or rebut the disqualifying information, financial statements, legal counsel, or documentation from rehabilitation institutes, or other related information to support the response.

(c) 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.

(4) If a favorable determination is made, individuals will be notified in writing.

(5) If an unfavorable determination is made, the individual will be issued a Letter of Decision (LOD) citing all factors that remain unmitigated, which caused the unfavorable determination and advise the individual of his or her appeal rights.

(6) Upon receipt of the LOD, the CSM, via the supervisor, will take action to ensure the individual no longer occupies a sensitive position and the appeals process will be handled per reference (a), chapter 8.

5. Appeals Process. The appeals process will be handled per reference (a).

6. Reestablishing eligibility after a denial or revocation. Refer to reference (a).

CHAPTER 7

ACCESS TO CLASSIFIED INFORMATION

1. Policy

a. No one has a right to have access to classified information solely because of rank, position, or security clearance eligibility.

b. Access to classified information will be limited to the minimum number of persons necessary to accomplish the mission, and will be on a need to know basis. 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 the assigned duties.

c. All individuals will complete a SF- 312 prior to being granted initial access to classified information and recorded in JPAS.

d. 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.

2. Need to Know

a. Access to classified information is not authorized solely based on 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.

b. Need to know is a determination that an individual requires access to specific classified information in the performance of assigned duties.

c. Need to know must be determined by every authorized holder of classified information prior to relinquishing that classified information to a prospective recipient.

(1) 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.

(2) These determinations must be based on reliable information from supervisors or security personnel in a position to know the prospective recipients security clearance eligibility and duties. Determinations may be made in person, by telephone, facsimile, or by encrypted electronic mail.

d. Classified discussions are prohibited in public areas, hallways, cafeterias, elevators, rest rooms, or smoking areas as the discussion may be overheard by persons who do not have a need to know. Individuals are obligated to report violations of the need to know principle to their supervisor and the CSM.

e. 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.

f. Access to classified information will be formally terminated when it is no longer required in the performance of assigned duties and/or when the individual's security clearance eligibility is denied or revoked.

g. Access to classified information may be suspended, upon receipt of potentially disqualifying information. The CSM will evaluate the information and make a suspension of access determination.

3. Classified information Non-Disclosure Agreement (SF-312)

a. All personnel will execute a SF-312 as a condition of access to classified information.

b. If an individual refuses to sign an SF-312 the BUMED PSP Manager, Echelon 3 Security Manager, or CSM, will deny access to classified information and report the denial to DoD CAF via JPAS under the “Report Incident” link.

4. Temporary Access

a. In the absence of potentially disqualifying information, the CSM may grant temporary access (also referred to as an "Interim Clearance”) to individuals pending completion of full investigative requirements and establishment of security clearance eligibility by DoD CAF. Potentially disqualifying information is identified in reference (a).

b. Interim Access to top secret information requires:

(1) An established secret or confidential clearance eligibility determination by DoD CAF.

(2) A favorable review of the completed e-QIP revealing no eligibility issues as outlined in reference (a), exhibit 10A.

(3) The submission of the SSBI request; and a favorable review of local records, as defined in, reference (a), paragraph 6-12.

c. Interim Access to Secret or Confidential information requires:

(1) A favorable review of the e-QIP revealing no eligibility issues per reference (a), exhibit 10A.

(2) The submission of an appropriate investigative request and a favorable review of local records, per reference (a).

d. When the CSM receives a LOI from DoD CAF to deny or revoke an individual's security clearance, the CSM will immediately withdraw temporary access or any interim security clearance.

e. Temporary access or assignment to a sensitive position is not authorized for individuals who have received a final unfavorable eligibility determination.

5. One Time Access. Refer to reference (a), chapter 9, paragraph 9-5.

6. Withdrawals or Adjustments to Access

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

b. The CSM will administratively withdraw an individual's access when a permanent change in official duties (e.g., rating/MOS changes) eliminates the DON requirement for access.

c. The CSM will debrief the individual as outlined in chapter 4, paragraph 4-11 and 4-12; pages(s) 4-9 thru 4-10 of reference (a).

d. When the level of access required for an individual's official duties changes, the CSM will adjust access accordingly.

e. The administrative withdrawal or downgrading of access is not authorized when prompted by developed potentially disqualifying information. In these cases, the CSM may suspend the individual's access to classified information and assignment to a sensitive position, and must report the suspension and the derogatory information to DoD CAF. A report of suspension of access for cause will automatically result in the DoD CAF suspension of the individual's security clearance eligibility.

7. Suspension of Access for Cause

a. When potentially disqualifying information becomes known concerning an individual who has been granted access to classified information or assigned to sensitive duties, the CSM

will determine whether, on the basis of all the facts available, to suspend the individual's access to classified information. The CSM will report the information and the suspension decision to DoD CAF within 10 days.

b. Once an individual's access is suspended for cause, DoD CAF will remove the individual's eligibility.

c. Once the individual's eligibility is removed, the CSM cannot reinstate access until DoD CAF adjudicates the issue and makes a favorable eligibility determination.

d. Suspension of access is required when a military or civilian employee with a security clearance is incarcerated for a period exceeding 30 days (to include work release programs) as the result of a conviction for a criminal offense.

e. Suspension of access is required when a military or civilian employee is absent without leave for 30 days or more or if a military member is declared a deserter.

f. Whenever a determination is made to suspend access to classified information ensure the command leadership is notified of the suspension.

(1) The individual concerned must be notified of the determination in writing. The notification must include a brief statement of the reason(s) for the suspension action and must be presented to the individual. The CSM must report all suspensions to DoD CAF no later than 10 working days from the date of the suspension action and remove the individual's access authorization from JPAS.

(2) The CSM will ensure that the manager or host command representative confiscate the individual's common access card (CAC) when appropriate and/or limit access to the installation and work area.

(3) The individual's supervisor must take the following actions:

(a) Remove the individual's name from all local access rosters and visit certifications.

(b) Ensure that the combinations to classified storage containers, secure areas, and vaults the individual had access to, are changed.

(c) Confiscate keys, including key cards used in any automated electronic control system.

(d) Brief the individual on the limitations of his or her use of his or her CAC.

(e) Cancel or hold in abeyance any permanent change of station orders.

(4) If after suspension of access, DoD CAF adjudicates the reported information favorably, that information will no longer be the basis for continued suspension of access.

(5) If after suspension of access, DoD CAF adjudicates the reported information unfavorably, the individual will be debriefed per reference (a).

8. Access by retired personnel. Refer to reference (a), chapter 9, paragraph 9-8; page 9-11.

9. Access by reserve personnel. Refer to reference (a), chapter 9, paragraph 9-9; page 9-12.

10. Access by investigative and law enforcement agents. Refer to reference (a), chapter 9, paragraph 9-10; page 9-12.

11. Access Authorization in legal procedures. Refer to reference (a), chapter 9, paragraph 9-11; page 9-12.

12. Contractor access. Refer to reference (a), chapter 9, paragraph 9-12; page 9-13.

13. Access authorization for persons outside of the executive branch of the Government. Refer to reference (a), chapter 9, paragraph 9-13; page 9-13.

14. Historical Researchers. Refer to reference (a), chapter 9, paragraph 9-14; page 9-14.

15. LAA for Non-U.S. Citizens. Refer to reference (a), chapter 9, paragraph 9-15; page 9-16.

16. Personnel exchange program access. Refer to reference (a), chapter 9, paragraph 9-16; page 9-18.

17. Facility access determination. Refer to reference (a), chapter 9.

CHAPTER 8

CONTINUOUS EVALUATION

1. Policy

a. An eligibility determination requires an examination of a sufficient amount of information regarding an individual to determine whether the individual is an acceptable security risk. It is not possible to establish with certainty that an individual will remain eligible for access to classified information or assignment to a sensitive position. To ensure that everyone who has access to classified information or is assigned to a sensitive position remains eligible, continuous assessment and evaluation is required.

b. As required by reference (a), this chapter establishes a program for continuous evaluation. This program relies on all personnel within the Command to report questionable or unfavorable information that can be relevant to a security clearance determination.

c. One of the keys to an active continuous evaluation program is positive reinforcement of reporting requirements in the form of management support, confidentiality, and employee assistance referrals.

2. Security Education

a. The ability of individuals to meet security responsibilities is proportional to the degree in which individuals understand what is required of them. Therefore, a key component of an effective continuous evaluation program is an effective security education program.

b. All personnel assigned to sensitive duties must receive indoctrination and orientation training. Along with understanding the prohibitions against improperly handling classified information, personnel must understand the continued trustworthiness expectations placed upon them. You may refer to chapter 4, paragraph 4-1 of reference (a), for the various types of required training.

3. Performance evaluation program. Refer to reference (a), chapter 10, paragraph 10-4.

4. Command reports of locally developed unfavorable information

a. Individuals must report to their supervisor or the CSM any incident or situation that could affect their continued eligibility for access to classified information. The ultimate responsibility for maintaining eligibility for access to classified information rests with the individual.

b. Co-workers must advise their supervisor or the CSM when they become aware and must report information with potential security clearance significance.

c. Supervisors and program managers play a crucial role in assuring the success of the continuous evaluation program. 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. The goal is early detection of an individual's problems.

d. Significant security issues. The following security issues or concerns must be reported to the CSM.

(1) Involvement in activities or association with persons who unlawfully practice or advocate the overthrow or alteration of the U.S. Government by unconstitutional means.

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

(3) Foreign citizenship, dual citizenship, or foreign monetary interests.

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

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

(6) Unexplained affluence or excessive indebtedness.

(7) Alcohol abuse.

(8) Illegal or improper drug use or involvement.

(9) Apparent mental, emotional, or personality disorders.

(10) Criminal conduct.

(11) Noncompliance with security requirements.

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

(13) Misuse of information technology system.

CHAPTER 9

CLASSIFIED VISITS

1. Policy

a. JPAS is the personnel security system of record for DoD use for personnel security administrative functions, including the administration of visits involving access to classified information.

b. Visit authorization letters or OPNAV 5521/27, Visit Request are no longer required for visits involving civilian, military, and contractor personnel whose access level and security management office affiliation are accurately reflected in JPAS. Visit requests submitted through JPAS will not be accepted if they do not reflect accurate access documentation including the non-disclosure agreement, date, and accurate affiliation documentation including appropriate security management office information.

c. If the command is sponsoring the visitor, we are responsible for ensuring and validating the accuracy of the access and affiliation data in JPAS before initiating the visit request.

d. The visited command releasing classified information is responsible for verifying need to know and positively identifying the visitors.

e. Employees who sponsor visitors may not authorize access to areas where the sponsor does not have appropriate area access.

f. All outgoing visits are the responsibility of the requesting program office.

g. In compliance with CNO records management guidance, a copy of all visit requests received through means other than JPAS, must be retained on file by the office sponsoring the visit for 2 years.

2. Visits by foreign nationals and representatives of foreign entities. Refer to reference (a), chapter 11, paragraph 11-3.

3. Classified visits by Members of Congress. Refer to reference (a), chapter 11, paragraph 11-4.

4. Classified visits by representatives of the General Accounting Office. Refer to reference (a) Chapter 11, paragraph 11-5.

APPENDIX A

ACRONYMS

Access National Agency Check with Written Inquires and Credit Check	ANACI
Assistant Command Security Manager	ACSM
Budget Submitting Office	BSO
Bureau of Medicine and Surgery	BUMED
Common Access Card	CAC
Critical-Sensitive	CS
Chief of Naval Operations	CNO
Contracting Officer's Representative	COR
Commanding Officer	CO
Command Security Manager	CSM
Controlled Unclassified Information	CUI
Department of Defense	DoD
Department of the Navy	DON
Department of Defense Central Adjudication Facility	DoD CAF
Deputy Assistant Secretary of Defense (Security and Information Operations)	DASD(S&IO)
Deputy Under Secretary of the Navy Plans, Policy, Oversight, and Integration	DUSN (Policy)
Designated Approving Authority	DAA
Electronic Questionnaires for Investigations Processing	e-QIP
Entrance National Agency Check	ENTNAC
Executive Officer	XO
Federal Bureau of Investigation	FBI
Full Field Investigation	FFI
Information Assurance Manager	IAM
Information Assurance Officer	IAO
Information Technology	IT
Investigation Service Provider	ISP
Joint Clearance and Access Verification System	JCAVS
Joint Personnel Adjudication System	JPAS
Limited Access Authorization	LAA
Limited Background Investigation	LBI
Letter of Decision	LOD
Letter of Intent	LOI
Mandatory Access Control	MAC
Medical Treatment Facility	MTF
Military Occupational Specialty	MOS
Minimum Background Investigation	MBI
National Agency Check	NAC

National Agency Check with Inquiries	NACI
National Agency Check and Inquiry Investigation plus a Credit Check	NACIC
National Agency Check with Law and Credit	NACLC
North Atlantic Treaty Organization	NATO
Naval Criminal Investigative Service	NCIS
Nondisclosure Agreement	NDA
Non-sensitive	NS
Non-Critical Sensitive	NCS
Office of Federal Investigations	OFI
Office of Management and Budget	OMB
Office of Personnel Management	OPM
Officer-in-Charge	OIC
Periodic Reinvestigation	PR
Personnel Security Manager	PSM
Plans, Policy, Oversight, and Integration	PPOI
Program Executive Officers	PEOs
Personnel Security Investigation	PSI
Personnel Security Program	PSP
Regional Assistant Security Manager	RASM
Restricted Data	RD
Security Coordinator	SC
Special-sensitive	SS
Security, Training, Assistance, and Assessment Team	STAAT
Sensitive Compartmented Information	SCI
Sensitive Compartmented Information Facility	SCIF
Secretary of the Navy	SECNAV
Security Education Training and Awareness	SETA
Single Scope Background Investigation	SSBI
Single Scope Background Investigation Periodic Reinvestigation	SSBI-PR
Special Security Office	SSO
Standard Form	SF
Unauthorized Absentee	UA
United States	U.S.

APPENDIX B

REFERENCES

(a) SECNAV M-5510.30 of Jun 2006

(b) SECNAV M-5510.36 of 1 Jun 2006

(c) DoD Instruction 5200.01 9 October 2008

(d) E.O. 13526

(e) DoD 5400.7-R, DoD Freedom of Information Act Program, 4 September 1998

(f) Department of the Navy Foreign Disclosure Manual of 1 September 2007

(g) DoD Instruction 5230.24 of 23August 2012

(h) DoD 5220.22-R, Industrial Security Regulation, 4 December 1985

(i) DoD 5200.2-R, Personnel Security Program, 23 February 1996

(j) DoD Instruction 5200.02 of 21 March 2014

(k) DoD Instruction 5230.24 of 23August 2012

(l) SECNAVINST 5500.36

(m) DoD Manual 5220.22, Volume 3, National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence of 17 April 2014

(n) E.O. 12829

(o) OPNAVINST 3120.32D

(p) 5 CFR 731

(q) Executive Order 11935, Citizenship Requirements for Federal Employment

(r) Public Law 110-181, Section 3002 (The Bond Amendment)

(s) E.O. 10450

(t) 5 CFR 732

(u) OMB Circular A-130

(v) 5 U.S.C. §552

(w) SECNAVINST 5510.34A

(x) E.O. 12968