DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, D.C. 20350-1000

SECNAVINST 5510.30C
DUSN
24 Jan 2020

SECNAV INSTRUCTION 5510.30C

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY PERSONNEL SECURITY PROGRAM

Ref: See enclosure (1)

Encl: (1) References
(2) Responsibilities
(3) Department of the Navy Personnel Security Program Supplement
(4) Command Security Program
(5) Counterintelligence Matters
(6) Security Education
(7) National Security Investigations
(8) Adjudication and Eligibility Determinations
(9) Unfavorable Eligibility Determinations and Restrictions
(10) Access to Classified Information
(11) Visitor Access to Classified Information
(12) Continuous Evaluation

1. Purpose

a. This instruction establishes the Department of the Navy (DON) Personnel Security Program (PSP) under the authority of references (a) and (b) in compliance with references (c) through (s). It supplements reference (b), where needed. When applying guidance of this instruction, the user must consult reference (b) to ensure proper application of DON and Department of Defense (DoD) PSP standards.

b. Provide DON commands, activities, and personnel with regulations and guidance governing the DON PSP in accordance with references (a) through (af) and enclosures (3) through (12). This is a major revision and should be read in its entirety.

2. Cancellation. SECNAVINST 5510.30B, SECNAV M-5510.30, and ALNAV's 075/11, 058/13, 079/13, 073/14, 083/14, and 005/16.

3. Definitions. For DoD definitions for the PSP see reference (b). Reference (b) can be obtained by accessing the Deputy Under Secretary of the Navy Security and Intelligence (DUSN (S&I)) Directorate Microsoft SharePoint Portal at: https://portal.secnav.navy.mil/Pages/default.aspx.

4. Applicability. This Instruction applies to the Offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all United States (U.S.) Navy (USN) and U.S. Marine Corps (USMC) installations, commands, activities, field offices, and all other organizational entities within the DON. This policy shall not alter or supersede the existing authorities delegated to the Director, DON Special Access Program (SAP) Central Office for SAP, or those delegated to the USMC Director of Intelligence (DIRINT) and the Director of Naval Intelligence (DNI) regarding the protection of intelligence sources, methods, and activities pursuant to reference (c) or the authorities delegated by the DNI to the Head of the Community Element (HICE).

5. Policy

a. This policy ensures maximum uniformity and effectiveness in the application of PSP policies within the DON and accomplishes the purpose of references (a) and (b). This instruction and the references complement each other and have been coordinated to achieve maximum compatibility.

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

6. Responsibilities. See enclosure (2).

7. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD) portal page: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Manager or the DRMD program office.

8. Forms

a. The following DoD Forms are available for download from the DoD Forms Management Program website: https://www.dtic.mil/whs/directives/infomgt/forms/index.htm/.

(1) DD Form 4414, Sensitive Compartmented Information Nondisclosure Agreement.

(2) DD Form 254, Contract Security Classification Specification.

b. The following forms are available for download from the U.S. General Services Administration Forms Library website: https://www.gsa.gov/portal/forms/:

(1) Optional Form (OF) 8, Position Description.

(2) Standard Form (SF) 312, Classified Information Nondisclosure Agreement.

(3) SF 86, Questionnaire for National Security Positions.

(4) SF 87, Fingerprint Card.

(5) SF 86A, Continuation Sheet for Questionnaires.

(6) SF 1847-1, Sensitive Compartmented Information (SCI) Non-Disclosure Agreement.

(7) SF 714, Financial Disclosure Report.

c. The following forms are available for download from the National Background Investigations Bureau (NBIB) Forms website: https://nbib.opm.gov/hr-security-personnel/reference-materials/nbib-access-forms:

(1) Investigations (INV) Form 79A, Report of Agency Adjudicative Action on NBIB Personnel Investigations.

(2) Personnel Investigation Processing System (PIPS) Form 12, Submitting Office Number (SON) Creation and Amendment Form.

(3) PIPS Form 11, Security Office Identifier (SOI) Creation and Amendment Form.

d. Department of Energy (DOE) Visitor Request 5631.20, Request for Visit or Access Approval, is available for download at the DOE website: https://www.energy.gov/cio/office-chief-information-officer/services/forms.

9. Information Management Control. The reporting requirements throughout this instruction are exempt from Information Management Control, per reference (t), Part IV, paragraph 7c, 7i, 7n, and 7o.

THOMAS B. MODLY
Acting

Distribution:
Electronic only, via Department of the Navy Issuances website https://www.secnav.navy.mil/doni/default.aspx.

REFERENCES

(a) DoD Instruction 5200.02 of 21 March 2014
(b) DoDM 5200.02, Procedures for the DoD Personnel Security Program of 3 April 2017
(c) SECNAVINST 5500.36A
(d) SECNAVINST 5510.36B
(e) SECNAVINST 5510.34B
(f) SECNAV M-5210.1
(g) SECNAVINST 5510.35D
(h) SECNAVINST 5312.12D
(i) SECNAVINST S5460.3H
(j) SECNAV M-5239.2
(k) DoDM 5105.21 Volume 3, SCI Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities of 5 April 2018
(l) ICPG 704.1 of 2 October 2008
(m) DoD Directive 5240.06 of 21 July 2017
(n) DoD Instruction 5210.91 of 12 August 2010
(o) SECNAVINST 5213.12D
(p) DoD Instruction 5200.46 of 9 September 2014
(q) 5 CFR 731
(r) Office of the Under Secretary of Defense Intelligence Memorandum of 12 June 18: Implementation of Security Executive Agent Directive 4: National Security Adjudicative Guidelines (10 December 2016)
(s) OPNAVINST 5400.45
(t) SECNAV M-5214.1
(u) Title 5, U.S.C.
(v) Title 10, U.S.C.
(w) DoDM 5220.22, National Industrial Security Program (NISP): Operating Manual of 18 May 2016
(x) SECNAVIST 5740.26B
(y) DoD Directive 5220.6 of 2 January 1992
(z) DoD Directive 5220.22R of 4 December 1985
(aa) Under Secretary of Defense for Intelligence (USD (I)) Memorandum (NOTAL) of 31 May 2009
(ab) DoD Directive 5100.55 of 27 February 2006
(ac) DoD Directive 5210.2 of 3 June 2011
(ad) DoD Instruction 6490.08 of 17 August 2011
(ae) DoD Directive 5210.48 of 24 April 2015
(af) DoD Directive 5230.11 of 16 June 1992

RESPONSIBILITIES

1. SECNAV is responsible for oversight, management, readiness, and compliance of the PSP.

2. The Under Secretary of the Navy (UNSECNAV) is responsible for implementing the PSP, in compliance with Presidential Directives and the provisions of Executive Orders, public laws, and directives issued by the DNI, Secretary of Defense (SECDEF), and other program authorities.

3. Assistant Secretary of the Navy Manpower and Reserve Affairs (ASN (M&RA)) provides oversight to ensure personnel security requirements for DON civilian personnel are properly identified in Joint Personnel Adjudication System (JPAS) or successor system, and that matters relating to the DON's civilian PSP and sensitive position designation are appropriately coordinated with DUSN (S&I).

4. The CNO is responsible for implementing an effective Navy PSP and complying with all directives issued by higher authority.

    a. Ensure matters relating to the Navy's PSP are appropriately coordinated with DUSN (S&I).

    b. Ensure personnel security requirements for Navy military and civilian members are properly identified in JPAS or successor system.

    c. Ensure personnel security requirements for Navy military members are properly coded in military personnel data systems, which ultimately will update JPAS or successor system.

    d. Ensure personnel identifying data and the position designation are accurately reflected and updated in the civilian personnel data systems, which ultimately will update JPAS or successor system.

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

f. Coordinate with DUSN (S&I) on all matters involving personnel security eligibility determinations on Navy military members.

g. Director, Special Programs Division (CNO N9SP), is the DON SAP Coordinator and is responsible for the management, administration, support, review, and oversight of the DON SAP security program.

h. The Director, Navy International Programs Office is delegated the authority to approve or disapprove requests for access to or transfer of DON technical data or disclosure of DON classified or sensitive unclassified information to foreign governments, international organizations, and their representatives in accordance with national disclosure policy.

i. The DNI is HICE, Navy and administers the SCI program for the Navy, including non-Service DON entities. The Special Security Office, Navy (SSO Navy) is designated as the Cognizant Security Authority (CSA). As the CSA, SSO Navy is responsible for the security management, implementation, and oversight of SCI security programs for the DON's SCI security program.

j. The HICE, Navy has designated Commander, U.S. Fleet Cyber Command (COMFLTCYBERCOM) Security Directorate the authority responsible for administration of SCI PSPs within the Department's Cryptologic Community. COMFLTCYBERCOM is assigned as Service Cyber Component to Commander, U.S. Cyber Command for all Navy cyberspace activities and as the Service Cryptologic Component Commander to the National Security Agency/Central Security Service (NSA/CSS).

5. The CMC is responsible for implementing an effective Marine Corps PSP and complying with all directives issued by higher authority.

a. Ensure matters relating to the Marine Corps PSP are appropriately coordinated with DUSN (S&I).

b. Ensure personnel security requirements for Marine Corps military and civilian members are properly identified in JPAS or successor system.

c. Ensure personnel security requirements for Marine Corps military members are properly coded in military personnel data systems, which ultimately will update JPAS or successor system.

d. Ensure personnel identifying data and the position designation are accurately reflected and updated in civilian personnel data systems, which ultimately will update JPAS or successor system.

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

f. Coordinate with DUSN (S&I) on all matters involving personnel security eligibility determinations on DON military members.

g. The CMC has delegated the DIRINT, Headquarters Marine Corps as HICE, USMC and administers the SCI program for the Marine Corps. SSO Navy (OPNAV N2N6I) is designated as the CSA and is responsible for the security management, implementation, and oversight of SCI security programs for the DIRINT.

6. The DUSN is designated as the DON Security Executive, per reference (d). DUSN is responsible, under the direction and control of the UNSECNAV, for establishing, directing, and overseeing an effective DON PSP, and for implementing and complying with all directives issued by higher authority.

7. The Director, Naval Criminal Investigative Service (DIRNCIS) serves as an advisor to the CNO as Special Assistant for Naval Investigative Matters (CNO N09N).

8. The Office of Chief Information Officer (OCIO) is responsible for providing Information Management and Information Technology (IT) policy and governance oversight for the DON. This includes enterprise architecture, data center optimization, privacy, Freedom of Information Act, civil liberties, information sharing, electromagnetic spectrum, cybersecurity, and IT policy compliance. The OCIO coordinates within the DON Secretariat, as well as with the Navy, Marine Corps, Military Departments, DoD, and other Federal agencies.

9. The Deputy Assistant Secretary of the Navy (Civilian Human Resources (DASN (CHR)), under the direction and control of ASN (M&RA), provides oversight to ensure personnel identifying data is accurately reflected and updated, in the Defense Civilian Personnel Data System or successor system, is consistent with information provided in JPAS or successor system, and that matters relating to the DON's civilian suitability position designation are appropriately coordinated with DUSN (S&I).

10. The DUSN, Senior Director for (S&I), under the authority, direction, and control of DUSN, provides staff support for the functions and responsibilities as described in reference (c).

11. The President, Personnel Security Appeals Board (PSAB) presides over the PSAB, a three-member panel appointed by the Director of Review Boards, to review and decide appeals of unfavorable DoD Consolidated Adjudications Facility (CAF) determinations. The decision of the PSAB is final and concludes the administrative appeal process to sustain or reverse a DoD CAF determination.

12. The Commanding Officer (CO) (used as a generic term for the head of any DON command and includes commander, commanding general, director, and officer in charge) is responsible for the effective management of the PSP within the command. Authority delegated by this instruction to a CO may be further delegated, unless specifically prohibited. "Command" is used as a generic term for the organizational entity and includes a ship, laboratory, facility, activity, unit, squadron, etc.

13. DON military and civilian personnel will:

a. Fully and accurately complete personnel security questionnaires and cooperate with personnel security investigators.

b. Be aware of personnel security eligibility standards and reporting requirements, and consult with local security officials whenever information develops that could affect eligibility, per reference (b).

14. The Defense Counterintelligence and Security Agency (DCSA) and the DoD CAF evaluates Personnel Security Investigations (PSI) and other relevant information to determine if granting or continuing national security eligibility is clearly consistent with the interests of national security.

DEPARTMENT OF THE NAVY PERSONNEL SECURITY PROGRAM SUPPLEMENT

1. Basic Policy. This overview applies to Total Force, personnel employed by, detailed to, or assigned to the DON, including Government civilians (both appropriated and NAF); members of the active and reserve components of the USN and USMC; temporarily assigned forces performing a full-time or training role or function of security, e.g., Auxiliary Security Force and Ship's Self Defense Force; expert or consultants performing services for the DON through personnel appointments or contractual arrangements; industrial or commercial contractor, licensee, certificate holder, or grantee, including subcontractors.

2. Special Programs

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

b. Most special programs requiring additional security measures have been established by authorities outside the DON. Although the requirements for these programs are included in this regulation, these programs are implemented and governed in the DON by references (g) through (l).

3. SAPs. Programs requiring security measures in addition to those requirements for the protection of TS, Secret, or Confidential classified information, which are established by and within the DoD, are referred to as DoD SAPs. A DoD SAP must be authorized by the SECDEF or by the Deputy Secretary of Defense (DEPSECDEF). CNO (N9SP) is responsible for the coordination of the approval, administration, support, review, oversight, and reporting of all DON SAPs. The UNSECNAV recommends to the DEPSECDEF, the establishment, modification, or disestablishment of DON SAPs.

4. Combat Operations. Security requirements may be modified as necessary to meet local conditions in combat or combat-related operations. In these circumstances, follow the provisions of this regulation as closely as possible. This exception does not

apply to regularly scheduled training exercises or operations. Exercises are not combat-related operations.

5. Waivers. When situations arise that require deviation from the standards of this instruction or any of its implementing directives, submit a waiver to the standard or requirement request to the DON Senior Agency Official via CNO or CMC (whichever is appropriate) for consideration and submission to USD (I) for approval.

6. Guidance. Requests for guidance or clarification of this regulation may be addressed formally or informally to, Room 4E572, Washington, DC, 20350-1000. For telephone inquiries, the Security Action Line (with a recorder for after-hours calls) may be reached at DSN 288-5027, commercial (703) 601-5027. Send e-mail requests to donsecurity_pers.fct@navy.mil. DUSN (S&I) homepage at https://portal.secnav.navy.mil/Pages/default.aspx provides policy updates, security awareness items, and other policy materials. Requests for guidance and clarification of this regulation by Navy commands may be addressed by CNO, Director of Navy Staff (DNS), formally or informally, and Marine Corps units may be addressed formally or informally to HQMC Plans, Policy & Oversight/Personnel Security (PP&O/PS).

7. Violations of the Provisions of this Instruction

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

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

COMMAND SECURITY PROGRAM

1. Overview. CO’s are responsible for compliance with and implementation of the DON PSP within their command. The effectiveness of the command's security program depends on the importance given to the program by the CO.

2. CO

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

b. Command security management responsibilities include:

(1) Designating an Activity Security Manager (ASM) in writing.

(2) Designating a TS Control Officer (TSCO) in writing if the command handles TS information.

(3) Designating an Information System Security Manager (ISSM) in writing if the command processes data in an automated system.

(4) Designating a Security Officer in writing to manage facilities security.

(5) Designating a Special Security Officer in writing to administer the command SCI security program.

(6) Issuing a written command security policy instruction.

(7) Establish an industrial security program when the command engages in classified procurement or when cleared contractors operate within areas under the CO’s control.

(8) Ensuring the ASM attends formal training within 180 days of assignment to the position and other command security professionals are appropriately trained, that all personnel receive required security education, and that the command has a robust security awareness program.

(9) Preparing an emergency plan for the protection of classified material.

(10) Ensuring that command security inspections, program reviews, and assist visits are conducted for effectiveness of the PSP in subordinate commands.

(11) Ensuring that the performance rating systems of all DON military and civilian personnel whose duties significantly involve the creation, handling, or management of National Security Information (NSI) include a security element on which to be evaluated.

(12) Ensuring implementation and required use of the JPAS, access to the Defense Information System for Security (DISS) or successor system to communicate with the DoD CAF to receive and respond to notifications of investigations and continuous evaluation alerts.

3. Security Manager

a. Every command in the Navy and Marine Corps eligible to receive sensitive or classified information is required to designate an ASM (also known as Command Security Manager (CSM)) in writing in accordance with reference (b).

(1) CNO, DNS, CMC, and HQMC PP&O/PS will maintain a copy of subordinate ASM designation letters. Navy Echelon I and II ASM will maintain a copy of their subordinate ASM designation letters, per reference (s). Marine Corps CO’s will maintain a copy of subordinate ASM designation letters. The designation letter should include the Unit Identification Code, Security Management Office Code, Electronic Questionnaires for Investigations Processing (e-QIP) four-digit identification number and return e-mail address for program management oversight.

(2) Navy Echelon I and II ASM data will be maintained by CNO, DNS, and CMC. HQMC PP&O/PS will maintain a copy of subordinate Marine Corps commands ASM data to promote program management goals and to allow proper registration for security awareness products, notification of training opportunities, and policy updates. Navy Echelon I and II, HQMC PP&O/PS, and Marine

Corps CO’s ASM will ensure all information is forwarded to subordinate commands as required.

b. The ASM will be afforded direct access organizationally to the CO and be organizationally aligned to ensure effective management of the command's security program.

c. The ASM may be assigned full-time, part-time, or as a collateral duty and must be a military officer, senior non-commissioned officer, E-7 or above, a civilian employee, GS-11 or above (or pay band equivalent), with sufficient authority and staff to manage the program for the command. The ASM must be a U.S. citizen and have been the subject of a favorably adjudicated Tier 5 (T5) background investigation (BI) completed within the five years prior to assignment.

d. The ASM must be designated by name and identified to all members of the command on organization charts, telephone listings, rosters, etc.

e. COs are required to obtain formal training for their ASM. The Naval Security Manager Course offered by the Security Education Training and Awareness Team and the Marine Corps Security Management Course satisfy this requirement.

4. Duties of the ASM

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

(1) The duties described here and in reference (d) may be assigned to a number of personnel and may even be assigned to individuals senior to the ASM. However, the ASM remains ultimately responsible to the CO for all program requirements.

(2) The ASM must be cognizant of the command security functions and ensure the security program is coordinated and inclusive of all requirements. Security management may involve direct supervision, oversight, coordination, or a combination thereof, to ensure that those individuals in the command who

have security duties are kept abreast of changes in policies and procedures, and are provided assistance in solving security problems.

b. The below listed duties and those provided in section 2 of reference (b) apply to every ASM:

(1) Serves as the CO’s advisor and direct representative in matters pertaining to the security of classified information held at the command.

(2) Serves as the CO’s advisor and direct representative in matters regarding the eligibility of personnel to access classified information and to be assigned to sensitive duties.

(3) Develops written command personnel security procedures, including an emergency plan which integrates emergency destruction drills where required.

(4) Formulates and coordinates the command's security awareness and education program.

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

(6) Ensures that all PSI are properly prepared and submitted to the DCSA and monitored until completed; and adjudicated by the DoD CAF for all personnel who will handle classified information or will be assigned to sensitive duties.

(7) Ensures that access to classified information is limited to those who are eligible and have the “need-to-know”.

(8) Ensures that PSI, eligibility, and accesses are properly recorded in the Joint Clearance and Access Verification System (JCAVS) or successor system, and that subordinate commands are properly registered in JCAVS or successor system, as necessary.

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

(10) Maintains liaison with the command SSO concerning information and personnel security policies and procedures.

(11) Coordinates with the ISSM on matters of common concern.

(12) Coordinates with the Human Resources Office on matters concerning civilian personnel to include, development of position descriptions, issues involving access to classified information, or assignment to sensitive positons. Uses the Position Designation Tool to determine position designations and to determine if civilian, contractors, or consultants require national security eligibility.

(13) Ensures that all personnel who have had access to classified information who are separating, retiring, or being terminated from employment have completed a Security Termination Statement in accordance with Section 4-12. The original statement is filed in the individual's Electronic Service Record or Official Personnel Folder (OPF) and a copy is saved in the command’s files.

(14) Ensures all personnel execute a Classified Information Nondisclosure Agreement (SF 312) prior to granting initial access to classified information and records execution of the SF 312 in JPAS or successor system.

5. TSCO. Commands that handle TS material will designate a TSCO, in writing. The TSCO must be an officer, senior non-commissioned officer, E-7 or above, or a civilian employee, GS-7 or above. The TSCO must be a U.S. citizen and have been the subject of a favorably adjudicated T5 investigation completed within five years of initial assignment, with T5 Reinvestigation (T5R) every five years thereafter. The duties of a TSCO are prescribed by reference (d).

6. Other Security Assistants

a. Activity Assistant Security Manager (AASM). Persons designated as AASM must be U.S. citizens, and either officers, enlisted persons E-7 or above, or civilians GS-7, or above. The designation must be in writing and a copy maintained by the ASM for oversight. AASM takes direction from the ASM and provides support, as needed. AASM must have a T5 BI completed and adjudicated by the DoD CAF, if they are designated to issue

interim security clearances; otherwise, the investigative and clearance eligibility requirements will be determined by the level of access to classified information required.

b. Security Assistant. Civilian and military member employees performing administrative functions under the direction of the ASM may be assigned in writing without regard to rate or grade as long as they have the eligibility needed for the access required to perform their assigned duties and tasking.

c. Top Secret Control Assistant (TSCA). Individuals may be assigned to assist the TSCO as needed. The designation will be in writing and a copy maintained by the TSCO for oversight. A person designated as a TSCA must be a U.S. citizen and either an officer, enlisted person E-5 or above, or civilian employee GS-5 or above. A T5 BI completed, adjudicated and eligibility granted by the DoD CAF is required. TS couriers are not considered to be TSCAs. Duties of a TSCA are listed, per reference (d).

7. Contracting Officer's Security Representative (COSR). Commands that award classified contracts to industry will appoint, in writing, one or more qualified security specialists as a COSR. The COSR is responsible to the security manager for coordinating with program managers and technical and procurement officials. The COSR will coordinate with the Contracting Officer's Representative to ensure that the personnel and information security requirements are properly recorded and the industrial security functions are accomplished when classified information is provided to industry for performance on a classified contract are on the DD Form 254, Contract Security Classification Specification, and that personnel security requirements are met when access to DON IT systems is at issue and the requirements are included in the Statement of Work for unclassified contracts.

8. ISSM

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

b. The ISSM is responsible for establishing, implementing and maintaining the DON information system and information assurance program and is responsible to the CO for developing, maintaining, and directing the implementation of the Information Assurance (IA) program within the command. The ISSM advises the CO on all IA matters, including identifying the need for additional IA staff. The IA Manager serves as the command's point of contact (POC) for all IA matters and implements the command's IA program. The ISSM coordinates information and personnel security matters with the ASM, as appropriate. The ISSM must have a favorable T5 completed within five years of initial assignment, which is updated by T5R every five years. The duties and functions of the ISSM are prescribed by reference (j).

9. SSO

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

b. The SSO and a subordinate SSO will be appointed, in writing, and each will be a U.S. citizen and either a commissioned officer or a civilian employee GS-9 or above, and must meet the requirements of reference (l). The same grade limitations apply to assistant SSOs. The ASM cannot function as the SSO unless authorized by the Director, Office of Naval Intelligence, or Commander, FLTCYBCOM.

c. Although the SSO administers the SCI program independent of the ASM, the ASM must account for all clearance and access determinations made on members of the command. There is great need for cooperation and coordination between the SSO and ASM, especially for personnel security matters. For individuals who are SCI eligible, the ASM and the SSO must keep one another advised of any changes in status regarding clearance and access

and of information developed that may affect eligibility. The ASM and SSO must also advise each other of changes in SCI and command security program policies and procedures as they may impact on the overall command security posture.

10. Inspections, Assist Visits, and Reviews

a. COs at Navy Echelon I and II levels and Marine Corps COs are responsible for evaluating the security posture of their subordinate commands.

b. Qualified personnel will conduct inspections, assist visits, and reviews to assess the command's overall security posture. Information and personnel security inspections may be conducted in unison unless otherwise required.

11. Security Servicing Agreements

a. Commands may perform specified security functions for other commands via security servicing agreements. Such agreements may be appropriate in situations where security, economy, and efficiency are considerations, including:

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

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

(3) A senior in the chain of command performs or delegates certain security functions of one or more subordinate commands.

(4) A command with particular capability for performing a security function agrees to perform the function for another.

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

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

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

12. Standard Program Requirements. Each command that handles classified information is required to prepare and keep current a written command security policy manual, specifying how security procedures and requirements will be accomplished in the command. See reference (d).

13. Planning for Emergencies. Commands will establish a plan for the protection and/or removal of classified NSI under its control during emergencies. Depending upon the location of the command, the plan may direct destruction of classified NSI in an emergency. The plan should be made part of the overall disaster preparedness plan of the command security program policy manual.

COUNTERINTELLIGENCE MATTERS

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

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

a. Individuals becoming aware of sabotage, international terrorism, espionage, deliberate compromise or gross negligence involving classified information, or other subversive activities will report all available information concerning such activities immediately to the security manager or CO at their command or at the most readily available command. The command receiving the report shall promptly notify the servicing NCIS office. The command will immediately contact the Director, NCIS (DIRNAVCRIMINVSERV WASHINGTON DC) by classified IMMEDIATE message, with DUSN (S&I) and (NAVY JAG WASHINGTON DC//17//) as information addressees if the servicing NCIS office cannot be contacted immediately and the report concerns sabotage, terrorism, espionage, or imminent flight or defection of an individual.

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

c. NCIS will then advise what additional action is to be taken, and will effect liaison and coordination with appropriate members of the U.S. intelligence community.

3. Contact Reporting

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

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 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 office for action, with an information copy to the DoD CAF. The report will, as a minimum, describe the nature and extent of the classified information to which the individual had access, and the circumstances surrounding the suicide or attempted suicide.

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

5. Unauthorized Absentees

a. When personnel who have access to classified information are determined to be in an unauthorized absentee status, the individual's CO will conduct an inquiry to determine if there are any indications from the individual's activities, behavior, or associations that the absence may be contrary to the interests of national security. If the inquiry develops such concerns, the command will report the pertinent information to

the nearest NCIS office by quickest means available.

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

6. Death or Desertion. When an employee of the DON who has access to classified information dies or deserts, the employee's CO must determine if any unusual indicators or circumstances may have existed that may cause security concern. If such concerns exist, the command will report these concerns by the most expedient means available and provide all pertinent information to the nearest NCIS office.

7. Foreign Travel

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

b. All personnel possessing security clearance eligibility are required to list all personal foreign travel as part of the required Periodic Reinvestigation (PR) in accordance with references (a) and (b) or other reporting guidance issued by the USD (I). The Investigative Service Provider (ISP) 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 individual is bound by affection or obligation, are not citizens of the U.S. Having a financial interest in a foreign country may also present a security risk.

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

c. All personnel with established security clearance eligibility are required to report foreign connections to their ASM in accordance with the references (b) and (r). ASMs must report these issues and coordinate resolution with the DoD CAF as appropriate.

SECURITY EDUCATION

1. Overview

a. Each command handling classified or sensitive 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 program is to ensure that all personnel understand the need and procedures for protecting classified or sensitive information. The goal is to develop fundamental security habits as a natural element of each task.

2. Responsibility

a. DUSN (S&I) is responsible for policy guidance, education requirements, and support for the DON security education program. Development of security education materials for use throughout the DON must be coordinated with DUSN (S&I) for consistency with current policies and procedures. This requirement does not apply to materials that are prepared for use in command programs.

b. Recruit Training Commands are responsible for indoctrinating military personnel entering the Navy and Marine Corps, with a basic understanding of what it means to be serving in a national security sensitive position and explaining what "classified information" is and why the information must be protected. Civilians being employed by the DON for the first time, who will handle classified material or work in a sensitive position, must also be given basic security indoctrination by the employing activity.

c. COs are responsible for security education in their commands, ensuring time is dedicated for training and awareness. Supervisors, in coordination with the ASM, are responsible for determining security requirements for their functions and ensuring personnel under their supervision understands 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 in accordance with references (b) and (d).

b. In formulating a command security education program, the ASM must provide the minimum briefing requirements of this regulation. ASMs must guard against allowing the program to become stagnant or simply comply with requirements without achieving the real goals of this instruction.

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

(1) Advise personnel of the adverse effects that unauthorized disclosure of classified information may have on national security. Further, advise 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 ASM 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 for 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 and accountability, storage, destruction, and transmission of classified information and material and alert them to the strict prohibitions against improper use and abuse of the classification system.

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

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

(8) Instruct personnel having knowledge, possession, or control of classified information on how to determine, before disseminating the information, that the prospective recipient has been authorized access, needs the information to perform his/her official duties, and can properly protect (store) the information.

(9) Advise personnel of the strict prohibition against discussing, transmitting, or electronic processing of classified information over a non-secure telephone, non-secure fax, unclassified IT systems, or in any other manner that may permit interception by an unauthorized person.

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

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

(12) Advise personnel that they are to report to their CO, activity head or designee, contacts with any individual regardless of nationality, whether within or outside the scope of the individual’s official activities, in which:

(a) Illegal or unauthorized access is sought to classified or otherwise 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

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

b. Initial Orientation of all DON personnel shall be provided not later than six months upon employment by the DON in the basic principles of security in accordance with reference (d).

c. Initial briefing of personnel with national security eligibility or assignment to sensitive duties at the time of assignment, regarding command security requirements in accordance with reference (b).

d. On-the-job training in specific security requirements for the duties assigned.

e. Annual refresher briefings for personnel with national security eligibility will receive annual refresher security training in accordance with references (b) and (d). Security education should be on a continuing basis, taking into account each person’s duties, experience, and past conduct involving the protection of classified or sensitive information. DoD Components will maintain records of all refresher training conducted.

f. An annual counterintelligence brief will be given to all personnel.

g. Special briefings as circumstances dictate.

h. Debriefing upon termination of access.

5. Initial Orientation

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

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

c. See reference (d) for guidance on initial orientation intent.

6. Initial Briefing

a. All personnel with national security eligibility will be given an initial security briefing per reference (b) before gaining access to classified information. All individuals will execute the appropriate nondisclosure forms in accordance with reference (b). If individuals decline to execute the nondisclosure forms, the DoD Component will withhold classified access and report the refusal to the DoD CAF. CNO and CMC will ensure maintenance of records of all initial briefings.

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

c. The timing and format for orientation will vary, depending on the size of the command. At large commands with a high turnover rate, briefings may be scheduled on a regular basis. At smaller commands where there is little turnover of personnel, individual security orientation briefings may be necessary.

d. Initial briefing is intended to brief:

(1) The command security structure (i.e., who the ASM is, who the TSCO is, SSO, etc.).

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

(3) Command security procedures for badging, security check-points, destruction, visitors, etc.

(4) Their responsibility to protect classified information.

(5) Their obligation to report suspected security violations.

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

e. Additionally, commands must ensure that individuals receive the requisite cybersecurity, 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 access level are key features of a core IA awareness program.

f. 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.

7. On-the-Job Training (OJT)

a. OJT is the phase of security education when security procedures for the assigned position are learned. ASMs will assist supervisors in identifying appropriate security requirements.

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

8. Refresher Briefing

a. Personnel with national security eligibility will be provided refresher training in their responsibilities at least once a year in accordance with references (b) and (d). Commands will include the entire workforce to ensure personnel understand obligations for reporting derogatory information and for protecting sensitive and classified information.

b. Security education should be on a continuing basis, taking into account each person’s duties, experience, and past conduct involving the protection of classified or sensitive information.

c. Records will be maintained of all refresher training conducted.

9. Counterintelligence Briefings. All DON personnel shall receive initial and annual Counterintelligence Awareness and Reporting training in accordance with reference (m). The ASM is responsible for arranging for the briefing with the local NCIS office or supporting USN or USMC CI office.

10. Special Briefings

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

(1) Foreign Travel Briefing:

(a) CO's will establish appropriate internal procedures requiring all personnel possessing national security eligibility to report to their security office all personal foreign travel at least 14 days in advance of the travel being performed.

(b) Personnel having access to classified information will be given a Foreign Travel Briefing by a CI agent, Security Manager, or other qualified individual, as a defensive measure prior to travel abroad. These personnel will also receive a foreign travel debriefing upon their return.

(c) Personnel with SCI eligibility will follow procedures in accordance with references (b), (k), and (o).

(d) Individuals who travel frequently or attend or host meetings with foreign visitors as described in paragraph b, need not be briefed for each occasion, but will be provided a defensive security and counterintelligence briefing at least once every six months and a general reminder of security responsibilities before each such activity.

(e) Personnel will be reminded of their responsibility to enter and exit the U.S. using a U.S. Passport, report all unofficial foreign travel, and report the use of a foreign passport when traveling outside the U.S.

(f) All personal foreign travel for personnel with national security eligibility will be entered in DISS or successor system and maintained for five years. Any previous manual foreign travel records will be forwarded to the gaining command upon transfer of the individual. The losing command will retain a copy of the foreign travel record on file for one year after the individual's departure. Foreign travel records of individuals who retire, separate, or terminate employment will be retained at the losing command until the expiration of the five-year period.

(2) New Requirement Briefings. Whenever security policies or procedures change, personnel whose duties would be impacted by these changes must be briefed in a timely manner.

(3) Program Briefings. Briefings that are specified or required by other program regulations (e.g., North Atlantic Treaty Organization (NATO), Single Integrated Operational Plan-Extremely Sensitive (SIOP-ESI), SCI, etc.).

(4) NATO Security Briefing. All personnel who are in a NATO billet and have access to a SIPRNET terminal accredited to receive and process NATO information must receive a NATO security briefing.

b. Special briefings will be recorded in JPAS as functionality permits, or records may be maintained locally in the form of rosters or other automated format, until JPAS or successor system of record keeping functionality is fully deployed.

11. Command Debriefing

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

(1) Transfers from one command to another.

(2) Terminating active military service or civilian employment.

(3) Temporarily separating for a period of 60 days or more, including sabbaticals, leave without pay status, or

transfer to the Inactive Ready Reserves.

(4) Expiration of a Limited Access Authorization (LAA).

(5) Inadvertent substantive access to information that the individual is not eligible to receive.

(6) Security clearance eligibility revocation.

(7) Administrative withdrawal or suspension of security clearance and SCI access eligibility for cause. Refer to Section 8 for additional information.

b. Debriefings must include the following:

(1) All classified material in individuals' possession must be returned.

(2) Individuals are no longer eligible for access to classified information.

(3) Reminder of the provisions of the Classified Nondisclosure Agreement (SF 312) to never divulge classified information, verbally or in writing, to any unauthorized person or in judicial, quasi-judicial, or in administrative proceedings without first receiving written permission from DUSN (S&I).

(4) There are severe penalties for disclosure.

(5) 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, any attempt by an unauthorized person to solicit classified information.

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

12. Security Termination Statements

a. Individuals must read and execute a Security Termination Statement at the time of debriefing, unless the debriefing is done simply because the individual is transferring from one command to another and will continue to require access to classified information or, for SCI access, the Security Debriefing Acknowledgement and Debrief statement on DD Form 4414, Sensitive Compartmented Information Nondisclosure Agreement.

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

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

d. The original signed and witnessed Security Termination Statement will be placed in the individual's official service record or the official personnel folder for permanent retention except, when the Security Termination Statement is executed at the conclusion of a Limited Access Authorization, the original will be retained in command files for two years.

e. If an individual refuses to execute the Security Termination Statement, the individual will be debriefed, before a witness if possible, stressing the fact that refusal to sign the Security Termination Statement does not change the individual's obligation to protect classified information from unauthorized disclosure as stated on the SF 312. The Security Termination Statement will be annotated to show the identity and signature of the witness, if one was present, and that the individual was debriefed, but refused to sign the Security Termination Statement. Send a copy of refusals to the DoD CAF via JPAS or successor system as an incident report.

f. The SECDEF has specifically directed that Security Termination Statements will be executed by senior officials (Flag and General Officers, ES-1 and above, Senior Executive Service (SES) and equivalent positions). The immediate senior official will ensure that the statement is executed and that failure to execute the statement is reported immediately to the Deputy Assistant Secretary of Defense and the DoD CAF via JPAS

or successor system as an incident report.

13. Training for Security Personnel

a. The DON Security Education Training and Awareness Team offers the Naval Security Manager Course for Navy security managers, security specialists and assistants. For details, visit the DUSN (S&I) website at: https://portal.secnav.navy.mil/orgs/DUSNP/Security-Directorate/SitePages/Home.aspx.

b. HQMC PP&O PS offers the USMC Security Management Course for USMC command leadership, security managers, security specialists, and assistants.

c. For other security training available to DON personnel, e-mail the DUSN (S&I), security education specialist at don_security_inf.fct@navy.mil.

14. Security Awareness. To enhance security, a security education program must include continuous and frequent exposure to current information. Both in-person and technological delivery methods are encouraged. Other media to promote security awareness may include signs, posters, bulletin board notices, and Plan of the Day reminders.

NATIONAL SECURITY INVESTIGATIONS

1. Overview

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 conduct sufficient to demonstrate the likelihood that an individual will carry out assigned federal government duties with the necessary integrity or efficiency of the service. Suitability adjudication of background information typically occurs after the qualification determination; however, it may take place at any point during the hiring process, e.g., a final suitability determination may be made after review of a completed OF-306, after review of completed application material, or after review of a completed BI. No individual will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made regarding his/her loyalty, reliability, and trustworthiness.

b. National security positions include those positions that involve activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage; and positions that require regular use of, or access to, classified information or assignment in a sensitive position. The DON mission is such that most DON positions are sensitive national security positions. A national security position will not be downgraded or reclassified as non-sensitive solely to aid in recruiting personnel or to retain personnel who no longer possess national security eligibility as required for a position.

c. Only the following officials are authorized to request BI on individuals under their jurisdiction:

(1) COs of organizations and activities listed on the Standard Navy Distribution List and Marine Corps COs (Battalion or higher).

(2) DCSA, Defense Vetting Directorate, Vetting Risk Operations Center (VROC), and DoD CAF.

(3) Chiefs of recruiting stations.

d. Suitability determinations are under the purview of Deputy Assistant Secretary of the Navy (Civilian Personnel) (DASN (CP)) for employment. DON National Security Position suitability, for employees in positions not subject to suitability or fitness to perform work for or on behalf of the DoD as a contractor, determinations are under DUSN (S&I) purview and are governed by this instruction.

e. A BI is conducted to gather information pertinent to the determinations established in the Federal Investigative Standards (FIS) in accordance with reference (b). The scope of the investigation conducted will be commensurate with the level of sensitivity of the access required or position occupied in in accordance with reference (b). Only the minimum investigation to satisfy a requirement may be requested. DUSN (S&I) must give prior approval to establish investigative requirements in addition to, or at variance with, those established here.

f. The DCSA conducts (or controls the conduct of) all BIs for the DON. DON elements are prohibited from conducting BIs, including local public agency inquiries, unless specifically requested to do so by an authorized investigative agency. An exception to this restriction is made for DON overseas commands employing foreign nationals for duties not requiring access to classified material. Reference (b) provides further details.

g. BIs will not be requested for any civilian or military personnel who will be retired, reassigned, or separated with less than one year of service remaining.

2. Position Designation. In order to adjudicate suitability and to provide the appropriate level of (BI), positions are designated according to potential risk. Reference (b) 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:

a. Special-Sensitive (SS). Potential for inestimable impact and/or damage.

b. Critical-Sensitive (CS). Potential for grave to exceptionally grave impact and/or damage.

c. Noncritical Sensitive (NCS) Potential for some to serious impact and/or damage.

3. Criteria for Designating Sensitive Positions

a. SS and CS positions require a favorably adjudicated T5.

b. NCS positions require that civilian personnel in NCS positions require a favorably adjudicated Tier 3 (T3)(for temporary or interim eligibility). A National Agency Check with Law and Credit (NACLC) favorably completed during a previous military or contractor employment may be used to support civilian appointment provided a T3 has been submitted to the ISP and the individual has not had a 24-month break in service since completion of the last investigation.

c. Seasonal employees (including summer hires) normally do not require access to classified information. If the position requires access to classified information, the proper investigation will be initiated to meet the required access level (see para 6-1 for age limitations). BIs will not be submitted for individuals below the age of 16. With the exception of military personnel, minors who are under the age of 18, will not be investigated nor granted national security eligibility.

d. The process of designating sensitive positions is best accomplished in coordination with the human resource officer, the position supervisor, program manager, the security manager, or the appropriate IT authority. Office of Personnel Management (OPM) Position Designation Tool:

(https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/) simplifies this process for civilian, contractors and consultants in national security positions. The CO may establish standard operating procedures to discharge this responsibility.

e. The sensitivity 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. The position sensitivity is identified on OF 8, Position Description, (Block 12), for civilians and will be recorded in JPAS or successor system. The investigation submitted must correlate with the sensitivity level identified in JPAS or the successor system.

(1) Contracts, grants, and other legal agreements or understanding with non-DoD entities involving sensitive duties will incorporate the security requirements specified herein according to applicable policy and guidance sections of reference (b).

(2) The ASM 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 or sensitive information will normally be predominating.

4. Types of BI. The term BI refers to an information gathering inquiry, where specified information is collected from specified sources to support eligibility determinations for DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DoD for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive national security positions, or other designated duties requiring such investigation. Investigations conducted for other basic purposes may have an impact on security

clearance determinations but are not BIs (examples of other types are investigations of compromise, criminal activity, sabotage, espionage, or subversion).

5. Federal Investigative Standards (FIS) for Civilian, Military, and Contractor Personnel

a. FIS provides consistent standards for investigations, to facilitate reciprocity across the government, and to ensure cost-effective and efficient protection of national interests. The standards apply to investigations used to determine eligibility for access to classified information, to hold a national security position, for physical and logical access, and for suitability for government employment. The FIS established a new tier and naming system for BI. The scope of a PSI may be neither raised nor lowered without the approval of the DNI. The tiered national security investigations authorized for use within the DON are as follows for civilians, military, and contractor personnel:

(1) T3: Investigations conducted to this standard are for positions designated as NCS, and/or requiring eligibility for L access or access to Confidential or Secret information. This is the lowest level of investigation acceptable for access to classified information, using SF 86, Questionnaire for National Security Positions, or its successor form to include the below requirements for military personnel:

(a) A favorably adjudicated T3 is required for each enlisted member, commissioned officer, Warrant Officer, Midshipman and Reserve Officer Training Corps candidate before appointment in the Navy and Marine Corps, including Reserve components, at the time of initial entry into the service.

(b) All derogatory information revealed during the enlistment or appointment process that results in a waiver of accession standards will be fully explained in a written summary attached to and forwarded with the SF 86.

(c) The authority to take action to deny acceptance or retention in the Navy and Marine Corps, except for loyalty reasons, is vested in the CHNAVPERS and the CMC. Cases

involving loyalty issues of Navy personnel will be forwarded to CNO for submission to DUSN (S&I) for referral to the SECNAV for action. Cases involving loyalty of USMC personnel will be forwarded to HQMC PP&O/PS for submission to DUSN (S&I) for referral to the SECNAV for action.

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

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

(2) T5. Investigations conducted to this standard are for positions designated as critical sensitive, special sensitive, and/or requiring eligibility for Q access or access to TS or SCI, using SF 86, or its successor form.

b. Reinvestigation. A reinvestigation updates a previous investigation and is authorized only for specific duties and access. All military members will undergo PR, maintain a favorable eligibility, and be subject to continuous evaluation. Civilian and contractor personnel will undergo PRs to the extent that the investigative coverage is proportional to the sensitivity level of the duties and/or access required. Reinvestigations may be performed at any time after national security eligibility has been granted. Additionally, DON employees in national security positions and contractor personnel performing national security duties without access to classified information will be subject to reinvestigation on a recurring basis. There are two tiered national security reinvestigations:

(1) Tier 3 Reinvestigation (T3R): T3R is the reinvestigation required for military, civilian, and contractor positions designated as non-critical sensitive, and/or requiring eligibility for L access or access to Confidential or Secret information, or assignment in a NCS position, respectively. T3Rs are also conducted at 10 years intervals for collateral positions or five-year intervals for personnel with Secret

security clearance in SAPs and those performing Explosive Ordnance Disposal or Personnel Reliability Program (PRP) controlled duties. The reinvestigation will be initiated no later than five years from the close date of the previous investigation.

(2) T5R: T5Rs are conducted on each military, civilian, and contractor occupying a SS or CS position or requiring continued national security eligibility at an equivalent level will undergo a T5R every five years. The T5R is also required to support personnel security determinations on personnel with continued assignment to NATO billets requiring TS Constellation Observing System for Meteorology, Ionosphere, and Climate (COSMIC) access, Nuclear Weapons PRP, privileged access IT, Presidential Support Activities (PSA), access to SIOP-ESI, and for LAAs for non-U.S. citizens employees. The T5R investigative elements include: a National Agency Check (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.

c. Reinvestigations will not be initiated more than 30 days prior to the due date (the date the previous equivalent or higher level BI closed). Personnel assigned to a NATO staff positions may submit a reinvestigation request up to one year in advance of the required timeframe in accordance with reference (b).

d. Individuals in a SAP will submit reinvestigations in accordance with the provisions outlined in reference (b).

e. Reimbursable Suitability/Security Investigation (RSI). An investigation conducted to resolve personnel security issues that arise after a BI is conducted, evaluated, or adjudicated. RSIs are scoped as necessary to address the specific matters to be resolved. They usually consist of record checks and interviews with potentially knowledgeable persons. The subject of the investigation may be interviewed to resolve conflicting information and/or to provide an opportunity to refute or mitigate adverse information. The term "RSI" applies to limited

inquiries, post-adjudication investigations, or other additional inquiries conducted by NBIB. If deemed appropriate, RSIs are requested by the DoD CAF to DCSA after coordination with the command. Commands will obtain the SF 86 as directed by the DoD CAF. RSIs do not cover investigations of criminal activity, sabotage, espionage, or subversion. Those are matters under the investigative jurisdiction of the NCIS. RSIs are requested and managed by the DoD CAF.

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

g. NAC. The NAC is an integral element of all BI and is the baseline for interim TS or interim SCI national security eligibility determinations. The NAC is a records checks of databases that includes the FBI Fingerprint (FP) check, FBI Name check, a list of previous investigations recorded in DCSA Security/Suitability Investigations Index (SSII), a Defense Central Index of Investigations (DCII) check, and a credit check. Checks such as Selective Service, Military Personnel Records, and State Department Passport Office are scheduled when certain conditions are met.

h. Advance NAC. The Advance NAC consists of an itemized list (generally FBI FP, FBI Name, DCSA's SSII and DCII checks) of the NAC results and search status.

i. FP Special Agreement Check. The FP Special Agreement Check (SAC) is an integral part of all initial investigations, and is conducted in conjunction with the submission of all initial BI and some reinvestigations. FP SACs will be electronically captured and submitted via the Secure Web FP Transmission portal.

j. Polygraph. Polygraph examinations may be used in PSIs under the conditions specified in and as stated in reference

(n). No unfavorable national security eligibility determination will be taken based solely on a polygraph examination that is interpreted as indicating deception or is inconclusive. Refusal to take a voluntary polygraph will be given no consideration, favorable or unfavorable, when making a national security eligibility determination. Admissions made during the polygraph interview or attempts to employ countermeasures to defeat a polygraph may be considered when making a national security eligibility determination.

6. Investigative Requirements for Civilians in Sensitive Positions

a. A previously conducted Access National Agency Check with Inquiries (ANACI) or Single Scope Background Investigation (SSBI) satisfies federal civilian employment suitability requirements for sensitive duty assignment provided there has been no break in service exceeding 24 months; however, a previously conducted NACLC will not. A T3 or T5 is required for reappointment to a federal government sensitive position if there has been a break in service greater than 24 months.

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

c. See reference (b) for more information.

d. Temporary Employment. A T3 is the minimum requirement for civilian summer hires in all designated non-critical sensitive positions including summer hires, intermittent and seasonal appointees, or work/study and cooperative education program employees. To the greatest extent possible, investigations requested to support sensitive duty assignment should be requested far enough in advance to allow completion and adjudication of the T3 prior to assignment. Any temporary, intermittent, summer hire, or seasonal employee who is granted national security eligibility must be 18 years of age or older on or before national security eligibility is granted. All waiver requests must be submitted to CNO, DNS, CMC, and HQMC PP&O/PS; and forwarded to DUSN (S&I) for consideration and

submission to Director, Defense Intelligence (Intelligence and Security) (DDI (I&S)).

e. Emergency Appointments. If the appointee does not have the necessary investigative basis for appointment, he/she may be placed in a non-critical sensitive position only as an emergency measure after the CO determines that delay in appointment would be harmful to the national security (not to exceed 180 days), the T3 has been requested, favorable fingerprint result received, and a check of locally available records is favorable. The CO's justification for the emergency appointment will be recorded in writing. Commands must maintain a central file of all emergency appointments for review during security and personnel management evaluations. The record of emergency appointments will include:

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

(2) Organizational location of the position.

(3) Position sensitivity and designation criterion.

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

(5) A statement that a check of locally available records was favorable.

(6) The date that the required BI was requested. For a critical-sensitive position, the record will also include the date of the T3 that formed the basis for emergency appointment.

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

(8) Additional investigative requirements for assignment to selected job series or duties are established and authorized by Section 5. Section 5 documents the requirements used for BI planning and budgeting.

(9) Mobilization. For the purpose of mobilizing selected civilian annuitants under reference (u) with a break in active service greater than 24 months, investigative requirements will be expedited or waived, depending on the sensitivity of the position. Priority will be afforded to mobilized reemployed annuitants being assigned to intelligence and security activities with respect to granting security clearances.

(10) U.S. Coast Guard. For the purposes of partial or full mobilization under provisions of reference (v). (Title 14 pertaining to the U.S. Coast Guard as an element of the DON), the requirement for a T3 upon reentry may be waived.

7. Investigative Requirements for DON Contractor Personnel

a. Investigative requirements for DON contractor personnel requiring access to classified information are managed under the National Industrial Security Program (NISP). Requests for investigation of contractor personnel for security clearance eligibility are processed by the Defense Counterintelligence and Security Agency (DCSA) Vetting Risk Operations Center (VROC) and adjudicated by the VROC. When SCI access is at issue, reference (k) applies. The VROC and the DoD CAF are the adjudicative authority for all DON contractor personnel requiring SCI access eligibility.

b. Contracts involving sensitive duties and/or DON systems, should incorporate the security requirements specified herein to ensure applicable personnel security requirements are included in all contracts, agreements, memorandums of understanding, and other documents in accordance with the Defense Federal Acquisition Regulations. Non-NISP adjudications for contract personnel are done by the requesting command, using reference (b).

c. Consultants hired by a DON Government Contracting Activity. A consultant who is individually hired by a DON command or activity, will work strictly at the command/activity,

and requires access to classified information only at the command/activity, or in connection with authorized visits, will have security clearance eligibility established under this regulation. The consultant is considered for security clearance purposes as an employee of the DON command/activity and is investigated by DCSA and adjudicated by the DoD CAF, as appropriate.

8. Specific Duty or Assignment Requirements

a. The following specific duties are assigned minimum investigative or clearance requirements:

(1) ASM. The designated security manager of a command must have a favorably adjudicated T5 or T5R completed within the past five years.

(2) Personnel Security Clearance Adjudication Officials. Any person selected to serve with a board, committee, or other group responsible for adjudicating personnel security cases shall have been the subject of a favorably adjudicated T5, T5R completed within the past five years.

(3) Appellate Authorities. Persons selected to serve with a board, committee, or other group responsible for adjudicating appeals of personnel security determinations must have a favorably adjudicated T5 or T5R completed within the past five years.

(4) Educational and Training Programs. Persons selected for duties in connection with formal programs involving the education and training of military or civilian personnel must have a favorably adjudicated T3 or T3R prior to assignment. This requirement applies to those assigned to formal programs and does not include those incidentally involved in training. It does not apply to teachers or administrators associated with university extension courses conducted on DON installations in the U.S.

(5) Cryptographic Duties. Personnel assigned to cryptographic duties must have the appropriate security clearance eligibility established prior to accessing U.S. cryptographic information. Interim security clearances are not valid for access to U.S. cryptographic information.

(6) Investigative Duties. Investigative agents and other personnel assigned to investigative agencies whose official duties require continuous access to investigative files and materials, require a favorably adjudicated T5 or T5R completed within the past five years.

(7) NAF. NAF employees assigned to positions of trust within DoD will be the subject of a favorably adjudicated Tier 1 (T1), (non-sensitive), investigation completed no greater than 24 months prior to appointment. A favorably completed prior investigation for Federal service which meets or exceeds the T1 standard will satisfy this requirement if there has not been a break in service greater than 24 months between Federal service and employment by NAF Instrumentalities. NAF employees requiring eligibility determination will be processed in accordance with reference (b). If access to a DON computer system and/or network is required, the position will be designated and the appropriate BI will be submitted in accordance with reference (b).

(8) American Red Cross/United Service Organization (U.S.O.). A favorably adjudicated T3 is required on American Red Cross or U.S.O. personnel as a prerequisite for assignment to activities overseas.

(9) Chemical Agents. Personnel whose duties involve access to or security of chemical agents require a favorably adjudicated T3 completed within the past five years before assignment.

(10) Arms, Ammunition, and Explosives (AA&E). Personnel operating a vehicle or providing security to a vehicle transporting Category I, II, or Confidential AA&E require a favorably adjudicated T3 or T3R.

(11) Contract Guards. Contract guards require a favorably adjudicated T3 or T3R.

(12) Foreign Nationals Employed Overseas

(a) A non-U.S. citizen employed overseas, who provides support to national security positions and who does not require access to classified information, will be subject to the

following record checks initiated (before employment) International, bi-lateral, or subsidiary agreements governing locally hired employees may require additional investigation. The minimum required checks are:

1. Host government law enforcement and security agency checks at the city, state (province), and national level whenever permissible by the laws of the host government and when practical, considering CI responsibilities in accordance with reference (b).

2. DoD-approved automated records checks.

3. FBI records (where information exists indicating residence by the non-U.S. citizen in the U.S. for one year or more since age 18).

(b) The commander assumes responsibility for permitting access to DoD systems, unclassified information, material, and areas when an investigation conducted by the host country does not meet the investigative standards of this regulation.

(c) The commander will allow access to unclassified information by a non-U.S. citizen only in accordance with applicable disclosure policies and when such access cannot cause significant or serious damage to U.S. national security.

(d) The commander may choose to include additional checks, as appropriate.

(13) Nuclear Weapon PRP. Reference (g) provides the standards of individual reliability required for personnel performing duties involving nuclear weapons and components. PRP requires commands to screen personnel before transferring them to training which leads to a PRP assignment. The investigative requirements for PRP assignment are based on the position designation. The PRP positions are designated as either critical or controlled.

(a) Critical PRP Position. The investigative requirement for initial assignment to a critical PRP position is a favorably adjudicated T5 completed within the past five years. A favorably adjudicated T5R may also satisfy this requirement.

If there is no investigation to satisfy the requirement for initial assignment, the command must request an T5. A SSBI-PR/T5R is required every five years.

(b) Controlled PRP Position. The investigative requirement for initial assignment to a controlled PRP position is a favorably adjudicated T3 or T3R completed within the past five years. An existing favorably adjudicated SSBI or SSBI-PR completed within the past five years will also suffice. When there is no investigation to satisfy the requirements for initial assignment, the command must request a T3, as appropriate. When requesting a new investigation, the request must be properly annotated to reflect PRP assignment. A T3 or T3R is required every five years for continued PRP assignment.

b. In addition to the above specific duties, there are minimum investigative and citizenship requirements for assignment to specified facilities necessitated by the nature of the command mission and operational structure. These specific facility requirements are unrelated to specific duties and are enumerated and authorized by Section 5. Section 5 documents the requirements used for BI planning and budgeting.

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

9. Specific Program Requirements

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

(1) SAP. SAP are discussed in paragraph 1-7 and are established in DoD under SAP Oversight Committee authority. SAP requirements may include, but are not limited to, special clearance eligibility, additional adjudication, unique investigative requirements, material dissemination restrictions, and formal identification of

personnel with need-to-know. These requirements are specifically determined by the SAP manager.

(2) SCI. The investigative requirement for access to SCI is a favorably adjudicated T5. A T5R is required to be submitted every five years. The requirements for SCI access are established under Director of National Intelligence authority. When military personnel are ordered to billets requiring SCI access, the transfer orders will identify the requirement. The losing command's ASM/SSO must ensure the required investigative requests are submitted promptly prior to transfer. If an individual is indoctrinated for SCI access, the CO may not administratively lower the individual's security clearance below the TS level without approval of the DoD CAF.

(3) Nuclear Command and Control-Extremely Sensitive Information (NC2-ESI). Investigative requirements for access to NC2-ESI information vary depending on whether the information to be accessed is SIOP or NC2-ESI.

(a) Access to NC2-ESI is based on need-to-know and requires security clearance eligibility commensurate with the classification of the information to be accessed.

(b) Access to NC2-ESI requires a TS security clearance eligibility based on a favorably adjudicated SSBI. The SSBI need not have been completed within the past five years to grant access to NC2-ESI, providing a new T5 or T5R is initiated within 30 days.

(4) PSA. Reference (o) prescribes the policies and procedures for the nomination, screening, selection, and continued evaluation of DON military and civilian personnel and contractor employees assigned to or used in PSA. There are two categories of PSA assignments, Category One and Category Two.

(a) Personnel nominated for Category One and Category Two duties must have been the subject of a favorably adjudicated SSBI completed within the 36 months preceding selection into Presidential Support duties.

(b) DON personnel in support of Presidential activities will be processed for expedited BI. The ASM will

monitor JPAS or successor system and submit a request to the DoD CAF requesting expedited adjudication when the BI is closed.

(c) The U.S. citizenship of foreign-born immediate family members of all Presidential Support nominees must be verified by investigation. If the individual marries or cohabitates after completion of the T5, a spouse NAC must be requested.

(5) NATO. An equivalent level U.S. security clearance is the basis for access to NATO classified information. See reference (b) for more information.

(a) The investigative basis for a NATO staff position/billet is a favorably adjudicated T5, T5R, T3 or T3R, depending on the level of clearance and access the billet requires. The investigation must have been completed within the five years preceding the assignment. Continued assignment to a NATO COSMIC billet requires T5R every five years.

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

(c) Personnel not assigned to a NATO staff position, but requiring access to NATO information in the normal course of their duties, must possess the equivalent final U.S. national security eligibility based upon the appropriate PSI.

(d) Personnel assigned to NATO staff positions may submit reinvestigation requests up to one year in advance of the required timeframe.

(6) Wounded Warrior Security and Intelligence Internship Program.

(a) PSIs in support of designated wounded Service Members may be submitted and processed regardless of the time remaining in service. Reinvestigations will be submitted in accordance with reference (b).

(b) Category 2 wounded, ill, or injured Service Members who expect to be separated with a medical disability rating of 30 percent or greater may submit investigative requests for TS or SCI eligibility before medical separation as long as they are serving in or have been nominated for a Wounded Warrior Internship Program.

(c) The investigations will be funded by the DoD office offering the internship. If the office offering the internship does not have funds available, the owning Military Department may choose to fund the investigation.

(d) Investigations submitted in support of Wounded Warrior Security and Intelligence Internship Program should:

1. Not request priority service.

2. Include the extra coverage code "WW" in Block B of the "Agency Use Only" section of the SF 86. This will expedite scheduling and completion of investigations submitted in support of the Wounded Warrior Security and Intelligence Internship Program.

3. Notify NBIB via e-mail to operationwarfighter@nbib.gov. Include the subject's full name, the e-Application (e-App) request identification number, and the DoD POC should NBIB need additional information.

b. A listing of investigation and citizenship requirements for assignment to special programs is provided and authorized by reference (b). Reference (b) and Section 5 documents the requirements used for BI planning and budgeting.

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

10. Reciprocity and Acceptability of Previously Conducted Investigations

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

b. Before initiating a new investigation, command security personnel will search JPAS and successor system or other linked automated investigative indices, such as JPAS Special Investigative Inquiry and the OPM Central Verification System, for evidence of a previously conducted investigation that meets requirements.

(1) If subject provides information regarding a previous investigation conducted by an agency other than DCSA, this information must be verified by the DoD CAF. Submit a request to DoD CAF via JPAS, or successor, advising of the adjudicative requirements, and provide the information regarding subject's previous investigation. The DoD CAF will verify and respond regarding eligibility and investigative reciprocity.

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

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

(1) The previous investigative file was never properly adjudicated.

(2) Potentially disqualifying information was developed since the last favorable adjudication.

(3) The most recent clearance or access authorization was conditional or based on a waiver.

(4) The individual is being considered for a higher level of clearance eligibility by the DoD CAF, or other official command program requirements.

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

e. Conversely, when it becomes necessary for a commanding officer to grant access to personnel from other military departments or DoD agencies who do not have the required security clearance eligibility, the DON command granting access will submit a request for investigation to DCSA indicating that the results are to be forwarded to the DoD CAF. The DoD CAF will be responsible for expeditiously transmitting results of the security clearance determination to the requestor.

f. Review of Prior Investigations. Prior BIs may only be requested for review in support of an official requirement.

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

(2) All requests must be justified and forwarded to the Defense Counterintelligence and Security Agency by following the "Pre-Placement" instructions outlined at the following link: https://www.dcsa.mil/mc/pv/gov_hr_security/requesting_files/.

11. Limitations on Requests for Investigation

a. BIs for purposes other than allowed by this policy manual regulation are not authorized unless detailed justification has been submitted to CNO, DNS or CMC, HQMC PP&O/PS for endorsement and forwarded to DUSN (S&I) for consideration and submission to DDI (I&S).

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

c. Requests for BIs will not be submitted on any civilian or military personnel who will be retired, resigned, or separated with less than one-year service remaining.

12. Command Responsibilities in BI Requests

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

(1) Ensure the investigative requirements for military and civilian employees are accurately recorded in appropriate personnel systems. This data will be used for programming and to validate electronic BI requests.

(2) Local Records Check. Check locally available records at the command and provide relevant data to the ISP concerning the subject to include: e-App, electronic fingerprints (e-FP), and signed releases, as necessary. Security offices are not authorized to conduct investigations off of the installation or through the internet (i.e. courthouse records, credit checks, law enforcement checks). Local record checks will be retained on file until final eligibility is determined. A review of local civilian law enforcement records, the National Crime Information Center, and the servicing NCIS office is prohibited.

(3) Validate Citizenship. For individuals who are born outside the U.S., extra coverage codes will be entered on the investigative request forms to ensure NBIB accomplishes the citizenship validation in accordance with national standards. Commands (Human Resource Office) will also validate citizenship of individuals before submitting initial BI requests. (Only U.S. citizens are eligible for security clearance or assignment to a sensitive national security position).

(4) Verify Date and Place of Birth and Education. When requesting an T5 or T5R, commands will attempt to validate subject's date and place of birth through review of available personnel records. However, for education verification, extra coverage codes will be entered on investigative request forms to

ensure DCSA accomplishes the education validation in accordance with T5 standards. This is not necessary when requesting a T3 or T3R.

(5) Ensure the investigation request is completed and prepared using current guidance to preclude rejection by DCSA. Current directions for completing investigation requests can be found at the DUSN (S&I) website, https://portal.secnav.navy.mil/Pages/default.aspx.

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

c. Pre-Screening Interview

(1) Before a request for a T5 for SCI access is submitted to DCSA, the nominee must undergo a pre-screening interview. Unfavorable information developed during the pre-screening interview that is not fully explained in the applicable remarks sections of the SF 86, will be explained in a written report that identifies the interviewer and is attached to the T5 submission. Note: Individuals who are in or selected for command status. (CO/Executive Officer) do not require a pre-screening interview.

(2) Questions pertaining to an individual's sexual orientation are not permitted on personnel security questionnaires, supplemental questionnaires, or screening forms, therefore will not be asked during subject pre-screening interviews.

13. BI Request Forms

a. E-QIP. E-Qip or successor application is the federal government standard automated request tool for BI. E-QIP or successor application are a part of the e-government, e-clearance initiative sponsored by the NBIB. E-QIP or successor applications allows applicants to electronically enter, update, and transmit their personal investigation data over a secure Internet connection to their employing agency or security management office for review and approval in conjunction with the BI request.

b. SF 86, “Questionnaire for National Security Positions.” The SF 86 is the currently approved method of requesting BI products from DCSA to support determinations of eligibility for assignment to sensitive national security positions or access to classified NSI. The subject of the investigation completes the SF 86 electronically. The Agency Use information and the release forms are imbedded in the SF 86. Requesting commands must electronically submit fingerprints with each request, except for the T5R/T3R via Secure Web Fingerprint Transmission (SWFT) portal. Access to SWFT can be obtained from the Navy’s Echelon I or II security offices, HQMC PP&O/PS, or Marine Corps COs. Hard copy submission is available using the SF 87 for all DON employee/applicant, military, volunteers as well as contractors until connection to the SWFT is obtained.

14. Preparation and Submission of Investigation Requests

a. The NBIB Federal Investigative Services Division (FISD) will accept BIs submitted electronically via e-QIP or successor system using the approved Standard Forms: SF 86, and the SF 86A, Continuation Sheet for Questionnaires. Use the SF 86A when additional space for documentation is required.

b. Directions for completing, preparing, and transmitting BI requests forms are on the DUSN (S&I) web page at: https://portal.secnav.navy.mil/Pages/default.aspx. It’s very important to follow request directions precisely, especially the directions regarding the “Agency Use” coding, as failure to properly code request will result in returned requests.

(1) Use the assigned Submitting Office Number (SON) and Submitting Office Identifier (SOI):

(a) The SON is authorized to obtain information on the case status of a BI. For the purpose of creating a new SON, the PIPS Form 12, SON Creation and Amendment Form is submitted to DUSN (S&I) via CNO, DNS or CMC, HQMC PP&O/PS for approval and submission to OPM. For the purpose of amendment to the SON, the PIPS Form 12 is submitted to OPM via CNO or CMC.

(b) The Navy Echelon I and II and HQMC PP&O/ASM is authorized an SOI until an automated solution is developed to receive advance fingerprint results and case closing transmittal reports via JPAS or successor system. The Navy Echelon I and II and HQMC PP&O/ASM can add additional users as required to

identify the appropriate official who will receive case results, data, or other information from DCSA. Security offices employees may contact the DCSA to obtain detailed information about a case. Approved employees are the only individuals who may receive information by telephone or secure e-mail. For the purpose of creating a new SOI, the PIPS Form 11, SOI Creation and Amendment Form is submitted to DUSN (S&I) via CNO, DNS or CMC, HQMC PP&O/PS for approval and submission to DCSA.

(2) The subject of each BI will provide their personal information as required by DCSA. At a minimum, the subject will:

(a) Provide accurate and complete data as part of the investigation.

(b) Complete the appropriate investigative forms through e-App and e-FP capture devices.

(c) Execute signed releases, as necessary, authorizing custodians of police, credit, education, employment, and medical and similar records to provide relevant record information to the NBIB.

15. Prioritizing Investigation Requests

a. The DCSA is the ISP for all DoD BIs. DCSA offers fee for service products with additional costs for priority processing. The DON centrally funds the PSP, and has allocated resources for the following:

(1) Standard Service T5 for critical sensitive positions, TS security clearance, and SCI access determinations. Use service code “70.”

(2) Standard Service T5R for reinvestigating personnel in critical sensitive positions, requiring TS security clearance eligibility and SCI access. Use service code “71.”

(3) Standard Service T3/T3R for initial Secret and Confidential security clearance, military accessions and for reinvestigation of all personnel with Secret and Confidential security clearance. Use service code “64” and reinvestigation code “65.”

(4) Standard Service T3/T3R for civilians assigned to non-critical sensitive positions and for initial Secret and Confidential security clearance determinations. Use service code “64” and reinvestigation code “65.”

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

c. If a mission critical requirement exists for other than standard service, DUSN (S&I) can negotiate priority processing for requests with DCSA.

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

(2) Navy commands may request priority processing authorization via their Echelon I or II ASM, contact DUSN (S&I) at donsecurity_pers.fct@navy.mil for review and approval. You must cite the policy requirement that prevents use of interim access or assignment to perform assigned duties and necessitates priority service expenditures. Requests for priority processing of Marine Corps investigations will be submitted via HQMC PP&O/PS at (703) 614-2320 or DSN 224-2320 and forwarded to DUSN (S&I) for review and approval at the above e-mail address.

16. Maintaining Questionnaire Information

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

b. Requesting an individual to prepare a questionnaire for BI purposes using either electronic questionnaires or paper forms constitutes solicitation of personal information that is

protected by reference (u). COs have a responsibility to ensure that the information provided by the individual receives the appropriate protection.

c. If an individual refuses to provide or permit access to relevant information for investigation purposes, after being advised of the effect of refusal, commands will terminate the BI request process and notify the DCSA or the DoD CAF via JPAS or successor system. The individual will not be eligible for access to classified information or assignment to sensitive duties unless the information is made available. Personnel indoctrinated for SCI access will be debriefed for cause.

17. Follow-Up Actions on Investigative Requests

a. Rejection of Investigation Requests. When an investigation request is rejected by DCSA because the request was not properly prepared, commands must take immediate corrective action and resubmit the request. All forms being resubmitted and the tickler copy of the request form will be annotated with the resubmission date. If a military subject has been transferred, the rejected BI request must be forwarded immediately to the gaining command for correction and resubmission.

b. Request Follow-up. Commands are required to monitor requested investigations to ensure they are initiated, completed, and adjudicated as required. JPAS or its successor provides the status of investigations and should be consulted within 30 days of submission of request to ensure the request is initiated and opened by the ISP. If JPAS or its successor reflects the investigation is still pending, query DCSA for status. If JPAS or its successor reflects the investigation closed within the last three months and the adjudication decision has not been received, a query to the DoD CAF is appropriate.

c. Cancellation of Investigation Requests. When an investigation is in a pending status and the subject is being released from active duty, discharged, is resigning, or circumstances permanently change to negate the need for the investigation, the command will notify the DoD CAF immediately. The DoD CAF will direct DCSA, as appropriate, to cancel the investigation.

18. Processing Completed Reports of Investigation

a. All BIs requested to support eligibility determinations on DON employees are forwarded to the DoD CAF, when completed, for adjudication. The DoD CAF will make the required eligibility determination based on the requirements identified on the BI request.

(1) When the BI contains information that requires expansion, adjudication of the BI will be held in abeyance pending completion of the additional investigative leads. Interim access may not continue in these situations.

(2) Initial investigations on civilians or non-DoD personnel supporting unclassified contracts that uncover suitability issues are forwarded to the HRO for civilian employment and to the ASM on non-DoD personnel supporting unclassified contracts for the appropriate suitability determination. After the suitability determination is made, the completed Investigation (INV) Form 79A, Report of Agency Adjudicative Action on DCSA Personnel Investigations must be returned to the DCSA.

(3) The ASM will consult JPAS or successor system to determine when investigations are completed and when the DoD CAF adjudication is concluded. The ASM must ensure they have properly in-processed the person under their Security Management Office control in JPAS or successor system so they receive pertinent information and notices from the DoD CAF.

b. The DoD CAF adjudicates investigations requested to support trustworthiness determinations and non-sensitive position assignments that can be favorably adjudicated. The DoD CAF forwards unfavorable investigations to submitting office number for the appropriate trustworthiness and suitability determinations.

19. Safeguarding Reports of Investigation

a. In recognition of the sensitivity of personnel security reports and records, particularly with regard to personal privacy, results of investigations must be handled with the highest degree of discretion. Any investigative material,

favorable or unfavorable, must be handled, stored, and transmitted using the following safeguards:

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

(2) BIs will not be made available for, or communicated to, selecting officials. For any other uses, specific written approval must be obtained from DDI (I&S) via DUSN (S&I) from CNO or CMC.

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

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

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

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

(7) When being transmitted by mail, or carried by persons not authorized to receive these reports, reports of investigations must be sealed in double envelopes or covers. The inner container will bear a notation that it is to be opened only by an official designated to receive reports of BIs.

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

b. Results of DCSA investigations may not be released outside DoD without the specific approval of DCSA.

ADJUDICATION AND ELIGIBILITY DETERMINATIONS

1. Overview

a. PSIs 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 eligibility 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 to determine whether the employment of an individual can reasonably be expected to promote the efficiency of the service. The focus of a personnel security adjudication is whether the assignment or continued assignment in a sensitive position, or authorization for access to classified information, can reasonably be expected to be clearly consistent with the interest of national security.

d. Employment suitability adjudications are based on standards and criteria established by reference (q), and are normally made by the employing command. Personnel security determinations are based on criteria established by reference (b) are made by the DoD CAF, as provided in paragraph 6-1. Only U.S. citizens are eligible for security clearance and require eligibility to execute official U.S. government functions and duties (including employees of contractors under the NISP).

e. Use the following legend to complete the e-QIP Agency Use Block for proper routing of the SF 86 to the DoD CAF:

(1) DoD Suitability. Used by Human Resource professionals to submit civilians for suitability investigations.

(2) DoD Homeland Security Presidential Directive-12. Used by security professionals for contractors in support of unclassified contracts requiring physical and/or logical access.

(3) DON submission for National Security Positions. Used by security professionals for all civilian, military, and contractor personnel who occupy a National Security position or require access to classified information.

(4) ASM and Human Resource personnel are required to obtain access to DISS or successor system to communicate with the DoD CAF, to receive notifications of investigation status, submit customer service requests (CSRs) and to validate fingerprint results. Access to DISS or successor system is available by contacting the Echelon I, II, or HQMC PP&O/PS security offices. DISS CSRs and Preconditions Overview can be obtained on the DUSN (S&I) website at https://portal.secnav.navy.mil/Pages/default.aspx.

f. NBIB forwards all completed PSIs for DON personnel to the DoD CAF. The DCSA and the DoD CAF are delegated the authority in the DoD to make de facto security determinations on investigations closed without actionable issues on national security cases. In cases without issue, a favorable security determination equates to a favorable suitability determination. All other (non-sensitive) investigations on civilian personnel must be adjudicated by the HRO and the ASM for non-NISP contractors for suitability in accordance with reference (b). The following workflow procedures have been established to accomplish this requirement:

(1) When the INV Form 79A indicates "No Actionable Issue," the investigation will not normally be returned to the requesting command. A favorable security determination on a "No Actionable Issue" case will result in an automatic favorable suitability determination. The DoD CAF will favorably adjudicate the investigation, as appropriate, and enter the favorable determination in JPAS or successor system, thus notifying the command of the favorable determination. The DoD CAF will complete the INV Form 79A accordingly and forward it to OPM Federal Investigative Services Division (FISD).

(2) Investigations for non-sensitive or public trust positions will be forwarded to the command for the suitability determination. The INV Form 79A indicates "Actionable Issues," the completed investigation, with the OPM Certification of Investigation and INV Form 79A, will be forwarded to the requesting command for a suitability determination for civilian

employees to the HRO and the ASM for non-NISP contractor. If the requesting command makes a favorable suitability determination, it will be indicated in the applicable blocks on the INV Form 79A and will be returned to OPM to enter the results in the Clearance Verification System. The ASM or HRO as the Component Adjudicator will enter the results in the DISS. If the suitability determination made by the command is unfavorable, it remains a personnel action and no DoD CAF action is required.

g. Adjudicative determinations, whether favorable or unfavorable, interim or final, will be entered into the DISS on the same day the determination is made.

2. Security Adjudication Criteria

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

b. Because the same standards, criteria, and procedures are applied to both security clearance and sensitive position eligibility adjudications, a determination by the VROC or 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 VROC or 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. National security eligibility determinations are a function distinct from granting access to classified NSI.

c. 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.

d. BIs may be adjudicated by e-adjudication using DNI-approved business rules, by certified adjudicators who have successfully completed the standards for experience, training, and certification to perform final adjudicative determinations, or by non-certified adjudicators operating under an approved risk management plan in accordance with reference (b).

e. All military positions are national security positions regardless whether or not the Service Member requires access to classified information and;

(1) All military members will undergo PRs, maintain a favorable eligibility, and be subject to continuous evaluation.

(2) All military members will undergo the T3 investigation at a minimum. The DoD CAF will adjudicate all military investigations and reinvestigations using the national security adjudicative guidelines.

(3) Military members who are denied or revoked a favorable national security eligibility determination will be afforded due process. Those individuals will be immediately referred to the servicing Military Department for appropriate action.

(4) Military members who are determined to be ineligible for access to classified material solely because of citizenship will be entered into JPAS as not eligible for access to classified material.

f. With the exception of military personnel, minors who are under the age of 18 will not be investigated nor granted national security eligibility.

g. All reliable information relevant to determining whether a person meets the national security eligibility standards is reviewed and evaluated by appropriately trained adjudicative personnel, in accordance with appropriate procedures approved by the Security Executive Agent. Final adjudication determinations

will be made by certified adjudicators, non-certified adjudicators operating under an approved risk management plan, or in accordance with approved automated procedures.

h. The prohibitions on security clearance eligibility imposed by the “Bond Amendment” and explained in paragraph 8-3 will likewise be considered to prohibit assignment to sensitive, SAPs, Restricted Data (RD), or SCI national security positions in accordance with Section 3343 of reference (u).

i. Emergency Appointments. In cases where a command must hire an individual prior to completion of an investigation for suitability or security determination, emergency appointment procedures contained in Section 5 apply.

3. Eligibility Determinations

a. No individual will be given access to classified information or assignment to sensitive duties unless a favorable personnel security determination has been made regarding his/her loyalty, reliability, and trustworthiness are such that entrusting them with access to classified information or assignment to a sensitive position is clearly consistent with the interests of national security. A PSI is conducted, as detailed in Section 5, to gather information pertinent to these determinations.

b. In 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 an overall common sense "whole person" adjudication, reached by application of the evaluation criteria in reference (b). The criteria are based on reference (b) requirements and applies to all U.S. government civilian and military personnel, consultants, contractors, and other individuals who require access to classified information or assignment to sensitive duties.

d. The DoD CAF establishes eligibility for all DON affiliated civilian and military personnel, after adjudication

of the prerequisite security investigation. The DoD CAF reestablishes eligibility after adjudication of each subsequent investigation. In the interest of efficiency, the DoD CAF establishes eligibility at the highest level supportable by the prerequisite security investigation.

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

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

g. When national security eligibility has been issued by another Federal agency, the security manager will submit a customer service request to the DoD CAF for re-certification of eligibility: the investigative agency, case number, date of investigation, and any other relevant information, so that DoD CAF may review and/or reissue national security eligibility, as applicable.

h. 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.

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

4. Security Clearance and Sensitive Duty Assignment

a. In making eligibility determinations, the DoD CAF apply the personnel security eligibility adjudication standard consistently to both sensitive national security position determinations and security clearance eligibility determinations. These determinations cannot be made exclusive

of each other. A determination that an individual is not eligible for assignment to a sensitive national security position will also result in the removal of eligibility for security clearance. Likewise, a determination that an individual is not eligible for a security clearance will result in the denial of eligibility for assignment to a sensitive national security position.

b. Security clearance eligibility is not de facto authorization for an individual to access classified information. Authorization to access classified information is a separate command level determination dependent on whether an individual who has the requisite eligibility also has a need for access to classified information in the performance of official duties.

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

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

(1) The term “security clearance eligibility” has replaced “security clearance,” when referring to a formal determination made by an authorized adjudicative entity that an individual meets national security standards. Security clearance eligibility is officially recorded and subject to due process procedures. Security clearance now refers to a state that exists whenever eligibility has been properly established by an authorized adjudicative entity and access has been properly authorized by the command. Security clearance is understood to exist at the level of access authorized.

(2) When a command authorizes access to classified information pending completion and formal adjudication of the required PSI, this action was termed “interim clearance” in the past. However, reference (b) standards more accurately refer to this action as “temporary access” because it is an access determination under command purview. It is not a clearance

determination and it carries no due process benefits. Detailed guidance for temporary access is provided in paragraph 9-4.

5. DoD CAF Determination Process

a. To ensure uniform application of the national security standards, the DoD CAF is the DoD authority for granting personnel security adjudication.

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

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

d. 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 by applying the adjudication criteria provided in reference (b).

e. 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.

(1) BIs are reviewed to ensure compliance with reference (b) standards. Investigations that do not meet reference (b) standards are returned to OPM for correction.

(2) If investigative limitations preclude compliance with reference (b) standards, the DoD CAF may permit adjudication of the deviant investigation at its discretion and considering the needs of the DON, provided the investigative coverage is substantially sufficient to support the adjudication.

(a) Whenever an eligibility determination is based on an investigation that does not meet reference (b) standards, the deviation of standards will be recorded in JPAS or successor system.

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

f. Although it is intended to rarely occur, considering the needs of the service, the DoD CAF may permit an affirmative eligibility determination when disqualifying issues have not been fully mitigated. There are two circumstances in which this exception to reference (b) adjudication criteria could occur, and both must be recorded in JPAS or successor system.

(1) Conditional exception. Eligibility may be authorized or continued by DoD CAF when disqualifying issues are present, with the provision that one or more additional compensatory measures be fulfilled. These measures or "conditions" will be fully defined to the individual concerned and the employing command, with the understanding that failure to fulfill the conditions will result in revocation of national security eligibility. Conditional eligibility determinations are usually reserved for situations in which the employee has exceptional skill or merit or has made exceptional contribution to the DON mission, and the employing activity is willing to provide the necessary resources to manage the defined risk and conditions. The security manager will monitor the individuals granted eligibility on conditions and report results to the DoD CAF semi-annually until the conditions are removed.

(2) Waiver exception. SCI access eligibility may be established or continued despite the presence of substantial issue information that would normally preclude access, such as the existence of foreign national family members. The waiver typically involves one specific disqualifying factor, which is waived due to meritorious circumstances. Reference (b) provides

guidance on SCI access eligibility standards and waivers. The DoD CAF records “Bond Amendment” waivers in JPAS or successor system.

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

h. All DoD CAF eligibility determinations are recorded in the JPAS or successor system on a daily basis.

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

6. Requesting Eligibility Determinations

a. A personnel security eligibility determination is required when an individual is initially nominated to perform sensitive national security duties or for access to classified information; a PSI is completed on an individual who occupies a sensitive position or has access to classified information; unfavorable information becomes available about an individual who occupies a sensitive position or has access to classified information; or the issues that prompted a previous unfavorable personnel security eligibility determination no longer exist and the command again requires the individual to perform sensitive duties or to have access to classified information.

b. When it is determined that an individual will require access to classified information to perform assigned duties, commands will consult JPAS to determine if the necessary security clearance eligibility was previously established. If it appears that the prerequisite investigation was completed but not properly adjudicated, or if eligibility was established by an adjudicative entity other than DoD CAF, the command will use

the CSR in DISS or successor system to request the DoD CAF reciprocally establish the required eligibility.

c. When the individual indicates that eligibility was established by a non-DoD entity, that eligibility determination may not be visible in JPAS or its successor. The command will gather details concerning the eligibility and investigation, and using DISS will request that DoD CAF "reciprocally" establish the required eligibility. Paragraph 7-7 provides details on reciprocal acceptance of eligibility determinations. The DoD CAF will either verify eligibility and reciprocally re-establish eligibility, or will direct the command to request the necessary PSI, as appropriate.

d. When it is determined that the individual does not have the investigation or eligibility required, the command will submit the appropriate request for investigation. Upon completion, the investigation will be forwarded to the DoD CAF where the required eligibility determination will be made and recorded in JPAS. Commands need NOT submit a separate eligibility request to the DoD CAF. The DoD CAF acts on the eligibility requirements recorded on the PSI request. For detailed instruction on the proper preparation of investigation request forms see the DUSN (S&I) website at https://portal.secnav.navy.mil/orgs/DUSNP/Security-Directorate/Personnel-Security/SitePages/Home.aspx/. Temporary access (interim clearance) procedures may be employed as necessary; refer to reference (b) for details.

e. Upon receipt of derogatory information, COs will determine whether, on the basis of all the facts, to suspend or limit an individual's access to classified information, or reassign the individual to non-sensitive duties pending a final eligibility determination by the DoD CAF. Paragraph 9-17 provides guidance on suspending access for cause. Regardless of the local access determination, commands must report all information, per Section 10 and reference (b), to the DoD CAF via the JPAS (or successor system) incident report function, and use other available means to forward relevant supporting documentation. The DoD CAF adjudicates the information and may validate continued eligibility, request more information, further investigation, or begin the unfavorable determinations process.

7. Reciprocal Acceptance of Eligibility Determinations

a. A personnel security eligibility determination by the DoD CAF, or another federal government agency, will not be duplicated when those investigations meet the scope and standards for the level of national security eligibility required. A previously granted national security eligibility or access may be re-certified in the DISS or successor system by the DoD CAF if:

(1) There is no break in continuous service greater than 24 months.

(2) Investigative basis is adequate for the eligibility to be established, and no new derogatory information is identified. Eligibility will be verified by the DoD CAF, without additional adjudication.

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

(4) Derogatory information includes any un-adjudicated information as outlined in reference (b).

b. Whenever security clearance eligibility has been established, the DoD CAF will not request prior investigative files for review unless:

(1) Potentially disqualifying information is developed since the last favorable adjudication.

(2) The individual is being considered for a higher level security clearance eligibility.

(3) The most recent eligibility determination was conditional or based on a waiver or deviation.

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

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

8. Eligibility Prohibitions

a. Only U.S. citizens who are employees of the executive branch of the U.S. Government (including employees of contractors under the NISP) are eligible for security clearance or assignment to sensitive duties.

(1) Occasionally, it is necessary for the DON to authorize access or assignment for persons not meeting these requirements, per reference (b).

(2) When this regulation refers to U.S. citizens, it makes no distinction between those who are U.S. citizens by birth, those who are U.S. nationals, and those who have derived U.S. citizenship or those who acquired it through naturalization.

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

b. Eligibility will not be established for persons who are not in a position which requires eligibility including persons in non-sensitive or public trust civilian positions; persons (such as guards and emergency service personnel) who may only have inadvertent access to sensitive information or areas; persons (such as maintenance, food services, or cleaning personnel) who perform non-sensitive, unclassified duties in areas where classified information can be reasonably prevented;

or persons (such as vendors and other commercial sales or service personnel) who do not require access to classified information and whose access to classified information can be prevented by a cleared escort. Reference (p) guidance is used for trustworthiness determinations for contractor personnel with no access to classified information.

c. Eligibility will not be established for identified persons commonly referred to as the “Bond Amendment,”. This mandate was enacted to preclude the initial granting or renewal of security clearance eligibility by the DoD under specific circumstances. The DoD CAF will determine applicability of Bond Amendment after adjudication of the prerequisite PSI. Bond Amendment waiver provisions and details are provided in reference (b).

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

e. Members of the U.S. Supreme Court, the Federal judiciary, and the Supreme Courts of the individual states are not processed for security clearance eligibility. They may be granted access to classified information to the extent necessary to adjudicate assigned cases. For SCI, access may be granted upon concurrence from Fleet Cyber or SSO Navy in accordance with reference (k). Section 9 provides access procedures.

9. Unique Eligibility Requirements

a. CO Clearance. Every CO must have a favorably adjudicated T5 or T5R and eligibility determination that is at least equivalent to the highest level of classified information maintained at the command.

(1) The incumbent CO will review the records of the prospective CO to ensure that the individual has the necessary investigation and clearance eligibility determination to assume command. In the absence of an incumbent CO, the next senior in the chain of command will ensure the records are reviewed.

(2) When the prospective CO does not have an adjudicated SSBI/SSBI-PR/PPR/T5 or T5R completed within the past five years, the incumbent CO will ensure that the required T5 or T5R request is submitted.

b. Cryptographic Duties. Commands cannot grant interim access for cryptographic duties. The DoD CAF must establish clearance eligibility before access is allowed to U.S. cryptographic information.

c. Reserve Personnel. Navy and Marine Corps reserve personnel in an "active status" are considered to have continuous service and may be granted access as necessary, when supported by the commensurate DoD CAF security clearance eligibility.

d. IRR. IRR members will have security clearance eligibility established by the DoD CAF as necessary. All due process procedures will be afforded IRR members nominated for security clearance. The ASM must maintain an owning or servicing relationship in JPAS or successor system.

e. Rating/Military Operations Specialty Requirements. To maintain mobility and operational readiness, the NAVPERSCOM (PERS-483) or CMC HQMC must ensure individuals have security clearance eligibility established by the DoD CAF to support potential subsequent assignments. The ASM must maintain an owning or servicing relationship in JPAS or successor system.

(1) Commands will use the continuous evaluation and vetting processes to maintain security clearance eligibility for military members. All military members will undergo PRs, maintain a favorable adjudication and eligibility, and be subject to continuous evaluation and continuous vetting procedures.

(2) Commands will forward credible derogatory information from any source including but not limited to, an incident report, continuous evaluation alert, or a BI to the DoD CAF for determination of continued eligibility for security clearance, as appropriate.

f. Personnel Assigned to Other Federal Agencies. The DoD CAF will establish and provide certification of security

clearance eligibility for DON employees assigned to other Federal agencies.

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

(1) For eligibility and access purposes, the consultant is managed by the contracting activity as an employee and the DoD CAF adjudicates eligibility.

(2) Consultants hired by (or under contract to) a DoD contractor to provide professional or technical assistance are considered employees of the contractor and are processed under the NISP if eligibility is required.

h. Members of congressional staffs may be processed for security clearance eligibility, as necessary, through the Security Division, Washington Headquarters Services in accordance with reference (b).

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

10. Eligibility Under the NISP

a. Employees of contractors granted facility clearances under the NISP may have personnel security clearance eligibility established when there is a bona fide requirement to access classified information in connection with performance on a classified contract or R&D program. Contractor personnel security investigations are conducted by DCSA and the results are forwarded to the VROC, the DoD adjudicative facility responsible for establishing security clearance eligibility for DoD contractors.

b. Employees of contractors requiring access to DON SCI are adjudicated for SCI access eligibility by the VROC or the DoD CAF.

c. Access to Secret or Confidential classified information may be permitted for eligible contractor employees by the VROC on a temporary basis, pending completion of the appropriate BI.

d. Access to TS classified information may be permitted for eligible contractor employees by the VROC on a temporary basis, pending completion of the appropriate BI. DON contracting commands in receipt of requests for interim TS access will validate the contract, the contractor's need-to-know, and the necessity for the interim access.

e. COs will report to the VROC, via JPAS or successor system, any adverse or questionable information that comes to their attention concerning a cleared contractor employee assigned to a worksite under their control. An information copy of the report will also be forwarded to the Cognizant Security Office identified on the DD Form 254. COs will also report adverse or questionable information to the VROC or DoD CAF when a cleared contractor employee has SCI access, or is a consultant whose clearance eligibility has been established by the VROC or DoD CAF.

f. Commands are responsible for ensuring all clearance eligibility and access requirements are identified on the DD 254. Command procedures for granting or denying access to classified information for cleared contractor personnel are provided in paragraph 8-12.

UNFAVORABLE ELIGIBILITY DETERMINATIONS AND RESTRICTIONS

1. Overview

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/her loyalty, reliability, and trustworthiness. A PSI is conducted, as detailed in Section 5, to gather information pertinent to these determinations.

b. The eligibility determination is the result of overall common sense "whole person" adjudication, reached by application of the evaluation criteria in reference (b). The criteria apply to all U.S. government civilian and military personnel, consultants, contractors, and other individuals who require access to classified information or assignment to sensitive duties.

c. Eligibility determinations are restricted to U.S. citizens determined to require eligibility to execute official U.S. government functions and duties (including employees of contractors under the NISP). Eligibility will not be established for individuals pursuant to the “Bond Amendment” identified in reference (b).

d. 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.

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

f. Commands are ultimately responsible for ensuring that the VROC and DoD CAF are apprised whenever credible derogatory information develops that suggests an individual may no longer be in compliance with personnel security standards. Commands will report the issues to the VROC or the DoD CAF for adjudication using JPAS or successor system within 72-hours and make a determination on whether the derogatory information warrants the suspension of access to classified information. (For SCI access, refer to reference (k) for reporting requirements.) Commands must implement a proactive continuous evaluation program as described in Section 11, per reference (b), to satisfy this requirement.

g. Regardless of an individual’s intent to appeal, once the VROC or the DoD CAF makes an unfavorable eligibility determination, the command must remove all accesses authorized and debrief the individual and remove civilian employees from designated sensitive positions in accordance with reference (b).

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

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

j. No separation under other than honorable conditions will be taken with respect to any Navy or Marine military member, nor will any action be taken to effect the separation, dismissal, discharge, or other involuntary separation for cause of any DON civilian employee or any contractor/consultant employee under the personnel security cognizance of the DON, in any case where the individual has held access to SCI and/or SAPs within 18

months prior to the proposed action, unless approval is first received from the program manager (i.e. the DNI for SCI access or CNO (N9SP) for SAPs).

2. Authorities and Responsibilities

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

(1) The DUSN will:

(a) Issue DON PSP policy.

(b) Assign responsibilities for overall management of the PSI program.

(c) Ensure timely due process is afforded in appeals of unfavorable DoD CAF personnel security determinations.

(2) The President, PSAB will:

(a) Preside over the PSAB, a three-member panel appointed by the Director of Review Boards, which reviews and provides final decisions on appeals of unfavorable DoD CAF determinations. The PSAB decision is final and concludes the administrative appeals process.

(b) Ensure the PSAB meets at least monthly and provides notice of the PSAB to sustain or reverse determinations made by the DoD CAF within 5 days of determination.

(3) CO’s will:

(a) Administratively withdraw access when the requirement for access to classified information no longer exists. Debrief the individual in accordance with Section 4, and notify the DoD CAF, via JPAS or successor system, that security clearance eligibility is no longer required.

(b) Continuously evaluate command personnel with

regard to their eligibility for access to classified information and/or assignment to a sensitive position, applying the criteria outlined in reference (b). Forward all potentially disqualifying information to DoD CAF via JPAS or its successor. The DoD CAF will review the information and reevaluate the individual's clearance eligibility using reference (r).

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

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

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

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

(g) Ensure final DoD CAF unfavorable personnel security eligibility determinations are immediately coordinated with supervisors, human resource specialists, and security personnel so that necessary actions are quickly taken to officially remove personnel accordingly from access to classified information and assignment to sensitive duties.

(h) Deny visitor access or restrict admittance to command areas, as deemed appropriate, when disqualifying information regarding an individual from another command is revealed. Ensure the individual's parent command, agency, or facility is notified of your action, to include the basis for that action. For contractor employees, report disqualifying

issues to both the Contractor's Facility Security Officer and to the VROC.

(4) The individual will:

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

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

b. To be accurate and efficient, the unfavorable determination process relies on a full and frank exchange of pertinent information and timely action by all responsible parties; timely adjudicative action at DoD CAF, timely and thorough response from individual as facilitated by command security officials, and prompt appeal consideration at PSAB.

3. Restrictions on the Granting or Renewal of Security Clearances

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

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

c. The SECNAV may not renew security clearances, absent a waiver, grant or renew security clearances that provide access to SAPs, SCI, or RD in accordance with reference (k).

4. Unfavorable Determinations Process

a. Commands will forward credible derogatory information from any source including but not limited to, an incident

report, continuous evaluation alert or a BI to the DoD CAF for determination of continued eligibility for security clearance, as appropriate. The DoD CAF will determine if the information is within the scope of the national security eligibility adjudicative guidelines, per reference (b). If a denial or revocation of national security eligibility is considered appropriate, the DoD CAF will issue to the individual concerned via JPAS or successor system a LOI and enclosed Statement of Reason (SOR) through the security manager to the individual to revoke or deny security clearance eligibility, SCI access, or sensitive position eligibility. The LOI and SOR will be as comprehensive and detailed as the protection of sources afforded confidentiality under the provisions of reference (u) and as national security permits and contain:

(1) A summary of the security concerns and supporting adverse information.

(2) Instructions for responding to the SOR.

(3) A copy of the relevant national security adjudicative guideline(s).

(4) A list and description of the information relied upon to render the proposed unfavorable national security eligibility determination.

(5) An explanation of each security concern, including the specific facts that triggered each security concern, the applicable adjudicative guideline(s) for each concern, and the disqualifying conditions and mitigating conditions for each adjudicative guideline cited.

b. The command will immediately present the LOI and SOR to the individual and assume a direct role in facilitating the process. The command will determine the individual's intent regarding a response in writing with an explanation, rebuttal, or mitigation for the derogatory information, and immediately complete and return the Acknowledgement of Receipt of the LOI via JPAS or successor system within 10 calendar days to the DoD CAF indicating whether the individual intends to submit a response to the contemplated action and whether the command has

granted an extension of time to submit the response. The LOI advises the individual that if they choose not to respond, absence an approved extension, or if the response is untimely, they will forfeit their right to appeal.

c. The command will notify the DoD CAF within 10 calendar days if they are unable to deliver the LOI or SOR to the individual. The notification will include information as to why the LOI or SOR could not be delivered (e.g., illness or death in the family or deployment) and when it is expected the individual can receive a copy of the LOI and SOR. The ASM must deliver the LOI and SOR immediately upon the individual’s return.

d. Acknowledgement of receipt of the LOI through JPAS or successor system to the DoD CAF and indicate the individual's intentions.

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

f. The command will review the information contained in the LOI and SOR to determine if it is in the best interest of national security to take interim action to suspend the individual's access to classified information or suspension of assignment to sensitive duties (or other duties requiring a trustworthiness determination) should be suspended while the unfavorable determination process continues. Individuals with interim or temporary access will have their access removed immediately. An incident report will not be submitted on the same information that is included in the LOI and SOR. The Commander’s decision(s) on access will be documented, signed, and a copy maintained by the security manager until the final adjudication. If access is suspended:

(1) It will be formally suspended in JPAS or successor system. Informal suspension (removal of access) is not authorized when an LOI or SOR is issued.

(2) The individual will be debriefed from access to classified information.

(3) The individual will sign a receipt, acknowledging receipt of the access suspension notification.

g. The ASM will serve as the liaison between the DoD CAF and the individual. The ASM will:

(1) Deliver the LOI and SOR and have the individual acknowledge receipt of the LOI and SOR. The ASM and a witness will document the delivery if the individual refuses acknowledgement.

(2) Obtain an acknowledgement receipt with the individual's intention to respond within the time specified and submit the receipt to the DoD CAF in JPAS or successor system within 10 calendar days.

(3) Explain the consequences of the proposed action and the need to respond in a timely fashion.

(4) Explain how to request extensions.

(5) Explain how to obtain copies of investigative records.

(6) Explain the procedures for responding to the LOI and SOR.

(7) Explain the individual's entitlement to obtain legal counsel or other assistance at their own expense within the relevant time periods.

h. When a security office receives a LOI and SOR, or a LOD and/or Letter of Revocation concerning an individual who is no longer assigned to the command, the LOI and SOR or the LOD or revocation will be returned to the DoD CAF with a statement indicating the individual's status. If the individual has been discharged from military service with no reserve obligation, is incarcerated, or is dropped from the rolls as a deserter, return the LOI and SOR or the LOD or revocation and upload the discharge orders or supporting documentation to the DoD CAF via JPAS or successor system.

i. The LOI or SOR response by the command and the individual:

(1) The commander and/or security manager will ensure that the individual acknowledges receipt of the LOI and SOR by signing and dating the response form enclosed in the LOI and SOR. The recipient of the LOI will indicate his or her intention of submitting a rebuttal or response to a LOI and SOR within 10 calendar days of receipt of the LOI and SOR. The receipt will be uploaded to the DoD CAF via JPAS or successor system and;

(a) Will not deny or revoke an individual’s national security eligibility without official documentation that the individual received the LOI and SOR. All LOIs and SORs will have a returned receipt submitted to the DoD CAF.

(b) If the individual refuses to sign the receipt, the refusal will be documented and signed by the commander or supervisor and returned to the DoD CAF.

(2) The individual’s reply to the LOI and SOR must be submitted no later than 30 calendar days from receipt of the LOI and SOR to prepare and submit a written response. No outside influence will be permitted to forfeit the individual's opportunity to reply. The commander has the authority to grant the recipient of the LOI up to 30 extension days (for a total of 60 days) for the preparation of a response, provided the DoD CAF is notified of the extension time granted. After the initial 30-day extension, requests for extensions must be directed to the DoD CAF with a valid justification.

(3) The commander and/or ASM will ensure that the individual is counseled as to the seriousness of the DoD CAF contemplated action and will offer advice and assistance needed in forming a reply. The person can obtain legal counsel or other assistance at his or her own expense, and may request a copy of the investigative files under the provisions of reference (u). If other than DON investigative records repository files exist, the Freedom of Information Act Office and/or Privacy Office will refer the request to the appropriate repository.

(4) The individual's written response should address each issue raised in the LOI and SOR. Failing to address each issue may result in the DoD CAF rendering an unfavorable determination. Any pertinent written documentation must be labeled in a manner to ensure it is properly associated with the issue(s) raised in the LOI and/or SOR. Letters of recommendation from commanders and/or supervisory personnel must be attached to the response. The individual will forward the response through the ASM to the DoD CAF.

(5) If an individual decides not to respond to the LOI and SOR after initially indicating an intent to respond, the ASM will upload a signed document from the individual, documenting the decision not to respond, prior to the 30-day suspense.

(6) The DoD CAF final decision will be forwarded through the servicing ASM to the individual.

j. The command must respond within 10 calendar days after delivery of the LOI to the recipient by forwarding the completed Acknowledgement of Receipt of the LOI to the DoD CAF via JPAS or successor system. Absent command or individual notification of intentions, the DoD CAF may issue a final determination after 90 calendar days from the date on the LOI based upon existing information.

k. The DoD CAF will adjudicate the response to the LOI within 90 calendar days of receipt and will either make a favorable determination and authorize eligibility or issue a LOD of the unfavorable determination.

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

m. If an unfavorable national security eligibility determination is received:

(1) The DoD CAF will provide a LOD or Letter to Revoke (LOR) in response to the individual’s written response to the LOI and SOR if the conditions presented were not favorably adjudicated. The LOD or LOR must provide the individual with a comprehensive and detailed written explanation of each security

concern, the applicable adjudicative guideline(s) related to each concern, and an explanation of the types of mitigating information they could provide to support their appeal.

(2) The LOD or LOR will inform the individual of their right to appeal the DoD CAF unfavorable national security determination. The letter will inform the individual of their right to:

(a) Be represented by counsel or other representative at their own expense.

(b) Request the documents, records and reports upon which the unfavorable national security determination was made.

(3) The individual must acknowledge the receipt of the LOD or LOR and indicate in writing if they will submit an appeal within 10 calendar days. If the individual refuses to acknowledge receipt or indicate whether an appeal will be submitted, the refusal will be documented and signed by the commander or supervisor and returned to the DoD CAF.

(4) The ASM will notify the DoD CAF within 10 calendar days if they are unable to deliver the LOD or LOR to the individual. The notification will include information as to why the LOD or LOR could not be delivered (e.g., illness or death in the family, deployment) and when it is expected that the individual can receive a copy of the LOD. The ASM must deliver the LOD immediately upon the individual’s return.

(5) Upon receipt of an LOD or LOR, the ASM will debrief the individual from access to classified information.

5. Appeals Process

a. The PSAB is the final appellate authority for unfavorable personnel security determinations made by the DoD CAF. If an individual chooses to appeal an unfavorable DoD CAF determination, the appeal may be made by personal appearance or in writing as follows:

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

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

b. Individuals may not choose both options. Having or not having a personal appearance will not bias the PSAB in making a fair determination.

c. DOHA Personal Appearances

(1) Individuals desiring to present a personal appeal must request a DOHA hearing within 10 days of receipt of the LOD or LOR.

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

(3) Individuals will be provided a notice designating time, date, and place for the personal appearance. For individuals at duty stations within the contiguous 48 states, the personal appearance will be conducted at the individual's duty station, a nearby suitable location, or by video-teleconference. For individuals assigned to duty stations outside the contiguous 48 states, the site of the personal appearance will be determined by the Director, DOHA or designee at (1) the individual's duty station; (2) a suitable location near the individual's duty station; or (3) at DOHA facilities located either in the Washington D.C. metropolitan area or the Los Angeles, California metropolitan area.

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

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

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

(7) Individuals who choose a personal appearance will have the opportunity to present, cross-examine witnesses, or obtain comments in writing for submission to the AJ at the proceeding. Individuals who desire to present the view of others must do so in writing (e.g., letters of reference, letters from medical authorities, etc.). The appeal should address the disqualifying issues identified by the LOD or LOR and should present any existing mitigation as defined in reference (b), to include pertinent supporting documentation.

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

(9) The value of a command perspective on the PSAB deliberations cannot be overstated. Since appeals presented to DOHA do not have the benefit of a command endorsement, commands are strongly encouraged to submit a position paper directly to the PSAB. However, due to time constraints, the PSAB will only solicit a command position when the DOHA personal appearance presents substantial information not included in the individual's rebuttal to the LOD or LOR. When this happens, a PSAB representative will contact the command to request the new information. The command will have 10 days to respond and will afford the individual the opportunity to review the information prior to submission to the PSAB.

d. PSAB Written Appeal Submissions

(1) Within 10 calendar days of receipt of the LOD or LOR, the individual will sign and return the notice of intent to appeal to the adjudication facility via their security office. The individual has 30 days from receipt of the LOD or LOR to submit a written appeal to the PSAB. The PSAB President or designee may grant a 30 calendar day extension of time for good cause demonstrated by the appellants (e.g., illness, death in the family or deployment).

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

(3) Written appeals should address the disqualifying issues identified by the LOD or LOR, and should present any existing mitigation as defined in reference (b), to include pertinent supporting documentation.

(4) Commands will provide a command perspective by submitting an endorsement to the individual's written appeal and will afford the individual the opportunity to review the written endorsement prior to the final submission to the PSAB.

e. PSAB Procedures

(1) The PSAB will review the DoD CAF case file, the individual's appeal (to include DOHA recommendations and command submissions as provided), and any supporting documentation submitted by the individual.

(2) If the PSAB agrees with the DOHA recommendation, the PSAB may adopt the DOHA recommendation in lieu of providing a PSAB written determination.

(3) The PSAB normally renders decisions within 45 days of receipt of the individual's appeal from the DoD CAF or 30 days from receipt of the DOHA recommendation.

(4) The PSAB may also request additional information or determine that information not contained in the adjudicative record or the appeal material is needed to render a final determination (e.g., updated credit bureau report, information from the command) the new information must be provided to the individual. The individual must be provided a reasonable period

of time to offer any rebuttal to this information, prior to it being considered by the PSAB.

(5) Personal appearances before the PSAB are prohibited; however the PSAB may request additional information from the appellant through the command.

(6) The PSAB will meet at least monthly, and within 10 days of the Board decision, will upload the decisions via JPAS or successor system, and notify the individual, via the individual's command, of the PSAB determination.

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

(1) The PSAB will direct the DoD CAF to grant or restore eligibility when the PSAB finds for the appellant. The PSAB's written decision will identify each adjudicative guideline issue stated in the LOD or LOR that formed the basis of the denial or revocation that remains unmitigated after the appeal and the rationale for the final disposition of the appeal. The DoD CAF will adjust the JPAS or successor system record to re-establish eligibility within two days of receipt of the PSAB determination letter.

(2) When the PSAB finds against the appellant, reconsideration is only possible, if at a later date (at least one year from the date of the final PSAB denial or revocation decision) the individual's command determines that a valid requirement for access to classified information exists and the issues which caused the unfavorable determination seem to have been mitigated either through the passage of time or other relevant positive developments. Paragraph 7-6 explains the reconsideration process. A copy of the PSAB determination letter will be provided to the DoD CAF for inclusion in the adjudicative record.

6. Reestablishing Eligibility After A Denial or Revocation. Following an unfavorable security determination, a request to reestablish eligibility normally a minimum of 12 months after the concluding unfavorable determination either by PSAB if appeal rights were exercised or by the DoD CAF if appeal rights were NOT exercised, and;

a. A commander may request reconsideration of unfavorable national security determinations for individuals within their command one year after the denial or revocation. The year is counted from the date of the denial or revocation decision by the DoD CAF; or, if the individual elected to appeal, one year from the date of the PSAB determination.

b. Individuals who terminate their affiliation with the federal government (including federal contract employment) for 24 months or more after an unfavorable national security determination are not subject to the reconsideration process. When attempting to re-affiliate with the DON these individuals will be submitted for a new BI.

c. Reconsideration will not be requested solely based on an individual’s personal desire to acquire eligibility. Reconsideration is not a personal right or entitlement. The individual must be in a position or have a duty assignment that requires national security eligibility.

d. If a denial or revocation is based on significant derogatory information that has been reported to a CI or law enforcement authority, the DoD CAF should consult with these authorities to ensure it has all relevant information before reviewing a reconsideration request.

e. The following should be met before a request for reconsideration is submitted:

(1) The individual's commander must determine that the issues which caused the unfavorable determination are mitigated as outlined in reference (b), either through the passage of time or other relevant positive developments.

(2) The command has a current mission critical requirement, including tentative selection to a federal position, for the individual to have access to classified information or to hold a sensitive position.

(3) Reconsideration requests are formally submitted from the commander or designee of the employing activity to the DoD CAF. Reconsideration requests must be fully detailed and justified, providing all relevant documentation that the

circumstances or conditions that resulted in the final adverse eligibility determination have been rectified or sufficiently mitigated to warrant reconsideration. The documentation required depends on the reason(s) for the denial or revocation, such as, a current evaluation for behavioral (psychological) health issues, an evaluation for drug or alcohol abuse, or current financial statements.

(4) Individuals whose current eligibility is either denied or revoked or who are pending reconsideration are not authorized temporary/interim access and/or temporary assignment to national security or sensitive positions.

(5) Any request for reconsideration submitted to the DoD CAF in accordance with the above provisions must outline the reasons for the denial or revocation and provide a rationale for favorable action. The request for reconsideration must be endorsed by the individual's commander or delegated representative. Commanders may delegate this responsibility to managers who are responsible for the supervision of the individual. The commander should be familiar with the information available to the decision authority and with the DoD CAF and/or PSAB’s rationale for denying the appeal. If the individual does not have a copy of the DoD CAF or PSAB’s original decision, as applicable, the commander should request a copy of the record.

(6) Once security offices submit their DoD Components request for re-consideration, no supplemental information will be accepted or considered unless requested by the DoD CAF. Should the DoD CAF request additional information, the Command must submit the documentation within the given timeframes.

f. The DoD CAF has the authority to grant or deny the reconsideration based on a review of the submitted documentation to determine the extent to which circumstances or conditions have been rectified or sufficiently mitigated.

(1) DoD CAF will assess the request and reestablish eligibility, if warranted.

(2) If a favorable determination is not possible, the DoD CAF will provide notification through the command to the DoD Component in writing, generally within 30 days from receipt of request for reconsideration.

(3) The individual will not be eligible for reconsideration for at least one year from the DoD CAF reconsideration decision.

(4) No due process is afforded for denial of a request for reconsideration.

ACCESS TO CLASSIFIED INFORMATION

1. Overview

a. The CO's responsibility for his or her command is absolute. The authority of the CO is commensurate with his or her responsibility. COs have ultimate responsibility and authority for all determinations regarding persons who may have access to classified information under their control.

b. COs will determine those position functions under their control that require access to classified information, and may authorize access to the incumbents of such positions who have officially been determined to be eligible by the appropriate adjudicative authority.

c. COs may grant access to classified information to any individual who has an official need-to-know, established security clearance eligibility, and about whom there is no known un-adjudicated disqualifying information.

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

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

f. Access to classified information will be limited to the extent possible, to the minimum number of persons necessary to accomplish the mission, and will be based on need-to-know. Additionally, the level of the classification and the amount of information authorized for access will be limited to the minimum level and amount required to perform assigned duties.

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

h. All individuals will complete a SF 312 prior to being granted initial access to classified information and recorded in JPAS or successor system.

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

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

(2) 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.

j. JPAS is the system of record for all DoD access determinations. COs will ensure that all access authorizations for individuals under their control are properly and promptly recorded in JPAS or successor system.

2. Need-to-Know

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

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

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

(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) The authorized holder must determine that the

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

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

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

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

(2) Although access can only be authorized for individuals with established security clearance eligibility at or above the level of classified information required, having security clearance eligibility does not equate to need-to-know.

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

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

3. Classified Information Nondisclosure Agreement (SF 312)

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

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

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

b. The SF 312 is available through the government supply system and must be used.

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

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

e. When there is no evidence that a DON military or civilian employee has previously signed an SF 312, the current SF 312 must be signed before access to classified information is authorized. Personnel who have signed other nondisclosure agreements for specific access, (such as SF Form 1847-1, SCI Non-Disclosure Agreement), must also execute the SF 312.

f. If an individual refuses to sign an SF 312, the command will deny the individual access to classified information and report the refusal to the DoD CAF via the JPAS or successor system "Report Incident" link.

g. COs will ensure personnel are provided explanation of the purpose of the SF 312 and have the opportunity to read the

Sections of Titles 18 and 50 of the U.S. Code and other references identified on the SF 312.

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

i. Executed SF 312s will be maintained in personnel files for 70 years from date of signature. Execution of the SF 312 will be recorded in JPAS or successor system.

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

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

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

All DON civilian personnel:
To their OPF

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

4. Interim Eligibility (or Temporary National Security Eligibility)

a. In the absence of adverse information, COs may grant interim eligibility (also referred to as temporary eligibility) to individuals pending completion of full investigative requirements and pending establishment of security eligibility by the DoD CAF. Adverse information is identified in reference (b).

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

(1) Interim eligibility may only be authorized by the CO or designee. The CO or designee must review the SF 86 to ensure no adverse information exists prior to granting an interim national security eligibility.

(2) Interim national security eligibility may be reciprocally accepted throughout the DoD and DON.

(3) An interim Secret or Confidential is valid for access to the level of eligibility granted. Access to RD, Communications Security (COMSEC) information, and NATO information is not authorized.

(4) An interim TS is valid for access to TS information. Access to RD, COMSEC, and NATO information at the Secret and Confidential level is authorized if the individual has final Secret national security eligibility.

(5) Interim SCI eligibility is granted by the DoD CAF.

(6) Interim national security eligibility for contractor personnel under the NISP is governed by VROC.

(7) Interim eligibility determinations and access are prohibited for NSA/CSS assignment, detail, or employment in accordance with reference (b).

(8) Interim eligibility will be valid for up to one year in addition to the following:

(a) A six-month extension may be made by the commander if the BI has not been completed, the adjudication is pending at the DoD CAF, and the individual still requires national security eligibility.

(b) The security manager will notify the DoD CAF of the extension via JPAS or successor system entry.

(c) Interim national security eligibility will be removed when credible derogatory information becomes known or if there is an incident report.

(d) The DoD CAF will update JPAS or successor system to reflect the withdrawal of interim eligibility after one year or after the expiration of an approved six-month extension.

(9) Interim national security eligibility will be documented in JPAS or successor system, whenever possible.

(10) The authority to request credit reports is limited to the ISP, the DoD CAF, and the PSAB. Financial concerns will be addressed through a review of the SF 86.

(11) In those instances where management has extended a tentative offer of employment to an individual who is deemed ineligible for interim national security eligibility, the BI may continue if management chooses to hold the final offer pending a final national security eligibility determination by the DoD CAF. The employee must be notified in writing by their employing activity that further access to classified information is expressly conditioned upon the completion of the BI and granting of national security eligibility.

(12) Prior to granting interim national security eligibility, one of the following documents must be used as acceptable proof of citizenship:

(a) A birth certificate certified with the registrar’s signature that bears the raised, impressed, or multicolored seal of the registrar’s office.

(b) A valid U.S. passport or passport card, unaltered, originally issued to the subject.

(c) A Department of State (DOS) Form FS-240, “Consular Report of Birth Abroad of a Citizen of the United States of America.”

(d) A DOS Form FS-545 or DS-1350, “Certification of Birth.”

(e) A U.S. Citizenship and Immigration Services (USCIS) Form N-560 or N-561, “Certificate of U.S. Citizenship.”

(f) A USCIS Form 550, “Certificate of Naturalization” or 570, “Replacement Certificate of Naturalization.” Copies can be made of naturalization papers for submission in accordance with reference (mm).

(13) Interim Confidential or Secret national security eligibility:

(a) When a valid need to access Secret information or occupation of a non-critical sensitive position is established, interim Secret national security eligibility may be issued. The interim will be recorded in the JPAS or successor system when the following criteria has been met:

1. Acceptable proof of citizenship.

2. Favorable review of a completed SF 86.

3. Favorable review of local personnel, base, military police, medical, and security records, as applicable.

4. An appropriate national security investigation opened by the ISP.

5. Favorable review of FBI Criminal History Report (fingerprint results).

(b) When a prior NACLC, ANACI, T3 or higher scope investigation exists that is less than five years old for Confidential or Secret but has not been adjudicated, interim national security eligibility is not required if:

1. There has not been a break in service greater than 24 months.

2. The required BI has been opened by the ISP.

3. A request is submitted to DoD CAF requesting a Secret national security eligibility be granted.

(14) Interim TS national security eligibility:

(a) When a valid need to access TS information is established, an interim TS national security eligibility may be issued.

(b) Favorable completion of all requirements cited for interim Secret or Confidential eligibility.

(c) Favorable review of an Advance NAC or favorable NAC results completed, which must be inclusive of a FBI fingerprint and name check.

(d) When a prior valid T5, SSBI, SSBI PR, PPR, or equivalent investigation exists that is no more than five years old and it has not been adjudicated, an interim national security eligibility is not required if:

1. There has not been a break in service greater than 24 months.

2. The required BI has been opened by the ISP.

3. A request is submitted to DoD CAF requesting a TS national security eligibility be granted.

c. Commands will record interim access in JPAS or successor system.

d. Interim access for SCI may be only authorized by the DoD CAF.

e. It is important to ensure that the request for investigation reaches its destination, especially when interim access is at issue. Since interim access is a stopgap measure

that anticipates a timely and favorable result, commands must be vigilant in monitoring these requests and are strongly encouraged to use JPAS or successor system when sending additional information and other required/related documentation to the DoD CAF.

f. When the command receives a LOI and a SOR from the DoD CAF to deny an individual's security clearance, the CO will immediately withdraw interim access.

g. Interim access or assignment to sensitive positions is not authorized for individuals who have received a final unfavorable eligibility determination. Requests for reinstatement may be submitted to the DoD CAF; however, interim access is not authorized until eligibility is reestablished.

5. One-Time Access. To support urgent operational or contractual requirements, cleared DON personnel are authorized one-time or short duration access to classified information at a higher level than their existing national security eligibility. In such situations, and only for compelling reasons in furtherance of the DON mission, an authority referred to in subparagraph c.(1), below, may grant higher level access on a temporary basis, subject to the terms and conditions prescribed below. This special authority may be revoked for abuse, inadequate record keeping, or inadequate security oversight. These procedures do not apply when circumstances exist which would permit the routine processing of an individual for the higher level national security eligibility:

a. If the access granted involves another agency’s classified information, then that agency must concur before access is granted.

b. Access must not exceed 180 days and is limited to specific, identifiable information that is made the subject of a written record.

c. Procedures and conditions for effecting emergency one-time access to the next higher classification level are as follows:

(1) Authorization for such one-time access or short duration access will be granted by a Flag or General Officer, a general court martial convening authority or SES equivalent member, after coordination with supporting security officials. Authorities may grant one-time or short-duration access to information classified at the same (or lower) level of access as that held by the authority.

(2) The recipient of the one-time access authorization must be a U.S. citizen and possess current DoD national security eligibility. The access required will be limited to classified information one level higher than the current clearance.

(3) Such access, once granted, will be canceled promptly when no longer required, at the conclusion of the authorized period of access, upon notification from the granting authority or if credible derogatory information is discovered, the individual should be debriefed.

(4) The employee to be afforded the higher level access will have been continuously employed by the DoD or a cleared DoD contractor.

(5) Local, personnel, and security records of the employee concerned will be reviewed to ensure there is no derogatory information.

(6) Whenever possible, access will be confined to a single instance or, at most, a few occasions. The approval for access will automatically expire 180 calendar days from date access commenced. At such time as it is determined that the need for access is expected to extend beyond 180 days, the individual concerned will be promptly processed for the level of national security eligibility required. When extended access has been approved, such access will be canceled at or before 180 days from original date of access.

(7) Access at the higher level will be limited to information under the control and custody of the authorizing official and will be afforded under the general supervision of a properly cleared employee. The employee charged with providing such supervision will be responsible for: (1) recording the higher level information actually revealed; (2) the date(s) such

access is afforded; and (3) the daily retrieval of the material accessed.

(8) Access at the next higher level of COMSEC, SCI, SAP, NATO, National Command and Control-Extremely Sensitive Information, or foreign government information is strictly prohibited.

(9) The exercise of this provision will be used sparingly and repeat use within any 12-month period for the same individual is prohibited. The approving authority will maintain a record (in accordance with DON records management policy and the DON's approved records management schedule) containing the following data with respect to each one-time access approved:

(a) The name and Social Security Number (SSN) of the employee afforded higher level access.

(b) The level of access authorized.

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

(d) An unclassified description of the specific information to which access was authorized and the duration of access along with the date(s) access was afforded.

(e) A listing of the local records reviewed and a statement that no credible derogatory information concerning the employee is known to exist.

(f) The approving authority's signature certifying subparagraphs (1) through (5), above.

(g) Copies of any pertinent briefings and/or debriefings administered to the employee.

6. Withdrawals or Adjustment of Access

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

b. COs will administratively withdraw an individual's access authorization when a permanent change in official duties eliminates the DON requirement for access. The command will debrief the individual as outlined in paragraphs 4-11 and 4-12 and file the completed Security Termination Statement (if required as stated in para 4-12) in the individual's service record or OPF. Commands will update JPAS or successor system accordingly to indicate that the individual no longer requires access.

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

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

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

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

7. Suspension of Access for Cause

a. When questionable or unfavorable information becomes available concerning an individual who has been granted access to classified information or assigned to sensitive duties, commands will report that information to the DoD CAF via JPAS or successor system "Report Incident" link within the same calendar day as the suspension. The Military Department Counter Intelligence Organization or FBI may direct this reporting not be done.

(1) COs will determine whether, on the basis of all the facts, to suspend or limit an individual's access to classified information, or reassign the individual to non-sensitive duties pending a final eligibility determination by the DoD CAF.

(2) Once an individual’s access is suspended for cause, the DoD CAF will remove eligibility and the command cannot reinstate access until DoD CAF adjudicates the issues and makes a favorable eligibility determination.

(3) Suspension of access is required when a civilian employee with security clearance is incarcerated (to include Work Release Programs) as the result of a conviction for a criminal offense or is absent without leave for a period exceeding 30 days.

(4) Suspension of access is required when a military member with a security clearance is discharged under Other Than Honorable conditions, is incarcerated (to include Work Release Programs) as the result of a conviction for a criminal offense or violations of the UCMJ, is declared a deserter, or is absent without leave for a period exceeding 30 days.

b. Whenever a determination is made to suspend access to classified information the following is required:

(1) The individual concerned must be notified of the determination in writing within 10 days by the CO or designee, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security.

(2) Commands and activities must report all suspensions to the DoD CAF no later than 10 working days from the date of the suspension action via JPAS or successor system, providing sufficient details to support adjudicative review.

(3) Remove the individual's access authorization from JPAS or successor system and remove the individual's name on all local access rosters and visit certifications, and notify all co-workers of the suspension.

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

(5) Cancel or hold in abeyance any PCS orders. Notify NAVPERSCOM (PERS-483) for Navy military members or HQ USMC for Marine military members.

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

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

(2) Alternatively, the CO may also elect to submit additional documentation to the DoD CAF that supports his/her concerns regarding the individual's disqualification. The DoD CAF will review and appraise the command accordingly.

8. Access by Retired Personnel

a. Retired personnel, including those on the temporary disability retirement lists, are not entitled to have access to classified information merely by virtue of their present or former status. When a CO decides to grant a retiree access to classified information in the furtherance of the DON mission, a request for access authorization may be submitted to the DoD CAF following the below guidance.

b. As an exception to the above, an active duty Flag/General Officer or equivalent civilian SES may waive the investigative requirement and grant a retired Flag/General Officer/civilian SES temporary access to classified information when he/she determines that there are compelling reasons in furtherance of a DON program or mission to grant such access. The period of access will not exceed one year.

(1) Access may only be granted to information classified at a level commensurate with the security clearance held by the retired Flag/General Officer/civilian SES at the time of his/her retirement. Granting SCI or SAP access is prohibited.

(2) Access will be granted only under the condition that the retiree does not remove classified materials from the confines of a government installation or other areas approved for storage of classified information.

(3) The Flag/General Officer/equivalent civilian SES granting the access will inform the DoD CAF within five days of this event by a written record of the following data for retention in JPAS or successor system for two years after access is granted:

(a) The name and SSN of the employee afforded access.

(b) The date and level of access authorized.

(c) Compelling reason to grant the higher-level access and the benefit to the DON mission or event.

(d) The identity of the approving authority.

(4) If continued access beyond the one-year limit is necessary, the report to the DoD CAF must be accompanied by requests for the appropriate BI and clearance.

9. Access by Reserve Personnel

a. Reserve personnel in an "active status" may be granted access as necessary, provided they hold the appropriate security clearance eligibility or the appropriate BI has been requested from the ISP. For Active Duty for training (less than 30 days) and inactive duty training (drills) procedures described in paragraph 9-4, may apply.

b. Reserve personnel may also be given access to COMSEC information necessary to maintain proficiency in their specialty. Details are provided in the Cryptographic Security Policy and Procedures Manual, (NOTAL), and in the

Electronic Key Management System (EKMS-1) Phase 4 Communications Security Material Systems Policy and Procedures for Navy EKMS Tiers 2 & 3.

10. Access by Investigative and Law Enforcement Agents

a. Investigative agents of other departments or agencies may obtain access to classified information only through coordination with NCIS.

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

11. Access Authorization in Legal Proceedings

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

b. OGC or OJAG will evaluate the request and certify that access to the specified classified information has been deemed necessary by the convening authority and will ensure the attorney requiring the access has completed the necessary PSI request forms. OGC or OJAG will then forward the certified access request to DUSN (S&I) for approval.

c. OJAG will submit the request for investigation to NBIB and will grant access upon receipt of approval from DUSN (S&I), as appropriate. Prior to access, the attorney will be required to sign the Classified Information Nondisclosure Agreement (SF 312).

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

12. Contractor Access

a. COs may grant access to classified information to contractor employees based on the contractor's need-to-know and verification of access. Section 9 provides visit request details.

b. COs may, at any time, deny contractor employees access to areas and information under their command control for cause. However, suspension or revocation of contractor security clearances can only be affected through DCSA. Action taken by a command to deny a contractor access to the command areas and information will be reported to the CSA. A report will also be forwarded to the VROC or DoD CAF if SCI access is involved. Refer to Section 10.

c. Additionally, restrictions on DoD contractors for access to information generated by foreign governments are described in the reference (e), Disclosure of Classified Military Information and Controlled Unclassified Information (CUI) to Foreign Governments, International Organizations, and Foreign Representatives.

13. Access Authorization for Persons Outside of the Executive Branch of the Government

a. The DHS is responsible for the submission of BI and adjudication of national security eligibility for state, local, tribal, and private sector employees or entities who are not supporting a DoD mission.

b. Members of the U.S. Supreme Court, the Federal judiciary, and the Supreme Courts of the individual states do not require national security eligibility. They may be granted access to DON classified information to the extent necessary to adjudicate cases being heard before their individual courts.

14. Historical Researchers

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

(1) Requests for access authorization for DON classified information will be processed by the Director of Naval History and Heritage Command, Office of the Chief of Naval Operations (DNS-H), 805 Kidder Breese Street, Southeast, Washington Navy Yard, DC 20374 or the Director of History and Museums, USMC, Marine Corps Education Command, Marine Corps University, History Division, CMC (Code HD) 3079 Moreell Avenue, Quantico, VA 22134.

(2) Upon receipt of a request for access authorization, CNO (DNS-H) or CMC (Code HD) will seek to declassify the requested records. If declassification cannot be accomplished, CNO (DNS-H) or CMC (Code HD) will:

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

(b) Obtain from the researcher completed investigative request forms appropriate for the level of access required and submit them with the recommendation requesting access authorization to DUSN (S&I), via HQMC PP&O/PS, for Marine Corps requests, who will advise whether access is authorized for the specific project.

(c) Have the researcher sign a Classified Information Nondisclosure Agreement (SF 312).

(d) Limit the researcher's access to specific categories of information over which the DON has classification jurisdiction or to information within the scope of the historical research if the researcher has obtained written consent from the DoD or non-DoD departments or agencies with classification jurisdiction over that information.

(e) Retain custody of the classified information at a DON installation or activity or authorize access to documents in the custody of the National Archives and Records Administration.

(f) Obtain the researcher's written agreement to safeguard the information and to submit any notes and manuscript for review by the DON or other DoD or non-DoD department or agency with classification jurisdiction, to determine that they

do not contain classified information.

b. Access authorizations are valid for not more than two years from the date of issuance. Extensions may be granted by DUSN (S&I), if recommended by CNO (DNS-H) or CMC (Code HD).

15. Limited Access Authorization (LAA) for Non-U.S. Citizens

a. Only U.S. citizens are eligible for U.S. national security eligibility. Access to classified information may be justified for compelling reasons in the furtherance of the DON mission to a non-U.S. citizen who possess a special expertise, who may at the discretion of the CO, be processed for limited access to classified information only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a compelling need for access to classified information and for which a cleared or clearable U.S. citizen is not available. A non-U.S. citizen, including an immigrant alien, may be issued a LAA if:

(1) The individual is a citizen of a country with which the U.S. has an agreement providing for security assurances.

(2) The investigative requirements for a LAA are equivalent to the investigative requirements of that country.

b. An LAA enables a non-U.S. citizen to have limited access to classified information, but a LAA is not a national security eligibility. An LAA may be justified in those rare circumstances when:

(1) A cleared or clearable U.S. citizen is not readily available or does not possess the skills or expertise required.

(2) The non-U.S. citizen possesses unique skill or expertise needed to support a specific U.S. Government requirement involving access to classified information.

(3) Access to classified information provided to the U.S. Government by another government or international organization will not be permitted under an LAA without written consent of the government of the organization to the country(ies) of which the individual is a citizen that provided the information.

(4) LAAs will be reviewed annually to determine if continued

access is in compliance with policy. DUSN (S&I) will maintain a record of all LAAs in effect and submit an annual report to the Office of the DDI(I&S) by January 15 for the preceding year providing a summary by access level (Secret or Confidential), country(ies) of citizenship, and employment location.

c. An export license or disclosure authorization is required to release classified information to a non-U.S. citizen who has been issued an LAA. Before submitting an application for an LAA, the requestors must obtain a written disclosure determination from a principal or designated disclosure official or obtain a DOS approved export license. This documentation must be submitted with the application for an LAA. The LAA cannot serve as an export authorization. An approved LAA is a determination that the non-U.S. citizen is eligible to receive the classified information governed by the disclosure authorization or DOS approved export license.

d. Personnel granted LAAs are not permitted physical custody of classified material, uncontrolled access to areas where classified information is stored or discussed. Classified information will be maintained in a location under the continuous control and supervision of an appropriately cleared U.S. citizen.

e. LAAs will not be granted to personnel who perform routine administrative or other support duties.

f. Non-U.S. citizens will not be eligible for access to any greater level of classified information than the U.S. Government has determined may be released to the country of which the person is a citizen, but not to exceed the Secret level.

g. Personnel granted LAAs will not be designated as a courier or escorts for classified material unless they are accompanied by an appropriately cleared U.S. citizen.

h. When a LAA is justified for a non-U.S. citizen, including an immigrant alien, the CO may submit a request via the Echelon II for submission to the CNO or Major Command via HQMC PP&O/PS for endorsement and submission to DUSN (S&I) if:

(1) The individual is a citizen of a country with which the U.S. has an agreement providing for security assurances.

(2) The investigative requirements for the LAA are

commensurate with the investigative requirements of that country.

(3) A favorably completed and adjudicated SSBI/T5 (within the immediately preceding five years) is required before granting an LAA. If the SSBI/T5 cannot provide full investigative coverage, a polygraph examination (if there are no applicable host country prohibitions) to resolve the remaining personnel security issues will be favorably completed in accordance with reference (ae) before granting access.

(4) If geographical, political, or medical situations prevent the full completion of the SSBI/T5 or prevent the polygraph examination to supplement a less than full SSBI/T5, an LAA may be granted only with the approval of the DDI(I&S).

(5) If an LAA is withdrawn and the person subsequently is again considered for a new LAA, an SSBI/T5 and polygraph examination may be required. The scope of the SSBI/T5 will cover the period since the previous investigation or 10 years, whichever is shorter.

(6) A PR/T5R will be conducted on every person with an LAA five years from the closing date of the previous SSBI/T5 or SSBI-PR/T5R, as appropriate.

i. An LAA granted under the provisions of this manual is not valid for access to:

(1) TS information.

(2) RD or formerly restricted data.

(3) Information that has not been determined releasable by a U.S. Government designated disclosure authority to the country(ies) of which the individual is a citizen.

(4) COMSEC information.

(5) Intelligence information.

(6) Information for which foreign disclosure has been prohibited in whole or in part.

(7) Information provided to the U.S. Government in confidence by a third party government and classified information

furnished by a third party government.

j. When a LAA is justified, a CO may submit a request to the Echelon II via the CNO and Major Commands will submit via HQMC PPO&S for endorsement, with the following information and supporting documentation to DUSN (S&I):

(1) Initial LAAs will contain a detailed justification and plan describing:

(a) The location of the classified material (security containers) in relationship to the location of the foreign national.

(b) The compelling reason for not employing a cleared or clearable U.S. citizen.

(c) A synopsis of an annual continuing assessment program to evaluate the individual’s continued trustworthiness and eligibility for access.

(d) A plan to control access to secure areas and to classified and controlled unclassified information.

(2) The identity of the individual for whom the LAA is requested, including full name, date and place of birth, current citizenship(s), SSN (if held), foreign passport number, any national identifying number issued by the individual’s country(ies) of citizenship, whether the individual is an immigrant alien or a FN; if an immigrant alien, the date and place such status was granted; and date and type of most recent PSI. (If a SSBI/T5 has not been completed within the past five years, a completed SF 86 must be forwarded to the ISP.)

(3) Grade/rank/organization and description of the position requiring access and the specific duties (delineated as precisely as possible) for which access is requested.

(4) The compelling reasons for the request including an explanation of the special skills or special expertise the individual possesses and the rationale for not employing a cleared or clearable U.S. citizen.

(5) A full description of the specified classified

information to be accessed, including classification.

(6) A copy of the foreign disclosure authority determination for the specified classified or CUI.

(7) An explanation as to how the command plans to control and limit the individual's access.

(8) A statement that the candidate has agreed to undergo a counterintelligence-scope polygraph examination when needed.

(9) The period of time for which access is required (not to exceed five years).

(10) Follow the procedures specified by the ISP when completing the SF 86 in those instances where a non-U.S. citizen does not have an SSN.

k. All LAA determinations, favorable and unfavorable, will be entered into the DoD adjudication system of record.

l. DUSN (S&I) will review the LAA request to ensure it meets program parameters.

(1) Requests that are incomplete or not properly justified will be promptly returned to the requester and/or subordinate unit with an explanation.

(2) No authorization for access to classified information can be issued until favorable adjudication of the SSBI/T5 or T5R is completed by the DoD CAF and authorization is approved by DUSN (S&I).

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

(1) Only at the Secret and Confidential levels. Limited access to Secret and Confidential information may be granted following completion of the SSBI by an authority as specified in enclosure (7) A.3 of reference (b).

(2) The classified information to which the non-U.S. citizen may have access will be approved for release to the person’s country

(or countries) of citizenship, in accordance with reference (af). Exceptions may apply in operational exigencies. In such cases, the SECNAV may approve the release of information to individuals granted an LAA when it is determined to be in the best interests of national security.

(3) Access to classified information will be limited to a specific program or project. The LAA will be cancelled upon completion of the program or project for which it was approved.

(4) Access by foreign nationals to DOD information systems containing classified information will comply with conditions prescribed in DODI 8500.01.

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

(6) Individuals with LAAs will be placed under the general supervision of appropriately cleared U.S. citizens. Supervisors will be made fully aware of the limits to access imposed and that physical custody of classified information by the individual is not authorized.

n. LAAs are authorized for five years. If a LAA is required in excess of five years, a new request must be submitted following the procedures outlined in paragraph 2, including a completed SSBI-PR request package. DUSN (S&I) will review the new request and may approve continuation of the LAA, as appropriate, pending favorable adjudication of the completed SSBI-PR/T5R.

o. If an individual granted a LAA is transferred to another position, the LAA previously granted is rescinded. The individual will be debriefed in accordance with Section 4. If the individual is transferring to other duties requiring a LAA, the command will request a new access authorization, again following paragraph 9-15 procedures. If the individual's SSBI is less than five years old, a new PSI may not be required. However, all other procedures must be followed to include updating the previous SF 86, initialing, and re-signing. Otherwise, a new SF 86 is required and submitted to continuous evaluation for the DoD CAF review.

p. Should a LAA be revoked, the individual will be

debriefed and a record of the signed debriefing statement (security termination) will be retained locally for a period of five years. No due process procedures are afforded under this program.

q. The LAA will be canceled or re-justified as described herein upon completion of the program or project.

r. National security eligibility previously granted to U.S. citizens who subsequently lost citizenship, such as citizens of a former U.S. Territory or Province, may be eligible for a LAA, provided these individuals possess a unique skill and a cleared US citizen is not available.

s. LAAs for non-U.S. citizen contractor personnel will be processed in accordance with reference (w).

t. Access to classified information outside the scope of the approved LAA will be considered a compromise of classified information and investigated.

16. Personnel Exchange Program Access. The degree of access by representatives of foreign governments, including Personnel Exchange Program personnel, will be scrupulously limited to that allowed by the foreign disclosure authorization issued by the Navy International Programs Office on a case-by-case basis.

17. NATO Access

a. Personnel assigned to a NATO staff position requiring access to NATO information will have been the subject of a favorably adjudicated T3 or T5 PSI (within five years prior to the assignment), in accordance with reference (ab) (United States Security Authority for North Atlantic Organization Affairs). Foreign nationals of a NATO member nation may be granted an LAA in accordance with reference (b).

b. Personnel not assigned to a NATO staff position, but requiring access to NATO information in the normal course of their duties, must possess the equivalent final U.S. national security eligibility based upon the appropriate PSI. A NATO Security Clearance Certificate is obtained by the CSA from the individual’s home country.

c. Personnel assigned to NATO staff positions may submit reinvestigation requests up to one year in advance of the required timeframe. NATO access is limited to performance on a specific NATO program or project.

18. SCI Access

a. SCI adjudication and eligibility determinations will be made in accordance with reference (b),(1), and (r).

b. The DoD CAF, as delegated by the HICE, is responsible for decisions rendered with respect to SCI access eligibility or ineligibility. In addition, the DoD CAF is also delegated the responsibility to adjudicate DON contractor personnel requiring SCI access eligibility under the NISP and reference (r).

c. When SCI access is removed from an individual for adverse reasons, the DoD CAF will review the adverse information and make a separate collateral eligibility determination. If an SCI access is removed for contractor personnel cleared through the NISP, the VROC, in coordination with the DoD CAF, will advise the contractor if loss of SCI access also warrants withdrawal of collateral eligibility.

d. The PSAB has been delegated the authority to review final appeals of unfavorable SCI access eligibility determinations. The decision of the PSAB regarding SCI eligibility is final.

e. The following basic procedures apply to request DoD CAF SCI access eligibility determinations:

(1) If it is determined that SCI access is required and a valid (i.e., was not conducted within the past five years) SSBI/T5 does not exist, an T5 (or an outdated PR/T5R exists) will be requested as directed by Section 5.

(2) If SCI access is required and a valid SSBI/T5 or SSBI-PR/T5R exists, the CO will request a SCI eligibility determination from the DoD CAF using the JPAS.

(3) Commands are required to report the citizenship of immediate family members as reference (b) imposes additional

procedural requirements for individuals with foreign national immediate family members.

(4) Upon favorable adjudication of the completed T5 or T5R, the DoD CAF will update the JPAS or successor system to reflect a final SCI eligibility determination.

f. Requests for exceptions to Intelligence Community Directive 704 for SCI access eligibility will be prepared as directed by reference (b) and forwarded to the DoD CAF.

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

(1) Information that could potentially affect an individual's eligibility must be reported to the DoD CAF in accordance with the procedures outlined in reference (b). The DoD CAF will either reaffirm eligibility or will begin the unfavorable determinations process.

(2) COs may suspend, or debrief for cause from SCI access in accordance with reference (b). Coordinate with the CSM, HRO and notify the DoD CAF.

(3) A SSBI-PR/T5R is required every five years for individuals with SCI access.

19. Access to and Dissemination of RD Including Critical Nuclear Weapon Design Information (CNWDI)

a. RD, as defined in the Atomic Energy Act of 1954 as amended is data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but does not include data declassified or removed from the RD category under Section 142 of the Act.

(1) Access to RD within and between DON commands, National Aeronautics and Space Administration (NASA), and

contractor activities will be governed by the same procedures and criteria as govern access to other classified information:

(a) Access is required in the performance of official duties.

(b) The individual has a valid security clearance commensurate with the level of access required for the information.

(2) Requests for access to RD not under the control of the DoD and/or NASA will be made in accordance with reference (ac), Access to and Dissemination of Restricted Data, 12 January 1978.

(a) Requests by members of DON commands requiring access to RD at DOE facilities will be made utilizing the DOE Visit Request Form 5631.20, Request for Visit or Access Approval, and will be submitted via the appropriate DON certifying official identified per reference (ac) to the Associate Deputy Assistant Secretary for Technical and Environment Support (DP-45), Department of Energy, Washington, DC 20585.

(b) Conflicts in guidance and inquiries relating to access and/or the protection of RD by DON personnel and commands should be referred to DUSN (S&I) for resolution.

(3) The following procedures apply to DON commands and personnel who disseminate RD under their control:

(a) Within and between DoD commands, to include DoD contractors, dissemination of RD information will be governed by the same procedures and criteria as govern the dissemination of other classified information; verify the identity of the prospective recipient, verify the prospective recipient's clearance, and insure the prospective recipient has an official "need-to-know."

(b) Dissemination of RD and formerly RD outside DoD will be made in accordance with reference (ab).

b. CNWDI is TS RD or Secret RD that reveals the theory of operation or design of the components of a thermo-nuclear or

implosion type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive material by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test or replace.

(1) Access to and dissemination of CNWDI is of particular concern due to the extreme sensitivity of this type of information. Access must be limited to the absolute minimum number of persons needed to meet mission requirements. To meet this objective, the following special requirements and procedures for controlling CNWDI information have been established:

(a) Final TS or Secret clearance as appropriate.

(b) Except in rare instances, only U.S. citizens will be granted access. When an immigrant alien possesses unique or very unusual talents and/or skills that are essential to the U.S. government that are not possessed to a comparative degree by an available U.S. citizen, a request with justification to use such individual will be forwarded to DUSN (S&I) for approval. LAA procedures apply.

(c) Requests by members of DON commands for access to CNWDI at DOE facilities will be made utilizing DOE Visit Request Form 5631.20 and must be submitted via an appropriate DON certifying official to the Associate Deputy Assistant Secretary for Technical and Environment Support (DP-45), DOE, Washington, DC 20585. Reference (ac) contains a listing of DON officials authorized to certify access to CNWDI at DOE facilities. Recommendations for changes to the list of DON approved certifying officials will be submitted, with supporting justification to DUSN (S&I) for approval and inclusion in reference (ac).

(d) Verification of "need-to-know." Certifying officials will not automatically approve requests for access to CNWDI, but will insist upon full justification and will reject any requests that are not completely justified. Certifying officials have a special responsibility to insure that this "need-to-know" principle is strictly enforced.

(e) Personnel having a need for access to CNWDI will be briefed on its sensitivity. Briefings and access authorizations will be recorded in appropriate security records and maintained in a manner that facilitates verification. Similarly, personnel whose CNWDI access is terminated (reassignment, etc.) must be debriefed. Individual briefing/debriefing records will be maintained two years after access is terminated. Each DON command will establish procedures and format for briefing/debriefing.

(2) For additional guidance refer to reference (ac) or contact DUSN (S&I).

20. Wounded Warrior Security and Intelligence Internship Program

a. PSIs in support of designated wounded Service Members may be submitted and processed regardless of the time remaining in service. Reinvestigations will be submitted in accordance with paragraph 6-2.

b. Category 2 wounded, ill, or injured Service Members who expect to be separated with a medical disability rating of 30 percent or greater may submit investigative requests for TS or SCI eligibility before medical separation as long as they are serving in or have been nominated for a Wounded Warrior Internship Program.

c. The investigations will be funded by the DoD office offering the internship. If the office offering the internship does not have funds available, the owning Military Department may choose to fund the investigation.

d. Investigations submitted in support of Wounded Warrior Security and Intelligence Internship Program should:

(1) Not request priority service.

(2) Include the extra coverage code “WW” in Block B of the “Agency Use Only” section of the SF 86. This will expedite scheduling and completion of investigations submitted in support of the Wounded Warrior Security and Intelligence Internship Program.

(3) Notify NBIB via e-mail to operationwarfighter@nbib.gov. Include the subject's full name, the e-App request identification number, and the DoD POC should NBIB need additional information.

VISITOR ACCESS TO CLASSIFIED INFORMATION

1. Overview

a. For the purposes of this policy manual, the term visitor applies as follows:

(1) A visitor on board a ship or aircraft is a person who is not a member of the ship's company or not a member of a staff using the ship as a flagship.

(2) A visitor to a shore establishment is any person who is not attached to or employed by the command or staff using that station as headquarters.

(3) A person on temporary additional duty is considered a visitor. Personnel on temporary duty orders, reservists on active duty for training, or those personnel assigned on a quota to a school for a course of instruction, may also be considered as visitors.

b. The movement of all visitors shall be controlled to ensure that access to classified information is deliberate and consistent with the purpose of the visit. If an escort is required for the visitor, a military, civilian, or a cleared contractor assigned to the command being visited may be assigned escort duties.

c. As a matter of convenience and courtesy, Flag Officers, General Officers and their civilian SES equivalents are not required to sign visitor records or display identification badges when being escorted as visitors. Identification of these senior visitors by escorts will normally be sufficient. The escort should be present at all times to avoid challenge and embarrassment and to ensure that necessary security controls are met. If the visitor is not being escorted, all normal security procedures will apply.

d. At the discretion of the CO, the general public may be permitted to visit on an unclassified basis only, (i.e., no classified areas, equipment or information, or CUI may be divulged to the general public). A written statement of command

safeguards will be prepared and implemented assuming the possibility of the presence of foreign agents among the visitors and ensuring proper protections are in place.

e. Visit Authorization Letters 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 or successor system.

2. Classified Visits

a. COs shall establish procedures to accommodate visits to their commands involving access to, or disclosure of, classified information. As a minimum these procedures will include verification of identity, validation of personnel security clearance eligibility, and access using JPAS or successor system, and a need-to-know determination.

b. The command sponsoring the visitor is responsible for ensuring the visitor's eligibility, access, and affiliation data are current and accurate in JPAS or successor system.

c. In addition to requirements for authorizing access to classified information, the visited command must also fulfill the local facility access and general visit control requirements. If local conditions necessitate formal visit request letters for visit/access control purposes, the command sponsoring the visitor must comply with local facility access requirements.

d. Visits involving access to and dissemination of RD, or to facilities of the DOE, are governed by the policies and procedures in reference (ab) (NOTAL).

3. Visits By Foreign Nationals and Representatives of Foreign Entities

a. Consult reference (e) concerning foreign visitors, whether or not the visitor requires access to classified, or CUI material.

b. Visits by foreign nationals and representatives of

foreign governments, foreign industry, or international organizations, must be approved, and the disclosure level for classified information determined, for each visitor. Official requests must be submitted by the applicable foreign government (normally its Washington, D.C. embassy), certifying the visitor's national clearances and need-to-know on their behalf.

4. Classified Visits By Members of Congress

a. When a direct request for a congressional visit, which would require disclosure of classified information, is received, guidance will be requested from the Office of Legislative Affairs (OLA) by the quickest practical means. If there is inadequate time to coordinate with OLA, the visit may be authorized and disclosure of classified may be made. Immediately thereafter, the OLA will be informed of the visit and the extent of the disclosure of information provided. In case there is a question as to whether particular classified information may be furnished to a member of congress, the CO will release the information and will immediately contact the SECNAV through the OLA.

b. Members of congress, by virtue of their elected status, do not require DoD security clearances. Clearance eligibility is required however, for congressional staff members accompanying a member of congress, paragraph 7-8.5 applies.

5. Classified Visits By Representatives of the General Accounting Office (GAO)

a. Properly investigated, adjudicated, and identified representatives of the GAO may request a visit and be granted access to classified DON information in the performance of their assigned duties and responsibilities, with some exceptions.

(1) The GAO normally will give advance notice to commands to be visited. Each announcement will include the purpose of the visit and names of representatives and, if access to classified information may be necessary, will certify the level of security eligibility of each GAO representative.

(2) Occasionally, GAO representatives in the Washington metropolitan area receive assignments, such as Congressional requests, which preclude the usual advance notice of visit, and verbal arrangements are made for visits. To assist the GAO in those instances, the DON commands will verify eligibility and access requirements through Director, Audit and Cost Management Division, (NAVINSGEN 4).

(3) As exceptions to the procedures described above:

(a) COs will not grant access to documents and information specified as not releasable or requiring approval of the SECNAV for release, enclosure (1) to reference (x), Relations with the GAO (NOTAL).

(b) Requests for classified defense information in the area of tactical operations and intelligence collection and analysis will be sent to the Comptroller of the Navy (via the CMC, for USMC cases) by the most expeditious means, to determine the relevance of the information to the statutory responsibilities of the GAO.

b. Questions and problems concerning clearances of individuals and release of classified information in connection with visits of the GAO will be addressed to the NAVINSGEN 4.

CONTINUOUS EVALUATION

1. Overview

a. A personnel security determination requires an examination of a sufficient amount of information regarding an individual to determine whether the individual is an acceptable security risk. Commanders will establish and maintain a program designed to evaluate on a continuing basis the status of personnel under their jurisdiction with respect to national security eligibility and ensure:

(1) Close coordination between security, human resource offices, medical, law enforcement, insider threat, counter-intelligence and legal communities, as well as managers and supervisors to ensure that all pertinent information available within a command is considered in the personnel security process.

(2) Commanders will report derogatory information to the DoD CAF per reference (b) via JPAS or its successor. Reporting of derogatory information is not discretionary.

b. Commanders will establish a continuous personnel security training and awareness program with a focus to inform the workforce of personnel security requirements for obtaining and maintaining national security eligibility and their responsibilities for protection of classified or sensitive information.

c. Commanders will ensure personnel assigned to sensitive duties receive an initial security briefing and annual refresher briefings on the national security implications of their duties and their individual responsibilities in accordance with reference (b). These briefings will emphasize the individual’s responsibility to meet the standards and criteria for national security eligibility as stated in the national security adjudicative guidelines. Ensure training records are maintained for three years after the subject has transferred, separated, or retired in accordance with reference (f).

d. Commanders will ensure personnel in national security or sensitive positions are provided with information about

available programs (e.g. employee assistance) designed to help employees address questions or concerns regarding issues that may affect their ability to remain eligible for access to classified information or assignment to sensitive positions to include:

(1) Initiatives designed in a manner that eliminates stigmas associated with seeking care. Commanders are encouraged to ensure all Service Members, civilians, and contractor personnel assigned are aware that seeking financial, marital, behavioral, and other types of counseling is a positive step in supporting continued national security eligibility.

(2) Initiatives to identify potential concerns at an early stage so that any assistance rendered by the employing activity will have a reasonable chance of precluding long-term, job-related security problems.

(3) Supervisory personnel are informed of their personnel security responsibilities and provided guidance on indications of potential personnel security concerns and procedures to be followed and reported in a timely manner. Programs will include:

(a) Training and continuous education on reportable behaviors.

(b) Procedures for immediate reporting of derogatory information and the associated investigations and administrative or disciplinary action to the DoD CAF.

(c) Outreach to inform personnel of programs to address behavior(s) that may affect their continued eligibility for access to classified information or assignment to a sensitive position.

(4) Ensure derogatory information and the administrative or disciplinary action taken as a result of management review or inquiry is reported to the appropriate security, law enforcement, or CI professionals for appropriate action. Upon coordination with CI and law enforcement professionals as necessary, unless directed otherwise by the supporting CI

professional, an incident report will be submitted in accordance to paragraph 8-7.

(a) Administrative or disciplinary action does not preclude the submission of derogatory information to the DoD CAF.

(b) Credible derogatory information shall be reported to the DoD CAF even if the individual will be departing the organization, retiring/separating military service, or separating from federal service.

(5) Credible derogatory information concerning cleared NISP contractor personnel shall be reported to the DoD CAF in accordance with paragraph 8-4.

(6) Reporting by health care professionals regarding military personnel is subject to the limitation required by reference (ad), Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members.

(7) Security professionals, at the direction of the commander, will:

(a) Report unfavorable information meeting the reportable behavior guidelines contained in reference (b), Section 11: “Continuous evaluation and Reporting Requirements” to DoD CAF, law enforcement, and/or NCIS. When authorized, forward the report to the adjudication facility via JPAS or successor system, as appropriate.

(b) Provide the following details for all security incidents or issues of a security concern (to the extent available):

1. Nature and seriousness of the conduct.

2. Circumstances surrounding the conduct.

3. The frequency and decency of the conduct.

4. The age of the individual at the time of the conduct.

5. The voluntariness or willfulness of the individual's participation or conduct.

6. The knowledge the individual had of the consequences involved.

7. The motivation for the conduct.

8. How the command became aware of the information.

9. Actions the individual has taken to correct the issue, including medical treatment, counseling, lifestyle changes, or other corrective actions.

10. The stability of the individual's lifestyle or work performance, including demonstrative examples.

11. Cooperation on the part of the individual in following medical or legal advice or assisting in command efforts to resolve the security issue.

12. A command recommendation to the supporting adjudication facility with a copy of that recommendation to the individual on whether to retain an individual's eligibility pending the conclusion of a national security investigation or when rendering a final determination.

13. Receive continuous evaluation alerts and respond to continuous evaluation alerts via JPAS or successor system as required.

14. Submit incident reports on individuals that separated from the DON or changed affiliation prior to the submission of derogatory information.

(8) Supervisors will:

(a) Continuously evaluate individuals with national security eligibility to determine if they continue to be trustworthy in accordance with the security standards in the adjudicative guidelines.

(b) Not review the security forms of anyone undergoing a PR who is under their supervision. Supervisory knowledge of any significant derogatory information is to be independent of the information reflected on the security form.

(c) Report any derogatory information that falls within the adjudicative guidelines to their cognizant security professional or commander. Failure to report derogatory information may trigger an adverse security action in accordance with paragraph 2b of this enclosure.

(d) Ensure the discharge of security responsibilities is included in personnel performance evaluations, pursuant to section 552a of reference(u) and in accordance with applicable DoD Component guidance.

(9) Individual responsibilities and/or self-reporting:

(a) Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties, receive briefings, and attend required security awareness training. Further, individuals must be aware of the standards of conduct required of persons with access to classified information or assignment to sensitive duties. Personnel will:

(b) Protect classified information in their custody from unauthorized disclosure.

(c) Be aware of, and comply with, reinvestigation, continuous evaluation, and reporting requirements.

(d) Report any information per references (b) and (d).

(e) Report all personal foreign travel for unplanned day trips to Canada or Mexico within five business days and any other foreign travel to the supporting security manager and/or SSO at least 14 working days in advance of departure date and request a foreign travel briefing. Report the use of a foreign passport when traveling outside the U.S.

(f) Contact the supporting security manager or SSO and request coordination with the DON supporting CI element to receive a foreign travel debriefing (when instructed to do so, prior to departure or when suspicious activity occurred during a trip abroad).

(10) Report the below listed matters to the supporting security office, who will, in-turn, immediately report to the CI office, any attempts by any U.S. persons, or representatives or citizens of foreign countries to:

(a) Cultivate a friendship to the extent of placing one under obligation that he or she would not normally be able to reciprocate, or by offering money payments or bribery to obtain information of actual or potential intelligence value.

(b) Obtain information of actual or potential intelligence value through observation, collection of documents, or by personal contact.

(c) Coerce by blackmail, by threats against, or promises of assistance to relatives living under foreign control.

(11) Individuals becoming aware of sabotage, international terrorism, espionage, deliberate compromise, or other subversive activities will report all available information immediately to the supporting CI office.

(12) Individuals with access to SCI information will comply with reporting requirements identified in reference (k).

(13) All employees are obligated to advise the appropriate authorities or officials when they become aware of any information, behavior, or conditions that may pose a security concern or that raise doubts whether a co-worker’s eligibility or access to classified information or assignment to sensitive duties is consistent with national security. If it is proven that an employee failed to report facts about a co-worker, an adverse national security eligibility action may be initiated against the employee who failed to report it.

(14) All commanders, to include supervisors, and installation support personnel will ensure derogatory information developed through personnel, law enforcement, or judicial punishment is forwarded to the commander through the supporting security manager. The supporting security manager will follow the incident reporting procedures in paragraph 8-7.

2. Security Education

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

b. Personnel assigned to sensitive duties must receive initial security briefing and annual refresher briefings on the national security implications of their duties and their individual responsibilities. These briefings will emphasize the individuals' responsibility to meet the standards and criteria for security eligibility per reference (b). Along with understanding the prohibitions against improperly handling classified information, personnel must understand the continued trustworthiness expectations placed upon them. This is essential if individuals are to recognize and properly respond to security issues.

c. Annual refresher briefings must advise personnel of pertinent security requirements for the protection of classified information and must inform personnel of security standards required of all individuals who access classified information. The briefing must emphasize the avenues open to personnel should they require assistance or otherwise have difficulty or concerns in maintaining trustworthiness standards.

d. Training topics include: DISS and e-App, orientation, indoctrination, initial briefings, refresher briefings, debriefings, termination briefings, travel briefings, foreign contact briefings, and intelligence threat briefings.

e. For assistance in meeting security education and training program requirements, visit the DCSA Center for

Development of Security Excellence (CDSE) website at http://www.cdse.edu. The CDSE website includes personnel security courses, job aids, reference guides, and webinars addressing the national security process, DISS, e-APP, and various "security shorts."

3. Employee Education and Assistance Program

a. The Commander will establish a program to help employees with questions or concerns regarding issues that may affect their ability to remain eligible for access to classified or assignment to sensitive positions to educate employees about personnel security responsibilities and to inform employees about guidance and assistance programs available. The education and assistance program will address issues that may affect employees' eligibility for access to classified information, or assignment to a sensitive position, and will include assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse issues.

b. Commands should act to identify individuals with personal issues at an early stage and guide them to programs designed to counsel and assist them. The goal is to assist individuals while there is still a reasonable chance of precluding a long-term employment or security clearance-related issue.

4. Performance Evaluation System

a. For Original Classification Authorities, security managers, security specialists, and all other personnel whose duties significantly involve the creating, handling, or management of classified information, refer to reference (d) regarding the performance contract or rating system that will include the management of classified information as a critical element or item to be evaluated. Guidelines on performance management are published by the Office of the Deputy Assistant Secretary of the Navy (Civilian Personnel/Office of Civilian Human Resources (ODASN (CP/CHR)). Questions may be addressed to the local HRO or the ODASN(CP/CHR) Code DP2.

b. In addition, supervisors will comment on the continued security clearance eligibility of subordinates who have access

to classified information in conjunction with regularly scheduled performance appraisals. To accomplish this requirement, commands may instruct supervisors to comment in writing, or to include statements on performance appraisal forms and/or separate correspondence addressed to security officials. The intent is to encourage supervisors to refer security concerns as soon as they become apparent, to provide supervisors an opportunity to annually assess their employees regarding continued eligibility to access classified information and for supervisors to be accountable for fulfilling their responsibilities.

5. Command Continuous Evaluation and Reporting Requirements. Commands shall report information to the DoD CAF via JPAS or successor system when unfavorable information as identified in reference (b) becomes available concerning an individual who has been granted access to classified information or assigned to sensitive duties. Commands will report all information per reference (b) without attempting to apply or consider any mitigating factors that may exist.

6. Additional Reporting Requirements for Individuals with Access to SCI Information. Individuals with access to SCI information will comply with reporting requirements identified in reference (k).

7. Financial Disclosure

a. Individuals who have been identified by their respective DoD Component head must file with their respective DoD Component a financial disclosure report in accordance with reference (k).

b. Financial disclosure information will be reported using SF 714, “Financial Disclosure Report,” or an equivalent form approved by the Security Executive Agent.

c. Failure to submit required financial information may result in the withdrawal of access to classified information.

8. Post-Adjudicative Issues

a. Upon receipt of a report of adverse information from any source, an adjudicator will evaluate the report and determine whether post-adjudicative actions are required. If the

adjudicator's review determines the reported information is not adequate or detailed enough to make an eligibility determination, the adjudicator may employ authorized means (e.g., requests for special investigations, interrogatories, contacts with subjects and employers, requests for information from security professionals, requests for medical or psychological evaluation, and record searches) to obtain additional information to make an eligibility determination.

b. Unfavorable information (e.g. government travel card misuse, abuse, or fraud, and administrative or disciplinary action taken as a result of management review or investigation) is reported to the appropriate security, law enforcement, or CI professionals for appropriate action. Upon coordination with CI and law enforcement professionals as necessary, unless directed otherwise by supporting CI professional, the incident report will be forward to the adjudication facility via JPAS.

c. The command may determine that the developed information is significant enough to require suspension to classified information or assignment to sensitive duties if they believe the behavior causes doubts about whether the individual's continued access is in the best interest of national security. Access to classified information or assignment to sensitive duties may be restored following supporting the DoD CAF's favorable national security determination. Suspension action must be accomplished in accordance with paragraph 9-7. When suspending SCI access, reference (k) procedures apply.

d. A command report of suspension of access for cause will automatically result in the suspension of the individual's clearance eligibility by the DoD CAF.

(1) Once clearance eligibility is suspended (or the individual is debriefed from SCI access for cause), the individual may not be granted access (or considered for re-indoctrination into SCI access) until clearance eligibility has been re-established by the DoD CAF.

(2) In cases where unfavorable information was developed at the local command and subsequently resolved by local investigation or inquiry, commands must notify the DoD CAF of the inquiry results. Commands may request temporary clearance eligibility. Temporary clearance eligibility authorization will

be at the DoD CAF discretion and is usually only possible if the local inquiry developed the necessary mitigation and there are no other unresolved security issues or other related pending inquiries or investigations.

e. The DoD CAF will evaluate and adjudicate all reported information and promptly notify the command of the determination regarding the individual's continued eligibility for access to classified information (including SCI access) and/or assignment to sensitive duties. However, if issues have not been resolved within 20 calendar days, action must be taken in accordance with reference (b). When unfavorable information relates to a contractor employee, the USD (I) and the VROC have the authority to take interim suspension action in accordance with reference (y), reference (z), and reference (aa).

f. If the reported information is incomplete or too limited to allow adjudication, the DoD CAF may either request that the command provide additional information or the necessary investigation request forms in order to open an investigation to resolve outstanding or missing information.