

**LESSON TOPIC 7.1****Personnel Security Policy****REFERENCES**

SECNAV M-5510.30, Chapters 5, 6, 7, 8, 9, and Appendix F  
Title 5, Code of Federal Regulation (CFR) 732.201

**LESSON****A. Sensitive National Security Positions (PSP 5-1 thru 5-3)**

## 1. Basic Policy

- a. Concerned with the protection of the nation from foreign aggression or espionage
- b. DON IT positions - Incumbent has access to DON IT systems or has IT-related duties with varying degrees of independence, privilege, access and/or impact on sensitive data and information - DON IT position levels:
  - IT-DAA - Exceptional privilege/control
  - IT-I - Privileged access
  - IT-II - Limited Privilege
  - IT-III - No Privilege, no sensitive information

NOTE: Record sensitivity and IT position determinations in JPAS (Most are sensitive)

2. CO will designate each Sensitive Position at one of three sensitivity levels (**PSP 5-2.2**)

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

## 3. Non-Sensitive positions - Have no potential for impact and/or damage as duties have limited relation to command mission

4. Criteria for Designating Sensitivity Level
  - Special-Sensitive (SS) - Agency head determines, also includes IT-DAA
  - Critical-Sensitive (CS) - Any position which includes: Access to Top Secret; Policy making or policy determining positions; Development of war plans, policies, or special operations of war; Investigative duties or making personnel security Determinations; Positions of public trust/contact of highest degree; I-IT (high risk) positions; and Any other positions designated by SECNAV or designee
  - Noncritical-Sensitive (NSP) - Any position which includes: Access to Secret and Confidential; AA&E duties, safeguarding DON personnel or property; Education/orientation of DOD personnel; Design, operation or maintenance of IDS systems; IT-II (Moderate Risk) Positions; and All other positions designated by SECNAV or designee
  - Non-sensitive (NS) - All other civilian positions designated as non-sensitive, including IT-III positions
5. Position Designation Decision Record - Maintained by Security Manager to identify:
  - Position Sensitivity Level
  - Required Investigation
  - Appropriate level of access to classified material required
  - Whether the position involves an IT risk

**B. Suitability for Civilian Employment (PSP 5-4)**

1. Suitability means "fitness" for employment
2. Office of Personnel Management (OPM) is responsible for establishing the program for investigating and adjudicating the suitability for federal employment.
3. OPM has delegated authority to adjudicate suitability to the Secretary of the Navy.

4. Suitability adjudications - command responsibility.  
(Based on standards and criteria established by OPM and contained in Title 5 CFR 731)
5. All completed investigations are forwarded to DOD CAF.
  - a. DOD CAF is delegated authority to make *de facto* suitability determinations on investigations closed without "actionable" issue. (A favorable security determination equates to a favorable suitability determination)
  - b. When investigation indicates "Actionable Issues", completed investigation forwarded to requesting command for a suitability determination. If command makes a:
    - Favorable suitability determination - Package will be returned to DOD CAF to make a security eligibility determination.
    - Unfavorable suitability determination, it remains a personnel action and no DOD CAF action is required.

#### **C. Trustworthiness Determinations**

1. Commanding Officer has prerogative to request Trustworthiness NAC (non-military) for duties not requiring access but if performed by untrustworthy persons could jeopardize safety/security. **(PSP 5-1)**
2. Public trust positions do not include national security positions and commands determine suitability (there is no DOD CAF action) **(PSP 5-1)**
3. Contractor Employees - A Facility Access Determination (FAD) will be included in contract specifications when trustworthiness determinations will be required on contractor employees **(PSP 9-20)**
4. Commanding Officer will use the Adjudicative Guidelines (CNO ltr 5520 Ser 09N2/6U871220 of 12 Sep 06) to guide determinations in above situations - Commanding Officers decision is final **(PSP 5-4)**

#### **D. Suitability to Serve in the Military (PSP 6-5)**

1. Determined after completion of personnel security investigation for:
  - Enlisted: Initially by recruiters, contingent on investigation results
  - Officers: USN - BUPERS; USMC - CMC
2. Authority to deny acceptance or retention
  - Non-loyalty issues - BUPERS/CMC
  - Loyalty issues - SECNAV

**E. Citizenship (PSP 5-6 and 7-8)**

1. Only U.S. citizens are eligible for security clearance, assignment to sensitive duties or access to classified information
  - a. No distinction is made between those who are U.S. citizens by birth, U.S. Nationals, and those who have derived U.S. citizenship or are naturalized  
  
(For security/assignment purposes, a person born in Puerto Rico, Guam, American Samoa, Northern Mariana Islands or U.S. Virgin Islands (if either parent is or was a U.S. citizen) is considered a U.S. citizen
  - b. Non U.S. citizens in Sensitive Positions - DUSN(PPO&I) must approve assignment to sensitive positions without access. (See PSP Exhibit 5B for waiver request procedure)
2. Dual citizenship - Not an automatic disqualifier for a clearance or assignment to sensitive or designated IT positions, however, it raises foreign influence and foreign preference concerns. No interim access or temporary assignment to sensitive duties.
3. Sensitive IT Positions - U.S. citizenship is a basic condition for assignment
  - a. Effective Oct 2006 DON non-U.S. citizens will **NOT** be permitted to be assigned or continued assignment to IT-DAA, IT-I and IT-II positions  
NOTE: See Exhibit 5B for waiver request format for sensitive positions with IT access

- b. IT-III Nonsensitive Positions - If access by non-U.S. citizens is necessary for mission accomplishment then those users will be strictly limited and have access only to information specifically entitled to and nothing else
- 4. Verification of U.S. citizenship required for assignment to sensitive position or access to classified material on personnel who are:  
**(PSP Appendix F)**
  - a. First time candidates
  - b. Candidates for clearance at a higher level than currently held
  - c. Officers - Officers must show proof of citizenship to be commissioned
  - d. Enlisted - DD 1966, Application for Enlistment - Armed Forces of the United States indicates documents cited at recruitment indicating citizenship.
  - e. Civilians - If hired after 1986 - had to show proof of U.S. citizenship. Previously hired employees were not required to submit proof of U.S. citizenship
- 5. Documentation required to prove U.S. citizenship can be found in PSP Appendix F
- 6. All documents submitted as evidence of birth must be original documents or certified copies.

**F. Clearance and Sensitive Assignment Eligibility Determinations**

- 1. Basic Policy **(PSP 7-1)**
  - a. Security clearance eligibility standards are based on the individual's loyalty, reliability and trustworthiness. (These standards apply to all U.S. Government civilian and military personnel, consultants, contractors, and other

individuals who require access to classified information or assignment to sensitive duties.)

- b. Access to classified information or assignment to sensitive duties must be consistent with the interests of national security.
- c. Determinations made on all favorable and unfavorable information per Adjudicative Guidelines (CNO ltr 5529 Ser 09N2/16U871220). (Final determination - Result of an overall common sense "whole person" adjudication.)
- d. Adjudicative guidelines used for determinations of security clearance eligibility are the same guidelines applied when determining eligibility to occupy a sensitive position.
- e. Once established, eligibility
  - Remains valid provided individual continues compliance with personnel security standards and has no break in service over 24 months
  - Does not expire and is not invalidated by overdue reinvestigation

## 2. Eligibility Prohibitions (PSP 7-8)

- a. Non-U.S. citizens
- b. Holding a current foreign passport

NOTE: To eliminate this as a disqualifier, individual may return foreign passport to the appropriate country embassy or consulate or, if impractical, may elect to destroy the foreign passport as witnessed by a DON security official (PSP 8-3)

- c. Position does not require eligibility
- d. Individuals identified under the "Bond Amendment" which precludes the initial granting or renewal of security clearance eligibility by DOD for personnel with access to Special Access Programs (SAP), Restricted Data (RD), or Sensitive compartmented Information (SCI) paragraphs (1),

(2) and (3) below apply and for all personnel paragraph (4) below applies: **(CNO ltr 5529 ser N09N2/8U223147 of 7 Jul 08, Interim guidance for the Implementation of Public Law 110-181, Section 2002 (The Bond Amendment) Regarding Adjudication of Security Clearances)**

- (1) Convicted of crimes, and incarcerated for not less than one year
  - (2) Discharged or dismissed from the Armed Forces under dishonorable conditions
  - (3) Determined to be mentally incompetent, as determined by competency proceedings conducted in a court or administrative agency with proper jurisdiction
  - (4) Unlawful user of a controlled substance or is an addict
- e. Members of Congress (Access may be granted as required for performance of duties)
  - f. Members of the U.S. Supreme Court, Federal judiciary and Supreme Courts (Access may be granted to extent necessary to adjudicate assigned cases)
3. Program Authority - Authority to determine eligibility for access to classified information or assignment to sensitive duties is vested in SECNAV and is delegated as follows: **(PSP 7-2)**
    - a. DUSN(PPO&I) will:
      - Issue DON Personnel Security Policy
      - Assign responsibilities for overall management of the PSP
    - b. Director, DOD CAF will
      - Adjudicate relevant information to determine security clearance eligibility and/or assignment to sensitive national security positions
      - Document personnel security determinations in

## JPAS

- Assist DON commands with queries regarding status of investigations at OPM

## c. Commanding Officers will:

- Request and monitor PSIs on command personnel
- Authorize, grant, limit and control access to classified information
- Ensure JPAS accurately reflects data on command personnel
- Maintain complete and accurate personnel security records
- Continuously evaluate command personnel for continued access to classified information - Notify DOD CAF of any derogatory information
- Coordinate personnel security eligibility determinations as appropriate
- Ensure personnel are referred to command assistance programs, if needed

## d. Employees will:

- Fully and accurately complete PSIs
- Be aware of personnel security eligibility standards and advice local security officials of anything which could effect eligibility

## 4. Responsibilities for critical personal and requirements data:

## a. Civilian Personnel/EEO will:

- Ensure personnel security requirements are identified to JPAS
- Ensure personnel identifying data is accurately reflected and updated in DCPDS
- Ensure that position sensitivity is accurately reflected and updated in DCPDS
- Coordinate with DUSN(PPO&I) and DOD CAF on all matters regarding assignment of civilians to sensitive national security positions

## b. DUSN(PPO&amp;I) and CMC will:

- Ensure personnel security requirements for military members are properly coded in military

- personnel data systems (which update JPAS)
  - Ensure PID data is accurately reflected and updated in military personnel data systems
  - Notify commands of eligibility and/or investigative requirements associated with transfers to new assignments
  - Coordinate with DUSN(PPO&I) and DOD CAF on all matters involving personnel security eligibility determinations on military members
5. Adjudicative Officials - A minimum level of review is required for all personnel security determinations **(PSP 7-5)**
- a. Commanding Officer will ensure command evaluations of unfavorable information is done by the Security Manager
  - b. DOD CAF adjudicative level requirements:
    - (1) SSBI/PR/SII
      - Favorable investigations=GS-9/11 or 0-2/3
      - Unfavorable Investigations undergo at least 2 levels of review, second must be by GS-11/12 or 0-3/4
    - (2) NACLC/ANACI
      - Favorable investigations=GS-7 or 0-1
      - Unfavorable=GS-9/11 or 0-3
    - (3) Unfavorable Continuous Evaluation Program (CEP) - Reviewed by an adjudicative official GS7/9 or 0-1/2 with second review level by a GS-11/12 or 0-4/5
    - (4) LOI/LOD - The LOI to deny or revoke will be approved and signed by an adjudicative official GS-12/13 or 0-4/5. The final notification of unfavorable personnel security determination (LOD) will be approved an adjudicative official of GS-14/15 OR 0-5/6

**G. Continuous Evaluation**

1. Means of monitoring behavior to ensure everyone who has access to classified information remains eligible **(PSP 10-1)**

2. Responsibilities: **(PSP 10-1)**

a. Commanding Officer - Establish and administer a program for continuous evaluation

NOTE: Program will rely on all personnel within command to report questionable or unfavorable information, which may be relevant to a security clearance determination.

b. Individuals - Report and seek assistance for any incident which could affect their continued eligibility for access

c. Co-Workers - Have an obligation to advise supervisor or appropriate security official when they become aware of information with potential security clearance significance

d. Supervisors/Managers - In a unique position to recognize problems early and react appropriately to ensure balance maintained regarding individual's needs and national security issues

3. Keys to Active Continuous Evaluation Program are security education and positive reinforcement of reporting requirements to include management support, confidentiality and Employee assistance Program referrals

4. Employee Assistance Programs - Inform employees about guidance and assistance programs available in command and guide individuals with personal issues to program **(PSP 10-3)**

5. Reports of Unfavorable Information - Commands will: **(PSP 10-5)**

a. Report unfavorable information as identified in the PSP Exhibit 10A, Continuous Evaluation Check

Sheet to DOD CAF using the Report Incident link  
JPAS (**PSP Exhibit 10A**) (See figure 7.1-1)

NOTE: Commands can use the Report Incident link in JPAS to just report derogatory information or to report derogatory and CO's suspension of access for cause (which will result in suspension of eligibility)

**Report to DOD CAF:**

1. Involvement in activities or sympathetic association with persons which/who unlawfully practice or advocate overthrow or altercation of the U.S. by unconstitutional means.
2. Foreign influence concerns/close personal association with foreign nationals or nations.
3. Foreign citizenship (dual citizenship) or foreign monetary interests.
4. Sexual behavior that is criminal or reflects a lack of judgment or discretion.
5. Conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations or unwillingness to cooperative with security clearance processing.
6. Unexplained affluence or excessive indebtedness.
7. Alcohol abuse.
8. Illegal or improper drug use/involvement.
9. Apparent mental, emotional or personality disorder(s).
10. Criminal conduct.
11. Noncompliance with security requirements.
12. Engagement in outside activities which could cause a conflict of interest.
13. Misuse of Information Technology Systems.

**Figure 7.1-1. Reporting requirements**

- b. Report unfavorable information without any mitigating factors that may exist
- c. Upon receipt of derogatory information, determine whether to suspend/limit access or reassign to non-sensitive duties
- d. Reports to DOD CAF should include the following information (if available):
  - Nature and seriousness of the conduct
  - Circumstances surrounding the conduct
  - Frequency and how recently conduct occurred
  - Age of individual at time of the conduct
  - Voluntariness or willfulness of the individual's participation or conduct
  - Knowledge individual had of consequences involved
  - Motivation for the conduct
  - How command became aware of the information
  - Actions individual has taken to correct issue, including medical treatment, counseling, lifestyle changes, or other corrective actions
  - Stability of individual's lifestyle or work performance, including demonstrative examples
  - Cooperation on the part of the individual in following medical/legal advice or assisting in command efforts to resolve the security issue