§ 156.5 National security positions.

(a) Procedures. The objective of the PSP is to ensure persons deemed eligible for national security positions remain reliable and trustworthy.

1 Duties considered sensitive and critical to national security do not always involve classified activities or classified matters. Personnel security procedures for national security positions are set forth in E.O. 12968, as amended; E.O. 10865, 32 CFR parts 154–155; ICD 704; and DoD Regulation 5220.22-R. The specific procedures applicable in each case type are set forth in DoD issuances.

2 Employees with access to automated systems that contain active duty, guard, or military reservists' personally identifiable information or information pertaining to Service members that are otherwise protected from disclosure by section 552a of title 5 United States Code, may be designated as national security positions within DoD, where such access has the potential to cause damage to national security.

(b) Sensitive Compartmented Information (SCI) Eligibility. Investigative and adjudicative requirements for SCI eligibility shall be executed in accordance with this part and ICD 704.

(c) Adjudication. (1) Personnel security criteria and adjudicative standards are described in E.O. 12968, as amended; 32 CFR parts 147, 154 and 155; ICD 704; and DoD Regulation 5220.22-R, as applicable, in accordance with Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.

(2) When an unfavorable personnel security determination is rendered:

(i) Individuals cannot be appointed or assigned to national security positions.

(ii) An individual currently occupying a national security position will be immediately removed from the national security position and placed, in accordance with agency policy, in an existing non-sensitive position if available. Placement in a non-sensitive position requires compliance with employment suitability standards. The national security position is not to be modified or a new position created to circumvent an unfavorable personnel security determination. The individual is to be placed in an appropriate status, in accordance with agency policy, until a final security determination is made.

(iii) To ensure consistency and quality in determinations of eligibility for national security positions, adjudicators must successfully complete the full program of professional training provided by the DSS Center for Development of Security Excellence (or equivalent training) and be certified through the DoD Professional Certification Program for Adjudicators within 2 years of program implementation or, for new hires, within 2 years of eligibility for certification testing.

(d) Appeal Procedures—Denial or Revocation of Eligibility. Individuals may elect to appeal unfavorable personnel security determinations in accordance with the procedures set forth in E.O. 12968, as amended; parts 154 and 155 of 32 CFR; ICD 704, and DoD Regulation 5220.22-R as applicable or as otherwise authorized by law.

(e) Polygraph. Under certain conditions, DoD Components are authorized to use polygraph examinations to resolve credible derogatory information developed in connection with a personnel security investigation; to aid in the related adjudication; or to facilitate classified access decisions.
(f) Continuous Evaluation. All personnel in national security positions shall be subject to continuous evaluation.

(g) Financial Disclosure. DoD Component implementation of the electronic financial disclosure requirement, consistent with E.O. 12968, shall be completed by the end of calendar year 2012.

(h) Reciprocal Acceptance of Eligibility Determinations. (1) DoD reciprocally accepts existing national security eligibility determinations or clearances from other government agencies in accordance with E.O. 13467, OMB Memorandums “Reciprocal Recognition of Existing Personnel Security Clearances” dated December 12, 2005 (Copies available on the Internet at http://www.whitehouse.gov/omb) and July 17, 2006 (Copies available on the Internet at http://www.whitehouse.gov/omb).

(2) Reciprocity for SCI eligibility shall be executed in accordance with ICD 704 and associated Director of National Intelligence guidance.

(3) Personnel who have been determined eligible for national security positions should not be subjected to additional security reviews, completion of a new security questionnaire, or initiation of a new investigative check, unless credible derogatory information that was not previously adjudicated becomes known, or the previous adjudication was granted by a condition, deviation, or waiver pursuant to provisions of OMB Memorandums “Reciprocal Recognition of Existing Personnel Security Clearances” dated December 12, 2005, or there has been a break in service of more than 24 months. Exceptions for access to SCI or special access programs are listed in the OMB Memorandums “Reciprocal Recognition of Existing Personnel Security Clearances” dated July 17, 2006.

(i) National Security Agency (NSA)/Central Security Service (CSS). Employees, contractors, military assignees, and others with similar affiliations with the NSA/CSS must maintain SCI eligibility for access to sensitive cryptologic information in accordance with 50 U.S.C. chapter 23.

(j) Wounded Warrior Security and Intelligence Internship Program. PSIs in support of wounded warriors may be submitted and processed regardless of the time remaining in military service. Investigations will be accelerated through a special program code established by the Office of the USD(I) to ensure expedited service by the investigating and adjudicating agencies.

(1) Category 2 wounded, ill, or injured uniformed service personnel who expect to be separated with a medical disability rating of 30 percent or greater may submit a PSI for Top Secret clearance with SCI eligibility prior to medical separation provided they are serving in or have been nominated for a wounded warrior internship program.

(2) The investigations will be funded by the DoD Component that is offering the internship. If the DoD Component does not have funds available, the Military Service in which the uniformed service personnel served may choose to fund the investigation.

§ 156.6 Common access card (CAC) investigation and adjudication.

(a) General. Individuals entrusted with access to Federal property, information systems, and any other information bearing on national security must not put the Government at risk or provide an avenue for terrorism.

(1) All individuals requiring a CAC must meet credentialing standards of OPM Memorandum, “Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD–12.” For those individuals who are subject to an interim credentialing decision before a security, suitability, or equivalent adjudication is completed, the OPM credentialing standards will be the basis for issuing or denying a CAC. The subsequent credentialing decision will be made upon receipt of the completed investigation from the ISP.

(2) If an individual is found unsuitable for employment in a covered position under 5 CFR 731.101, ineligible for access to classified information under E.O. 12968, or disqualified from appointment in the excepted service or from working on a contract, the unfavorable decision is a sufficient basis for nonissuance or revocation of a CAC, but does not necessarily mandate this result.

(b) Investigation. A favorably adjudicated National Agency Check with