**DEPARTMENT OF DEFENSE** **BILLING CODE 5001-06**

**Office of the Secretary**

**32 CFR Part 156**

**[DOD-2008-OS-0160]**

**RIN 0790-AI42**

**Department of Defense Personnel Security Program (PSP)**

**AGENCY:** Department of Defense.

**ACTION:** Final rule.

**SUMMARY:** This rule updates policies and responsibilities for the Department of Defense (DoD) Personnel Security Program (PSP) in accordance with the provisions of current U.S. Code, Public Laws, and Executive Orders (E.O.). This rule establishes policy and assigns responsibilities related to the operation of the DoD PSP, including investigative and adjudicative policy for determining eligibility to hold a national security position. This rule also establishes investigative and adjudicative policy for the Department's personal identity verification (PIV) credential.

**EFFECTIVE DATE:** This rule is effective [INSERT 30 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER].

**FOR FURTHER INFORMATION CONTACT:** Dr. Kelly Buck, (703) 604-1130

**SUPPLEMENTARY INFORMATION:**

**Executive Summary**

**I. Purpose and Legal Authority for this Rule**

This rule updates policies, assigns responsibilities, and prescribes procedures for the Department of Defense (DoD) Personnel Security Program (PSP) in accordance with the

provisions of current U.S. Code, Public Laws, and Executive Orders (E.O.). This rule establishes PSP policy related to the operation of the DoD PSP, including investigative and adjudicative policy for determining eligibility to hold national security positions. This rule also establishes Homeland Security Presidential Directive (HSPD)-12 investigative and adjudicative policy for the Department's personal identity verification (PIV) credential. Legal authorities for this rule are E.O. 12968, as amended; E.O. 10450, as amended; E.O. 10865, as amended; E.O. 13526; E.O. 12829, as amended; E.O. 13467; E.O. 13488; E.O. 12333, as amended; 5 U.S.C. 301 and 7532; section 1072 of Public Law 110-181, as amended; 15 U.S.C. 278g-3; 40 U.S.C. section 11331; 10 U.S.C. 1564; 50 U.S.C.; 3343; 5 CFR parts 731, 732 and 736, and Homeland Security Presidential Directive (HSPD)-12.

**II. Summary of Major Provisions of this Rule**

The DoD Directive (DoDD) 5200.2, Personnel Security Program (PSP), codified at 32 CFR Part 156, was issued April 9, 1999. The Department is reissuing the DoD Directive as a DoD Instruction to update existing policy regarding operation of the DoD Personnel Security Program and to establish new policy implementing HSPD-12.

The updated policy incorporates Joint Security and Suitability Reform Team efforts to revise Executive branch-wide policy and procedures needed to implement reform. The Intelligence Reform and Terrorism Prevention Act of 2004, E.O. 13467, E.O. 12968, as amended, E.O. 10865, and HSPD-12 are some of the current Federal laws, directives and statutes that affect the DoD PSP. Since this rule was last published, additional executive orders have been issued directing alignment of security, suitability and reciprocal acceptance of prior investigations and determinations.

The procedural guidance for the DoD PSP is currently being updated and will subsequently be proposed as a rule codified at 32 CFR Part 154. The investigative and adjudication procedural guidance for the DoD Federal PIV credential pursuant HSPD-12 is undergoing coordination and will also be proposed a separate rule.

**III. Costs and Benefits of this Rule**

This is an update to an existing rule regarding personnel security investigative and adjudicative policy and implements new department policy related to HSPD-12. The personnel security program has no discernable increase in anticipated costs and benefits as the program is being updated to conform to current national security guidance. The latter dealing with HSPD-12 is an unfunded mandate. However, this rule does not increase costs; rather it implements the requirements of HSPD-12 in the most efficient and effective manner possible by ensuring uniform implementation. The benefits inherent to both the personnel security and HSPD-12 programs enhance security as directed by the Intelligence Reform and Terrorism Prevention Act of 2004 and subsequent implementing policies.

**Public Comments**

The Department of Defense (DoD) published a proposed rule on February 2, 2011 (76 FR 5729). One comment was received and is addressed below:

Comment: Given the increasing use of DNA (deoxyribonucleic acid) as an investigatory tool by federal, state, and local law enforcement agencies, the DoD should consider requiring applicants to provide a DNA sample. That provided DNA sample would be profiled and compared to available databases. This would help insure that no

applicant for a clearance is a subject of an active federal, state, or local criminal investigation based on DNA evidence.

This would achieve the same end as the current collection of fingerprints from applicants that are run against Federal Bureau of Investigation databases. However, the additional use of DNA would recognize the greater prevalence of DNA evidence in criminal investigations.

I do note that DNA is distinctly different from fingerprints in that a search of databases may produce a result that does not link to the DoD clearance applicant but could instead provide a linkage to a familial relative of the applicant. This secondary issue would have to be examined by DoD and the legal community.

I also believe other federal agencies with similar personnel security programs should consider the collection of DNA samples from applicants to insure appropriate reciprocity of clearances between those agencies and DoD.

DoD Response: The Federal Government is looking into the feasibility of using biometric identifiers other than fingerprints in the security clearance process. However, any such requirement such as the suggested collection of DNA from clearance applicants would be covered in a separate rulemaking. As the comment correctly notes, such a policy would be best coordinated with the other federal agencies with personnel security programs to insure appropriate reciprocity of clearances between agencies.

Additional Changes by DoD: Other changes were made to the final rule from what was in the proposed due to additional coordination within the Department. These changes include:

(a) The title for § 156.5 has been changed from “Procedures-sensitive positions, duties, and classified access” to “National Security Positions” to incorporate the positions, duties, and access into one common phrase. The term is listed in the definitions section and its use in the part provides for ease of reading.

(b) Adjustments were made to the part to apply correct U.S. Code, Public Laws, or Executive Orders to the appropriate paragraph(s).

(c) Changes were made in the “Responsibilities” section to update the new title name for the Deputy Under Secretary of Defense for Intelligence and Security (previously known as the Deputy Under Secretary of Defense for HUMINT, Counterintelligence, and Security).

(d) Required responsibilities were also added for the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Under Secretary of Defense for Policy.

(e) Verbiage was added that prohibits the use of DoD adjudication systems of record for use as a pre-hiring tool. Additional language directs the removal of personnel from national security positions who have received unfavorable security determinations.

(f) Any other changes made to the part were made for ease and clarity of reading.

**Regulatory Procedures**

**E.O. 12866, “Regulatory Planning and Review'' and EO 13563, “Improving Regulation and Regulatory Review”**

It has been certified that 32 CFR Part 156 does not:

(1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition;

jobs; the environment; public health or safety; or State, local, or tribal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency;

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in these Executive Orders.

**Section 202, Public Law 104-4, "Unfunded Mandates Reform Act"**

It has been certified that 32 CFR Part 156 does not contain a Federal mandate that may result in the expenditure by State, local and tribal governments, in aggregate, or by the private sector, of $100 million or more in any one year.

**Public Law 96-354, "Regulatory Flexibility Act" (5 U.S.C. 601)**

It has been certified that 32 CFR Part 156 is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities.

**Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)**

It has been certified that 32 CFR Part 156 does not impose reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995.

**E.O. 13132, "Federalism"**

It has been certified that 32 CFR Part 156 does not have federalism implications, as set forth in E.O. 13132. This rule does not have substantial direct effects on:

(1) The States;

(2) The relationship between the National Government and the States; or

(3) The distribution of power and responsibilities among the various levels of Government.

List of Subjects in 32 CFR Part 156

Government employees, Security measures.

Accordingly, 32 CFR Part 156 is revised to read as follows.

**PART 156--DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM (PSP)**

Sec.



Authority: E.O. 12968, as amended; E.O. 10450, as amended; E.O. 10865, as amended; E.O. 13526; E.O. 12829, as amended; E.O. 13467; E.O. 13488; E.O. 12333, as amended; 5 U.S.C 301 and 7532.; section 1072 of Public Law 110-181, as amended; 15 U.S.C. 278g-3; 40 U.S.C. 11331; 10 U.S.C. 1564; 50 U.S.C. 3343; 5 CFR parts 731, 731.101, 732, and 736; and HSPD-12.

**§ 156.1 Purpose.**

This part updates policies and responsibilities for the DoD Personnel Security Program (PSP) consistent with E.O. 12968, as amended; E.O. 10450, as amended; E.O. 10865, as amended; E.O. 13526; E.O. 12829, as amended; E.O. 13467; E.O. 13488; E.O. 12333, as amended; 5 U.S.C. 301 and 7532; section 1072 of Public Law 110-181, as amended; 15 U.S.C. 278g-3; 40 U.S.C. 11331; 10 U.S.C. 1564; 32 CFR parts 147, 154 through 156; 50 U.S.C. 3343; 5 CFR parts 731, 731.101, 732 and 736; and HSPD-12.

**§ 156.2 Applicability.**

This part applies to the Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the “DoD Components”).

**§ 156.3 Policy.**

It is DoD policy that:

(a) The Department shall establish and maintain a uniform DoD PSP to the extent consistent with standards and procedures in E.O. 12968, as amended; E.O. 10450, as amended; E.O. 10865, as amended; E.O. 13526; E.O. 12829, as amended; E.O. 13467; E.O. 13488; E.O. 12333, as amended; 32 CFR parts 147, 154 through 156; 5 CFR parts 731, 731.101, 732 and 736; 5 U.S.C. 301 and 7532; section 1072 of Public Law 110-181, as amended; 15 U.S.C. 278g-3; section 11331 of 40 U.S.C.; 10 U.S.C. 1564; 50 U.S.C. 3343; and the Intelligence Community Directive Number 704 (ICD 704) (available on the Internet at http://www.dni.gov).

(b) DoD PSP policies and procedures shall be aligned using consistent standards to the extent possible; provide for reciprocal recognition of existing investigations and adjudications; be cost-effective, timely, and provide efficient protection of the national interest; and provide fair treatment of those upon whom the Federal Government relies to conduct the Nation's business and protect national security.

(c) Discretionary judgments used to determine eligibility for national security positions are an inherently governmental function and shall be performed by appropriately trained and favorably adjudicated Federal Government personnel or appropriate automated procedures.

(d) No negative inference may be raised solely on the basis of mental health counseling. Such counseling may be a positive factor that, by itself, shall not jeopardize the rendering of eligibility determinations or temporary eligibility for access to national security information. However, mental health counseling, where relevant to adjudication for a national security position, may justify further inquiry to assess risk factors that may be relevant to the DoD PSP.

(e) The DoD shall not discriminate nor may any inference be raised on the basis of race, color, religion, sex, national origin, disability, or sexual orientation.

(f) Discretionary judgments that determine eligibility for national security positions shall be clearly consistent with the national security interests of the United States. Any doubt shall be resolved in favor of national security.

(g) No person shall be deemed to be eligible for a national security position merely by reason of Federal service or contracting, licensee, certificate holder, or grantee status, or

as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

(h) No person shall be appointed or assigned to a national security position when an unfavorable personnel security determination has been rendered.

(i) Eligibility for national security positions shall be granted only to persons who are U.S. citizens for whom the investigative and adjudicative process has been favorably completed. However, based on exceptional circumstances where official functions must be performed prior to completion of the investigative and adjudicative process, temporary eligibility for access to classified information may be granted while the investigation is underway.

(j) As an exception, a non-U.S. citizen who possesses an expertise that cannot be filled by a cleared or clearable U.S. citizen, may hold a national security position or be granted a limited access authorization to classified information in support of a specific DoD program, project, or contract following a favorable security determination by an authorized adjudication facility.

(k) The DoD shall establish investigative and adjudicative policy and procedures to determine whether to issue, deny or revoke common access cards (CACs) in accordance with the standards of the Homeland Security Presidential Directive (HSPD)-12 (available in the Public Papers of the Presidents of the United States: George W. Bush (2004, Book II, page 1765) found on the Internet at http://www.gpo.gov/); Office of Management and Budget Memorandum (OMB) M-05-24 (available on the Internet at http://www.whitehouse.gov/omb); Federal Information Processing Standards Publication 201-1 (FIPS 201-1) or successor (available on the Internet at http://csrc.nist.gov/); 48

CFR, Chapter 1, Parts 1-99 (Federal Acquisition Regulation); 48 CFR, Chapter 2, Parts 201-253 (Defense Federal Acquisition Regulation Supplement), and the Office of Personnel Management (OPM) Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," dated July 31, 2008 (available on the Internet at http://www.opm.gov/), as applicable.

(l) Information about individuals collected as part of the investigative and adjudicative process shall be managed in accordance with applicable laws and DoD policies, including those related to privacy and confidentiality, security of information, and access to information.

**§ 156.4 Responsibilities.**

(a) The Under Secretary of Defense for Intelligence (USD(I)) shall:

(1) Develop, coordinate, and oversee the implementation of policy, programs, and guidance for the DoD PSP.

(2) In coordination with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and the General Counsel of the DoD (GC, DoD), develop policy for DoD personnel for the CAC personnel security investigation (PSI) and adjudication in accordance with HSPD-12; OMB Memorandum M-05-24; FIPS 201-1; and OPM Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12."

(3) In coordination with the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) and the GC, DoD, develop policy for contractor investigations for CAC adjudication, outside the purview of the National Industrial Security Program, under the terms of applicable contracts in accordance with HSPD-12;

OMB Memorandum M-05-24; FIPS 201-1; the Federal Acquisition Regulation; the Defense Federal Acquisition Regulation Supplement; and OPM Memorandum, “Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12.”

(4) Issue guidance implementing the policy in this part.

(b) The Deputy Under Secretary of Defense for Intelligence & Security (DUSD(I&S)), under the authority, direction, and control of the USD(I) shall:

(1) Ensure that the PSP is consistent, cost-effective, efficient, and balances the rights of individuals with the interests of national security.

(2) Develop and publish revisions to 32 CFR Part 154.

(3) Approve, coordinate, and oversee all DoD personnel security research initiatives and activities to improve the efficiency, effectiveness, and fairness of the DoD PSP.

(4) Ensure that the Defense Security Service (DSS) provides education, training, and awareness support to the DoD PSP.

(5) Serve as the primary contact between DoD, the Red Cross, United Service Organizations, and other organizations with direct DoD affiliation for all matters relating to the DoD PSP.

(6) When appropriate, approve requests for exceptions to the DoD PSP relating to national security eligibility requirements for access to classified information except North Atlantic Treaty Organization (NATO) classified information. Requests for exceptions involving access to NATO classified information shall be sent to the Office of the Under Secretary of Defense for Policy.

(7) Develop guidance, interpretation, and clarification regarding the DoD PSP as needed.

(8) Conduct oversight inspections of the DoD Components for implementation and compliance with DoD personnel security policy and operating procedures.

(9) In furtherance of coordinated Government-wide initiatives under E.O. 13467, develop a framework setting forth an overarching strategy identifying goals, performance measures, roles and responsibilities, a communications strategy, and metrics to measure the quality of security clearance investigations and adjudications to ensure a sound DoD PSP that will continue to meet the needs of DoD.

(c) The USD(AT&L) shall:

(1) Establish acquisition policy, procedures, and guidance, in coordination with the USD(I) that facilitate DoD Component compliance with the DoD PSP.

(2) Establish regulatory requirements within the Federal Acquisition Regulation and Defense Federal Acquisition Regulation for contracts and agreements that require non-DoD personnel to adhere to personnel security procedures in the performance of a contract or agreement.

(d) The Under Secretary of Defense for Policy (USD(P)) is the approval authority for requests for exceptions to the DoD PSP involving access to NATO classified information.

(e) The GC, DoD shall:

(1) Provide advice and guidance as to the legal sufficiency of procedures and standards involved in implementing the DoD PSP and exercise oversight of the established administrative due process procedures of the DoD PSP.

(2) Perform functions relating to the DoD PSP including the maintenance and oversight of the Defense Office of Hearings and Appeals (DOHA).

(f) The Heads of the DoD Components shall:

(1) Designate a senior agency official, consistent with the provisions of E.O. 12968, as amended, who shall direct and administer the DoD PSP consistent with this part.

(2) Comply with the policy and procedures regarding investigation and adjudication for CAC issuance and distribute this guidance to local and regional organizations.

(3) Provide funding to cover Component requirements for PSIs, adjudication, and recording of results to comply with the DoD PSP.

(4) Enforce requirements for prompt reporting of significant derogatory information, unfavorable administrative actions, and adverse actions to the appropriate personnel security, human resources, and counterintelligence official(s), as appropriate, within their respective Component.

(5) Perform functions relating to the DoD Security Professional Education Development Program to ensure the security workforce in their respective Component has the knowledge and skills required to perform security functional tasks.

(6) Provide requested information and recommendations, as appropriate, on any aspect of this part and the DoD PSP to the USD(I).

(7) Enforce the requirement that DoD personnel security adjudication system(s) of records, within their respective Components, shall only be used as a personnel security system of records and shall not be used as a pre-hiring screening tool.

**§ 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 and other types of protected information or assignment to national security positions. Adjudications of eligibility for national security positions, regardless of whether they involve access to classified information, must be made in accordance with the 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. A final security determination is the granting, denial or revocation by an appropriate central adjudications facility or an appeal board decision, whichever is later.

(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 the 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 uniform 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 non-issuance or revocation of a CAC, but does not necessarily mandate this result.

(b) Investigation. A favorably adjudicated National Agency Check with Inquiries (NACI) is the minimum investigation required for a final credentialing determination for CAC.

(1) An interim credentialing determination can be made based on the results of a completed National Agency Check or an Federal Bureau of Investigation National Criminal History Check (fingerprint check), and submission of a request for investigation (NACI or greater).

(2) Individuals identified as having a favorably adjudicated investigation on record, equivalent to (or greater than) the NACI do not require an additional investigation for CAC issuance.

(3) There is no requirement to reinvestigate CAC holders unless they are subject to reinvestigation for national security or suitability reasons as specified in applicable DoD issuances.

(4) Existing CAC holders without the requisite background investigation on record must be investigated in accordance with OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors," dated August 5, 2005.

(c) Adjudication. The ultimate determination whether to authorize CAC issuance or revoke the CAC must be an overall common-sense judgment after careful consideration of the basic and, if applicable, supplemental credentialing standards in OPM Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," each of which is to be evaluated in the context of the whole person. These standards shall be evaluated to determine if there is a reasonable basis to believe that issuing a CAC to the individual poses an unacceptable risk.

(1) Each case is unique and must be judged on its own merits. To the extent pertinent to the individual case, when evaluating the conduct, the adjudicator should consider: the nature and seriousness of the conduct, the circumstances surrounding the conduct, the recency and frequency of the conduct, the individual's age and maturity at the time of the conduct, contributing external conditions, and the presence or absence of rehabilitation or efforts toward rehabilitation.

(2) Final credentialing standards are:

(i) Basic Credentialing Standards. All CAC adjudications must apply the basic credentialing standards. CAC shall not be issued when a disqualifying factor cannot be mitigated.

(ii) Supplemental Credentialing Standards. The supplemental credentialing standards, in addition to the basic credentialing standards, shall apply generally to individuals who are not subject to adjudication for eligibility for a sensitive position or access to classified information, suitability for Federal employment or fitness. These standards may be applied based on the risk associated with the position or work on the contract.

(3) All interim and final adjudicative determinations shall be made by cleared and trained Federal Government personnel. Automated adjudicative processes shall be used to the maximum extent practicable.

(4) Adjudication decisions of CAC investigations shall be incorporated into the Consolidated Central Adjudication Facility as directed by the Deputy Secretary of Defense.

(5) CAC adjudicators must successfully complete formal training through a DoD adjudicator course from the DSS Center for Development of Security Excellence to achieve maximum consistency and fairness of decisions rendered.

(6) Federal Government credentialing standards do not prohibit employment of convicted felons who have been released from correctional institutions, absent other issues, if they have demonstrated clear evidence of rehabilitation.

(d) Appeals. CAC applicants or holders may appeal CAC denial or revocation.

(1) No separate administrative appeal process is allowed when an individual has been denied a CAC as a result of a negative suitability determination under 5 CFR Part 731, an

applicable decision to deny or revoke a security clearance, or based on the results of a determination to disqualify the person from an appointment in an excepted service position or from working on a contract for reasons other than eligibility for a Federal Credential as described in OPM Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12." If a later denial or revocation of a CAC results from an applicable denial or revocation of a security clearance, suitability decision, or other action for which administrative process was already provided on grounds that support denial or revocation of a CAC, no separate appeal for CAC denial or revocation is allowed.

(2) Initial civilian and contractor applicants who have been denied a CAC, and for whom an appeal is allowed under this paragraph, may elect to appeal to a three member board containing no more than one security representative from the sponsoring activity.

(3) Contractor employees who have had their CAC revoked, and for whom an appeal is allowed under this paragraph, may appeal to DOHA under the established administrative process set out in 32 CFR Part 155.

(4) Decisions following appeal are final.

(5) Individuals whose CACs have been denied or revoked are eligible for reconsideration 1 year after the date of final denial or revocation, provided the sponsoring activity supports reconsideration. Individuals with a statutory or regulatory bar are not eligible for reconsideration while under debarment.

(e) Foreign Nationals. Special considerations for conducting background investigations of non-U.S. nationals (foreign nationals) are addressed in OPM Memorandum, "Final

Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12." The following criteria shall be met prior to CAC issuance to foreign nationals:

(1) The background investigation must be completed and favorably adjudicated before issuing CACs to foreign nationals.

(2) Foreign nationals are not eligible to receive CAC on an interim basis.

(3) At foreign locations:

(i) Foreign national background investigations may vary based on standing reciprocity treaties concerning identity assurance and information exchange that exist between the United States and its allies. This includes foreign military, civilian, or contract support with a visit status and security assurance that has been confirmed, documented, and processed in accordance with USD(P) policy.

(ii) The type of background investigation may also vary based upon agency agreements with the host country when the foreign national CAC applicant (such as a DoD direct or indirect hire) has not resided in the United States for at least 3 of the past 5 years or is residing in a foreign country. The investigation must be consistent with NACI, to the extent possible, and include a fingerprint check against the Federal Bureau of Investigation (FBI) criminal history database, an FBI Investigations Files (name check) search, and a name check against the Terrorist Screening Database.

(4) At U.S.-based locations and in U.S. territories:

(i) Foreign nationals who have resided in the United States or U.S. territory for 3 years or more must have a NACI or greater investigation.

(ii) Components may delay the background investigation of foreign nationals who have resided in the U.S. or U.S. territory for less than 3 years until the individual has been in

the U.S. or U.S. territory for 3 years. When the investigation is delayed, the Component may, in lieu of a CAC, issue an alternative facility access credential at the discretion of the relevant Component official based on a risk determination.

(f) Recording Final Adjudication. Immediately following final adjudication, the sponsoring activity shall record the final eligibility determination (active, revoked, denied, etc.) in the OPM Central Verification System as directed by OPM Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," and maintain local records for posting in a DoD repository when available.

(g) Reciprocity of CAC Determinations. (1) The sponsoring activity shall not re-adjudicate CAC determinations for individuals transferring from another Federal department or agency, provided:

(i) Possession of a valid personal identity verification (PIV) card or CAC can be verified by the individual's former department or agency.

(ii) The individual has undergone the required NACI or other equivalent suitability, public trust, or national security investigation and received favorable adjudication from the former agency.

(iii) There is no break in service greater than 24 months and the individual has no actionable information since the date of the last completed investigation.

(2) Interim CAC determinations are not eligible to be transferred or reciprocally accepted. Reciprocity shall be based on final favorable adjudication only.

**§ 156.7 Definitions.**

These terms and their definitions are for the purposes of this part:

Continuous evaluation. Defined in section 1.3(d) of E.O. 13467.

Contractor. Defined in E.O. 13467.

Employee. Defined in E.O. 12968, as amended.

Limited access authorization. Defined in 32 CFR Part 154.

National security position. (1) Any position in a department or agency, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security.

(i) Such positions include those requiring eligibility for access to classified information.

(ii) Other such positions include, but are not limited to, those whose duties include:

(A) Protecting the nation, its citizens and residents from acts of terrorism, espionage, or foreign aggression, including those positions where the occupant's duties involve protecting the nation's borders, ports, critical infrastructure or key resources, and where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security;

(B) Developing defense plans or policies;

(C) Planning or conducting intelligence or counterintelligence activities, counterterrorism activities and related activities concerned with the preservation of the military strength of the United States;

(D) Protecting or controlling access to facilities or information systems where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security;

(E) Controlling, maintaining custody, safeguarding, or disposing of hazardous materials, arms, ammunition or explosives, where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security;

(F) Exercising investigative or adjudicative duties related to national security, suitability, fitness or identity credentialing, where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security;

(G) Exercising duties related to criminal justice, public safety or law enforcement, where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security; or

(H) Conducting investigations or audits related to the functions described in paragraphs (1)(ii)(B) through (G) of this definition, where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security.

(2) The requirements of this part apply to positions in the competitive service, positions in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and career appointments in the Senior Executive Service within the executive branch. Departments and agencies may apply the requirements of this part to other excepted service positions within the executive branch and contractor positions, to the extent consistent with law.

Unacceptable risk. Threat to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, privileged, proprietary, financial, or medical records; or to the privacy of data subjects, which will not be tolerated by the Government.

DATED: March 20, 2014.

AARON SIEGEL

Alternate OSD Federal Register

Liaison Officer

Department of Defense

[FR Doc. 2014-06544 Filed 03/31/2014 at 8:45 am; Publication Date: 04/01/2014]