(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.

PART 157—DOD INVESTIGATIVE AND ADJUDICATIVE GUIDANCE FOR ISSUING THE COMMON ACCESS CARD (CAC)

Sec.

AUTHORITY: HSPD–12, E.O 13467, E.O. 13488, FIPS 201–2, and OPM Memorandum.

SOURCE: 79 FR 55624, Sept. 17, 2014, unless otherwise noted.

§ 157.1 Purpose.

This part establishes policy, assigns responsibilities, and prescribes procedures for investigating and adjudicating eligibility to hold a Common Access Card (CAC). The CAC is the DoD personal identity verification (PIV) credential.

§ 157.2 Applicability.

This part applies to:

(a) the Office of the Secretary of Defense, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), 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 Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the ''DoD Components'').

(b) The Commissioned Corps of the U.S. Public Health Service (USPHS), under agreement with the Department of Health and Human Services, and the National Oceanic and Atmospheric Administration (NOAA), under agreement with the Department of Commerce.

§ 157.3 Definitions.

These terms and their definitions are for the purpose of this part.

Actionable information. Information that potentially justifies an unfavorable credentialing determination.

CAC. The DoD Federal PIV card.

Contractor. Defined in Executive Order 13467, ''Reforming Processes Related to Sustainability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information''.

Contractor employee fitness. Defined in E.O. 13467.

Debarment. A prohibition from taking a competitive service examination or from being hired (or retained in) a covered position for a specific time period..

Drugs. Mood and behavior-altering substances, including drugs, materials, and other chemical compounds identified and listed in 21 U.S.C. 801–830 (also known as ''The Controlled Substances Act of 1970, as amended'') (e.g., marijuana or cannabis, depressants, narcotics, stimulants, hallucinogens), and inhalants and other similar substances.

Drug abuse. The illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Employee. Defined in E.O. 12968, ''Access to Classified Information''.

Fitness. Defined in E.O. 13488, ''Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust''.

Fitness determination. Defined in E.O. 13488.

Logical and physical access. Defined in E.O. 13467.

Material. Defined in 5 CFR part 731.

Reasonable basis. A reasonable basis to believe occurs when a disinterested observer, with knowledge of the same facts and circumstances, would reasonably reach the same conclusion.

Terrorism. Defined in 19 U.S.C. 2331.

Unacceptable risk. A threat to the life, safety, or health of employees, contractors, vendors, or visitors; to the U.S. Government physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial, and medical records; or to the privacy rights established by The Privacy Act of 1974, as amended, or other law that is deemed unacceptable when making risk management determinations.

U.S. National. Defined in U.S. OPM Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD–12'' (available at *http://www.opm.gov/investigate/resources/final_credentialing_standards.pdf*).

§ 157.4 Policy.

It is DoD policy that:

(a) Individuals appropriately sponsored for a CAC consistent with DoD Manual 1000.13, Volume 1, ''DoD Identification Cards: ID Card Life-Cycle,'' January 23, 2014, (available at *http://www.dtic.mil/whs/directives/corres/pdf/*

100013_vol1.pdf) must be investigated and adjudicated in accordance with this part. Individuals not CAC eligible may be processed for local or regional base passes in accordance with Under Secretary of Defense for Intelligence (USD(I)) policy guidance for DoD physical access control consistent with DoD Regulation 5200.08–R, ''Physical Security Program'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf*) and local installation security policies and procedures.

(b) A favorably adjudicated National Agency Check with Inquiries (NACI) or equivalent in accordance with revised Federal investigative standards is the minimum investigation required for a final credentialing determination for a CAC.

(c) Individuals requiring a CAC must meet the credentialing standards in accordance with the U.S. Office of Personnel Management (OPM) Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD–12''; and U.S. Office of Personnel Management Memorandum, ''Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide (available at *http://www.opm.gov/investigate/resources/decision_making_guide.pdf*) and this part.

(d) A CAC may be issued on an interim basis based on a favorable National Agency Check or a Federal Bureau of Investigation (FBI) National Criminal History Check (fingerprint check) adjudicated by appropriate approved automated procedures or by a trained security or human resource (HR) specialist and successful submission to the investigative service provider (ISP) of a NACI, or a personnel security investigation (PSI) equal to or greater in scope than a NACI. Additionally, the CAC applicant must present two identity source documents, at least one of which is a valid Federal or State government-issued picture identification.

(e) The subsequent final credentialing determination will be made upon receipt of the completed investigation from the ISP.

(f) Discretionary judgments used to render an adjudicative determination for issuing the CAC are inherently governmental functions and must only be performed by trained U.S. Government personnel who have successfully completed required training and possess a minimum level of investigation (NACI or equivalent in accordance with revised Federal investigative standards). Established administrative processes in 32 CFR part 156 and DoD Directive 5220.6, ''Defense Industrial Personnel Security Clearance Review Program'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/522006p.pdf*) must be applied.

(g) Adjudications rendered for eligibility for access to classified information, eligibility to hold a sensitive position, suitability, or fitness for Federal employment based on a NACI or higher level investigation may result in a concurrent CAC decision for that position.

(h) Favorable credentialing adjudications from another Federal department or agency will be reciprocally accepted in accordance with conditions stated in the procedural guidance in this part. Reciprocity must be based on final favorable adjudication only.

(i) CAC applicants or holders may appeal CAC denial or revocation in accordance with the conditions stated in the procedural guidance in this part. Appeals must be processed as indicated in the procedural guidance in this part.

(j) Non-U.S. nationals at foreign locations are not eligible to receive a CAC on an interim basis. Special considerations for conducting background investigations of non-U.S. nationals are addressed in U.S. OPM Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD–12.'' An interim CAC may be issued to non-U.S. nationals in the U.S. or U.S. territories if they have resided in the U.S. or U.S. territory for at least 3 years, and they satisfy the requirements of paragraph (e) of this section and paragraph (a)(4)(ii)(A) of §157.6.

(k) Individuals who have been denied a CAC or have had a CAC revoked due to an unfavorable credentialing determination are eligible to reapply for a credential 1 year after the date of final adjudicative denial or revocation.

(l) Individuals with a statutory or regulatory bar are not eligible for reconsideration while under debarment, see paragraph (d)(6) of §157.6.

(m) The Deputy Secretary of Defense directed all reports of investigations conducted as required for compliance with Homeland Security Presidential Directive-12, ''Policy for a Common Identification Standard for Federal Employees and Contractors'' (available at *http://www.dhs.gov/homeland-security-presidential-directive-12*) to be sent to the consolidated DoD Central Adjudications Facility.

(n) When eligibility is denied or revoked, CACs shall be recovered whenever practicable, and shall immediately be rendered inoperable. In addition, agencies' physical and logical access systems shall be immediately updated to eliminate the use of a CAC for access.

§ 157.5 Responsibilities.

(a) The USD(I) must:

(1) In coordination with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and the General Counsel of the Department of Defense (GC, DoD), establish adjudication procedures to support CAC credentialing decisions in accordance with DoD Manual 1000.13, Volume 1, ''DoD Identification (ID) Cards; ID Card Life-Cycle''; U.S. Office of Personnel Management Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD–12''; U.S. Office of Personnel Management Memorandum, ''Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide; Office of Management and Budget Memorandum M–05–24, ''Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors'' (available at *http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf*); U.S. Office of Personnel Management Federal Investigations Notice Number 06–04, ''HSPD 12—Advanced Fingerprint Results'' (available at *http://www.opm.gov/extra/investigate/FIN06_04.pdf*); Homeland Security Presidential Directive-12, ''Policy for a Common Identification Standard for Federal Employees and Contractors''; 5 U.S.C. 552, 552a and 7313; Federal Information Processing Standards Publication 201–2, ''Personal Identity Verification (PIV) of Federal Employees and Contractors'' (available at *http://csrc.nist.gov/publications/PubsFIPS.html*); Executive Order 13467, ''Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information''; Executive Order 13488, ''Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust''; 15 U.S.C. 278g–3; 40 U.S.C. 11331; and U.S. Office of Personnel Management Federal Investigations Notice Number 10–05, ''Reminder to Agencies of the Standards for Issuing Identity Credentials Under HSPD–12'' (available at *http://www.opm.gov/investigate/fins/2010/fin10-05.pdf*) for issuing a CAC to Service members and DoD civilian personnel.

(2) In coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and the GC, DoD, establish adjudication procedures to support a CAC credentialing decision for contractors in accordance with the terms of applicable contracts and the references cited in paragraph (a)(1) of this section, the Federal Acquisition Regulation (available at *http://www.acquisition.gov/far/current/pdf/FAR.pdf*), and the Defense Federal Acquisition Regulation Supplement (available at *http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html*).

(3) Issue, interpret, and clarify CAC investigative and adjudicative guidance in coordination with the Suitability Executive Agent as necessary.

(b) The USD(P&R) must, in coordination with the GC, DoD, implement CAC PSI and adjudication procedures established herein as necessary to support issuance of a CAC to Service members and DoD civilian personnel in accordance with the references cited in paragraph (a)(1) of this section.

(c) The USD(AT&L) must, in coordination with the GC, DoD, implement CAC PSI and adjudication procedures

established by the USD(I) for contractors in accordance with the terms of applicable contracts and the references cited in paragraph (a)(1) of this section, Federal Acquisition Regulation, current edition; and Defense Federal Acquisition Regulation Supplement, current edition.

(d) The GC, DoD must:

(1) Provide advice and guidance as to the legal sufficiency of procedures and standards involved in adjudicating CAC investigations.

(2) Perform functions relating to the DoD Homeland Security Presidential Directive (HSPD)–12 Program in accordance with DoD Directive 5220.6, ''Defense Industrial Personnel Security Clearance Review Program'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/522006p.pdf*) and DoD Directive 5145.01, ''General Counsel of the Department of Defense'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/514501p.pdf*) including maintenance and oversight of the Defense Office of Hearings and Appeals (DOHA) and its involvement in contractor CAC revocations as specified in paragraph (b)(6)(i)(B) of §157.6 of this part.

(3) Coordinate on USD(P&R) implementation of CAC PSI and adjudication procedures, in accordance with the references cited in paragraph (a)(1) of this section, for Service members and DoD civilian personnel, and USD(AT&L) implementation of USD(I) procedures for CAC PSI and adjudication in accordance with the terms of applicable contracts and the references cited in paragraph (a)(1) of this section, Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement.

(e) The Heads of the DoD Components must:

(1) Comply with and implement this part.

(2) Provide resources for PSIs, adjudication, appeals, and recording of final adjudicative results in a centralized database.

(3) Require individuals sponsored for a CAC to meet eligibility requirements stated in DTM 08–003.

(4) Provide appeals boards for those individuals appealing CAC denial or revocation as specified in paragraph (b)(6)(i)(A) of §157.6.

(5) Enforce requirements for reporting of derogatory information, unfavorable administrative actions, and adverse actions to personnel security, HR, and counterintelligence official(s), as appropriate.

(6) Require all PSIs submitted for non-DoD personnel to be supported by and comply with DoD PIV procedures in contracts that implement requirements of paragraphs 4.1303 and 52.204–9 of Federal Acquisition Regulation, current edition.

(7) Require all investigations and adjudications required for non-DoD personnel to be in response to a current, active contract or agreement and that the number of personnel submitted for investigation and adjudication does not exceed the specific requirements of that contract or agreement while ensuring compliance with HSPD–12.

§ 157.6 Procedures.

(a) *CAC Investigative Procedures*—(1) *Investigative Requirements.* (i) A personnel security investigation (NACI or greater) completed by an authorized ISP is required to support a CAC credentialing determination based on the established credentialing standards promulgated by OPM Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD–12''.

(ii) 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.

(iii) 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.

(2) *Submission of Investigations.* Investigative packages must be submitted promptly by HR or security personnel to the authorized ISP. Fingerprints for CAC applicants must be taken by HR or security personnel. DoD Components using the OPM as the ISP may request advanced fingerprint check results in accordance with OPM Federal Investigations Notice Number 06–04.

(3) *Reciprocity.* (i) The sponsoring Component must not re-adjudicate CAC determinations for individuals

transferring from another Federal department or agency, provided:

(A) The individual's former department or agency verifies possession of a valid PIV.

(B) The individual has undergone the required NACI or other equivalent (or greater) suitability or national security investigation and received favorable adjudication from the former department or agency.

(C) There is no break in service 2 years or more and the individual has no actionable information since the date of the last completed investigation.

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

(4) *Foreign (Non-U.S.) Nationals.* DoD Components must apply the credentialing process and standards in this part to non-U.S. nationals who work as employees or contractor employees for the DoD. However, special considerations apply to non-U.S. nationals.

(i) *At Foreign Locations.* (A) DoD Components must initiate and ensure completion of a background investigation before applying the credentialing standards to a non-U.S. national at a foreign location. The background investigation must be favorably adjudicated before a CAC can be issued to a non-U.S. national at a foreign location. The type of background investigation may vary based on standing reciprocity treaties concerning identity assurance and information exchanges that exist between the U.S. and its allies or agency agreements with the host country.

(B) The investigation of a non-U.S. national at a foreign location must be consistent with a NACI, to the extent possible, and include a fingerprint check against the FBI criminal history database, an FBI investigations files (name check) search, and a name check against the terrorist screening database.

(ii) *At U.S.-Based Locations and in U.S. Territories (Other than American Samoa and Commonwealth of the Northern Mariana Islands).* (A) Individuals who are non-U.S. nationals in the United States or U.S. territory for 3 years or more must have a NACI or equivalent investigation initiated after employment authorization is appropriately verified.

(B) Non-U.S. nationals who have been in the United States or U.S. territory for less than 3 years do not meet the investigative requirements for CAC issuance. DoD Components may delay the background investigation of a Non-U.S. national who has been in the U.S. or U.S. territory for less than 3 years until the individual has been in the United States or U.S. territory for at least 3 years. In the event of such a delay, an alternative facility access identity credential may be issued at the discretion of the relevant DoD Component official, as appropriate based on a risk determination in accordance with DoD 5200.08–R, ''Physical Security Program'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf*) and U.S. Office of Personnel Management Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD–12.''

(C) The U.S. territories of American Samoa and the Commonwealth of the Northern Mariana Islands are not included in the ''United States'' as defined by the Immigration and Nationality Act of 1952, as amended (Pub. L. 82–414).

(5) *Investigations Acceptable for CAC Adjudication.* A list of investigations acceptable for CAC adjudication is located in the Table. These investigations are equivalent to or greater than a NACI. This list will be updated by the USD(I) as revisions to the Federal investigative standards are implemented.

TABLE—FAVORABLY ADJUDICATED INVESTIGATIONS ACCEPTABLE FOR CAC ADJUDICATION

Investigation	Description
ANACI	Access National Agency Check and Inquires.
BGI–0112	Upgrade Background Investigation (1–12 months from LBI).
BGI–1336	Upgrade Background Investigation (13–36 months from LBI).
BGI–3760	Upgrade Background Investigation (37–60 months from LBI).
BI	Background Investigation.

TABLE—FAVORABLY ADJUDICATED INVESTIGATIONS ACCEPTABLE FOR CAC ADJUDICATION—Continued

Investigation	Description
BIPN	Background Investigation plus Current National Agency Check.
BIPR	Periodic Reinvestigation of Background Investigation.
BITN	Background Investigation (10 year scope).
CNCI	Child Care National Agency Check plus Written Inquires and Credit.
IBI	Interview Oriented Background Investigation.
LBI	Limited Background Investigation.
LBIP	Limited Background Investigation plus Current National Agency Check.
LBIX	Limited Background Investigation—Expanded.
MBI	Moderate Risk Background Investigation.
MBIP	Moderate Risk Background Investigation plus Current National Agency Check.
MBIX	Moderate Risk Background Investigation—Expanded.
NACB	National Agency Check/National Agency Check plus Written Inquires and Credit Check plus Background Investigation Requested.
NACI	National Agency Check and Inquires.
NACLC	National Agency Check with Law and Credit.
NACS	National Agency Check/National Agency Check plus Written Inquires and Credit Check plus Single Scope B.I. Requested.
NACW	National Agency Check plus Written Inquires and Credit.
NACZ	National Agency Check plus Written Inquires and Credit plus Special Investigative Inquiry.
NLC	National Agency Check, Local Agency Check and Credit.
NNAC	National Agency Check plus Written Inquires and Credit Plus Current National Agency Check.
NSI	NSI—NACI/Suitability Determination.
PRI	Periodic Reinvestigation.
PRS	Periodic Reinvestigation Secret.
PRSC	Periodic Reinvestigation Secret or Confidential.
PPR	Phased Periodic Reinvestigation.
SPR	Secret Periodic Reinvestigation.
SSBI	Single Scope Background Investigation.
SSBI–PR	Periodic Reinvestigation for SSBI.

(b) *CAC Adjudicative Procedures*—(1) *Guidance for Applying Credentialing Standards During Adjudication*. (i) As established in Homeland Security Presidential Directive–12, credentialing adjudication considers whether or not an individual is eligible for long-term access to Federally controlled facilities and/or information systems. The ultimate determination to authorize, deny, or revoke the CAC based on a credentialing determination of the PSI must be made after consideration of applicable credentialing standards in OPM Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD–12.''

(ii) Each case is unique. Adjudicators must examine conditions that raise an adjudicative concern, the overriding factor for all of these conditions is unacceptable risk. Factors to be applied consistently to all information available to the adjudicator are:

(A) The nature and seriousness of the conduct. The more serious the conduct, the greater the potential for an adverse CAC determination.

(B) The circumstances surrounding the conduct. Sufficient information concerning the circumstances of the conduct must be obtained to determine whether there is a reasonable basis to believe the conduct poses a risk to people, property or information systems.

(C) The recency and frequency of the conduct. More recent or more frequent conduct is of greater concern.

(D) The individual's age and maturity at the time of the conduct. Offenses committed as a minor are usually treated as less serious than the same offenses committed as an adult, unless the offense is very recent, part of a pattern, or particularly heinous.

(E) Contributing external conditions. Economic and cultural conditions may be relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk if the conditions are currently removed or countered (generally considered in cases with relatively minor issues).

(F) The absence or presence of efforts toward rehabilitation, if relevant, to address conduct adverse to CAC determinations.

(*1*) Clear, affirmative evidence of rehabilitation is required for a favorable adjudication (e.g., seeking assistance and following professional guidance, where appropriate; demonstrating positive changes in behavior and employment).

(*2*) Rehabilitation may be a consideration for most conduct, not just alcohol and drug abuse. While formal counseling or treatment may be a consideration, other factors (such as the individual's employment record) may also be indications of rehabilitation.

(iii) CAC adjudicators must successfully complete formal training through a DoD CAC adjudicator course from the Defense Security Service Center for Development of Security Excellence or a course approved by the Suitability Executive Agent.

(2) *Credentialing Standards.* HSPD–12 credentialing standards contained in OPM Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD–12'' must be used to render a final determination whether to issue or revoke a CAC based on results of a qualifying PSI.

(i) *Basic Standards.* CAC credentialing standards and the adjudicative guidelines described in paragraph (c) of this section are designed to guide the adjudicator who must determine, based on results of a qualifying PSI, whether CAC issuance is consistent with the basic standards, would create an unacceptable risk for the U.S. Government, or would provide an avenue for terrorism.

(ii) *Supplemental Standards.* The supplemental standards are intended to ensure that the issuance of a CAC to an individual does not create unacceptable risk. The supplemental credentialing standards must be applied, in addition to the basic credentialing standards. In this context, an unacceptable risk refers to an unacceptable risk 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, including classified, privileged, proprietary, financial, or medical records; or to the privacy of data subjects.

The supplemental credentialing standards, in addition to the basic credentialing standards, must be used for CAC adjudication of individuals who are not also subject to the following types of adjudication:

(A) Eligibility to hold a sensitive position or for access to classified information,

(B) Suitability for Federal employment in the competitive service, or

(C) Qualification for Federal employment in the excepted service.

(3) *Application of the Standards.* (i) CAC credentialing standards shall be applied to all DoD civilian employees, Service members, and contractors who are CAC eligible, have been sponsored by a DoD entity, and require: (a) Physical access to DoD facilities or non-DoD facilities on behalf of DoD; (b) logical access to information systems (whether on site or remotely); or (c) remote access to DoD networks that use only the CAC logon for user authentication.

(ii) If an individual is found unsuitable for competitive civil service consistent with 5 CFR part 731, ineligible for access to classified information pursuant to E.O. 12968, or disqualified from appointment in the excepted service or from working on a contract, the unfavorable decision may be sufficient basis for non-issuance or revocation of a CAC, but does not necessarily mandate this result.

(4) *Adjudication.* The CAC adjudicators will consider the information provided by the CAC PSI in rendering a CAC credentialing determination. The determination will be unfavorable if there is a reasonable basis to conclude that a disqualifying factor in accordance with the basic CAC credentialing standards is substantiated, or when there is a reasonable basis to conclude that derogatory information or conduct relating to supplemental CAC credentialing standards presents an unacceptable risk for the U.S. Government.

(i) If a DoD Component or DOHA proposes to deny or revoke a CAC under conditions other than those cited in paragraph (b)(3)(ii) of this section, the DoD Component or DOHA, as appropriate in accordance with paragraph (b)(6)(i) of this section, must issue the

individual a written statement (also known as a letter of denial (LOD) or revocation (LOR)) identifying the disqualifying condition(s). The statement must contain a summary of the concerns and supporting adverse information, instructions for responding, and copies of the relevant CAC credentialing standards and adjudicative guidelines from this section. The written LOD or LOR must be as comprehensive and detailed as permitted by the requirements of national security and to protect sources that were granted confidentiality, and as allowed pursuant to provisions of 5 U.S.C. 552 and 552a. (Section 552a is also known and hereinafter referred to as ''The Privacy Act of 1974, as amended.'')

(ii) The individual may elect to respond in writing to the DoD Component or DOHA, as appropriate, within 30 calendar days from the date of the LOD or LOR. Failure to respond to the LOD or LOR will result in automatic CAC denial or revocation.

(iii) When, subsequent to issuance of an interim or final CAC, the U.S. Government receives credible information that raises questions as to whether a current CAC holder continues to meet the applicable credentialing standards, the DoD Component may reconsider the credentialing determination using the procedures in this part.

(5) *Denial or Revocation.* (i) DoD Components must deny or revoke a CAC if the individual fails to respond to the LOD or LOR within the specified timeframe or the response to the written statement has not provided a basis to reverse the decision.

(ii) Denial or revocation of a CAC must comply with applicable governing laws and regulations:

(A) The U.S. Coast Guard shall afford individuals appeal rights as established in applicable Department of Homeland Security and U.S. Coast Guard Issuances.

(B) CAC provides Service members with Geneva Convention protection in accordance with DoD Instruction 1000.1, ''Identification (ID) Cards Required by the Geneva Conventions'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/100001p.pdf*), and authorized benefits (e.g. medical) and must not be revoked or denied pursuant to the provisions of this part. CAC for Military Service members will be surrendered only upon separation, discharge, or retirement.

(C) In certain instances a CAC provides other benefits or specific privileges to civilian employees (e.g. medical, post exchange and commissary) when assigned overseas long-term; or protected status to civilian employees and contractors who are accompanying U.S. forces during overseas deployments in accordance with DoD Instruction 1000.1. CAC for DoD civilians or contractors in this circumstance will not be revoked pursuant to the provisions of this part, but may be surrendered as part of other adverse employment or contracting actions or procedures.

(iii) When eligibility is denied or revoked, the CAC shall be recovered whenever practicable, and shall immediately be rendered inoperable. In addition, agency's physical and logical access systems shall immediately be updated to eliminate the use of the CAC for access.

(6) *Appeals.* (i) Individuals who have been denied a CAC or have had a CAC revoked due to an unfavorable credentialing determination must be entitled to appeal the determination in accordance with the following procedures:

(A) Except as stated in paragraph (b)(6)(ii) of this section, new civilian and contractor applicants who have been denied a CAC may elect to appeal to a three member board composed of not more than one security representative and one human resources representative.

(B) Contractor employees who have had their CAC revoked may appeal the unfavorable determination to the DOHA in accordance with the established administrative process set out in DoD Directive 5220.6.

(ii) This appeal process does not apply when a CAC is denied or revoked as a result of either an unfavorable suitability determination consistent with 5 CFR part 731 or a decision to deny or revoke eligibility for access to classified information or eligibility for a sensitive national security position, since the person is already entitled to

seek review in accordance with applicable suitability or national security procedures. Likewise, there is no right to appeal when the decision to deny the CAC is based on the results of a separate determination to disqualify the person from an appointment in the excepted service or to bar the person from working for or on behalf of a Federal department or agency.

(iii) The DoD Component will notify the individual in writing of the final determination and provide a statement that this determination is not subject to further appeal.

(7) *Recording Final Determination.* Immediately following final adjudication, the sponsoring activity must record the final eligibility determination (e.g., active, revoked, denied) in the OPM Central Verification System as directed by OPM Memorandum, ''Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD–12.'' DoD Component records will document the adjudicative rationale. Adjudicative records shall be made available to authorized recipients as required for appeal purposes.

(c) *Basic Adjudicative Standards.* (1) A CAC will not be issued to a person if the individual is known to be or reasonably suspected of being a terrorist.

(i) A CAC must not be issued to a person if the individual is known to be or reasonably suspected of being a terrorist. Individuals entrusted with access to Federal property and information systems must not put the U.S. Government at risk or provide an avenue for terrorism.

(ii) Therefore, conditions that may be disqualifying include evidence that the individual has knowingly and willfully been involved with reportable domestic or international terrorist contacts or foreign intelligence entities, counterintelligence activities, indicators, or other behaviors described in DoD Directive 5240.06, ''Counterintelligence Awareness and Reporting (CIAR)'' (available at *http://www.dtic.mil/whs/directives/corres/pdf/524006p.pdf*).

(2) A CAC will not be issued to a person if the employer is unable to verify the individual's claimed identity.

(i) A CAC must not be issued to a person if the DoD component is unable to verify the individual's claimed identity. To be considered eligible for a CAC, the individual's identity must be clearly authenticated. The CAC must not be issued when identity cannot be authenticated.

(ii) Therefore, conditions that may be disqualifying include:

(A) The individual claimed it was not possible to provide two identity source documents from the list of acceptable documents in Form I–9, Office of Management and Budget No. 1115–0136, ''Employment Eligibility Verification,''(available at *http://www.uscis.gov/files/form/i-9.pdf*) or provided only one identity source document from the list of acceptable documents.

(B) The individual did not appear in person as required by Federal Information Processing Standards Publication 201–2.

(C) The individual refused to cooperate with the documentation and investigative requirements to validate his or her identity.

(D) The investigation failed to confirm the individual's claimed identity.

(iii) No conditions can mitigate inability to verify the applicant's identity.

(3) A CAC will not be issued to a person if there is a reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity.

(i) A CAC must not be issued to a person if there is a reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity in an attempt to obtain the current credential.

(A) Substitution occurred in the identity proofing process; the individual who appeared on one occasion was not the same person that appeared on another occasion.

(B) The fingerprints associated with the identity do not belong to the person attempting to obtain a CAC.

(ii) No conditions can mitigate submission of fraudulent information in an attempt to obtain a current credential.

(4) A CAC will not be issued to a person if there is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by

the Privacy Act, information that is proprietary in nature, or other sensitive or protected information.

(i) Individuals must comply with information-handling regulations and rules. Individuals must properly handle classified and protected information such as sensitive or proprietary information.

(ii) Individuals should not attempt to gain unauthorized access to classified documents or other sensitive or protected information. Unauthorized access to U.S. Government information or improper use of U.S. Government information once access is granted may pose a significant risk to national security, may compromise individual privacy, and may make public information that is proprietary in nature, thus compromising the operations and missions of Federal agencies.

(iii) A CAC must not be issued if there is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act of 1974, as amended, information that is proprietary in nature, or other sensitive or protected information.

(iv) Therefore, conditions that may be disqualifying include any attempt to gain unauthorized access to classified, sensitive, proprietary or other protected information.

(v) Circumstances relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk include:

(A) Since the time of the last act or activities, the person has demonstrated a favorable change in behavior.

(B) The behavior happened so long ago, was minor, or happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's ability to safeguard protected information.

(5) A CAC will not be issued to a person if there is a reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately.

(i) A CAC must not be issued to a person if there is a reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately.

(ii) Therefore, conditions that may be disqualifying include:

(A) Documented history of fraudulent requests for credentials or other official documentation.

(B) Previous incidents in which the individual used credentials or other official documentation to circumvent rules or regulations.

(C) A history of incidents involving misuse of credentials that put physical assets or personal property at risk.

(iii) Circumstances relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk include:

(A) The behavior happened so long ago, was minor, or happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's ability and willingness to use credentials lawfully and appropriately.

(6) A CAC will not be issued to a person if there is a reasonable basis to believe the individual will use Federally-controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

(i) Individuals must comply with rules, procedures, guidelines, or regulations pertaining to information technology systems and properly protect sensitive systems, networks, and information. The individual should not attempt to use federally-controlled information systems unlawfully, make unauthorized modifications, corrupt or destroy, or engage in inappropriate uses of such systems. A CAC must not be issued to a person if there is a reasonable basis to believe the individual will do so or has done so in the past.

(ii) Therefore, conditions that may be disqualifying include:

(A) Illegal, unauthorized, or inappropriate use of an information technology system or component.

(B) Unauthorized modification, destruction, manipulation of information, software, firmware, or hardware to corrupt or destroy information technology systems or data.

(iii) Circumstances relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk include:

(A) The behavior happened so long ago, was minor, or happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's ability and willingness to conform to rules and regulations for use of information technology systems.

(d) *Supplemental Adjudicative Standards.* (1) A CAC will not be issued to a person if there is a reasonable basis to believe, based on the individual's misconduct or negligence in employment, that issuance of a CAC poses an unacceptable risk.

(i) An individual's employment misconduct or negligence may put people, property, or information systems at risk.

(ii) Therefore, conditions that may be disqualifying include:

(A) A previous history of intentional wrongdoing on the job, disruptive, violent, or other acts that may pose an unacceptable risk to people, property, or information systems.

(B) A pattern of dishonesty or rule violations in the workplace which put people, property or information at risk.

(C) A documented history of misusing workplace information systems to view, download, or distribute pornography.

(D) Violation of written or recorded commitments to protect information made to an employer, such as breach(es) of confidentiality or the release of proprietary or other information.

(E) Failure to comply with rules or regulations for the safeguarding of classified, sensitive, or other protected information.

(iii) Circumstances relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk include:

(A) The behavior happened so long ago, was minor, or happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's current trustworthiness or good judgment relating to the safety of people and proper safeguarding of property and information systems.

(B) The individual was not adequately warned that the conduct was unacceptable and could not reasonably be expected to know that the conduct was wrong.

(C) The individual made prompt, good-faith efforts to correct the behavior.

(D) The individual responded favorably to counseling or remedial training and has since demonstrated a positive attitude toward the discharge of information-handling or security responsibilities.

(2) A CAC will not be issued to a person if there is a reasonable basis to believe, based on the individual's criminal or dishonest conduct, that issuance of a CAC poses an unacceptable risk.

(i) An individual's conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about his or her reliability or trustworthiness and may put people, property, or information systems at risk. An individual's past criminal or dishonest conduct may put people, property, or information systems at risk.

(ii) Therefore, conditions that may be disqualifying include:

(A) A single serious crime or multiple lesser offenses which put the safety of people at risk or threaten the protection of property or information. A person's convictions for burglary may indicate that granting a CAC poses an unacceptable risk to the U.S. Government's physical assets and to employees' personal property on a U.S. Government facility.

(B) Charges or admission of criminal conduct relating to the safety of people and proper protection of property or information systems, regardless of whether the person was formally charged, formally prosecuted, or convicted.

(C) Dishonest acts (e.g., theft, accepting bribes, falsifying claims, perjury, forgery, or attempting to obtain identity documentation without proper authorization).

(D) Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, or other intentional financial breaches of trust.

(E) Actions involving violence or sexual behavior of a criminal nature that

poses an unacceptable risk if access is granted to federally-controlled facilities or federally-controlled information systems. For example, convictions for sexual assault may indicate that granting a CAC poses an unacceptable risk to the life and safety of persons on U.S. Government facilities.

(F) Financial irresponsibility may raise questions about the individual's honesty and put people, property or information systems at risk, although financial debt should not in and of itself be cause for denial.

(G) Deliberate omission, concealment, or falsification of relevant facts or deliberately providing false or misleading information to an employer, investigator, security official, competent medical authority, or other official U.S. Government representative, particularly when doing so results in personal benefit or which results in a risk to the safety of people and proper safeguarding of property and information systems.

(iii) Circumstances relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk include:

(A) The behavior happened so long ago, was minor in nature, or happened under such unusual circumstances that it is unlikely to recur.

(B) Charges were dismissed or evidence was provided that the person did not commit the offense and details and reasons support his or her innocence.

(C) Improper or inadequate advice from authorized personnel or legal counsel significantly contributed to the individual's omission, of information. When confronted, the individual provided an accurate explanation and made prompt, good-faith effort to correct the situation.

(D) Evidence has been supplied of successful rehabilitation, including but not limited to remorse or restitution, job training or higher education, good employment record, constructive community involvement, or passage of time without recurrence.

(3) A CAC will not be issued to a person if there is a reasonable basis to believe, based on the individual's material, intentional false statement, deception, or fraud in connection with Federal or contract employment, that issuance of a CAC poses an unacceptable risk.

(i) The individual's conduct involving questionable judgment, lack of candor, or unwillingness to comply with rules and regulations can raise questions about an individual's honesty, reliability, trustworthiness, and put people, property, or information systems at risk.

(ii) Therefore, conditions that may be disqualifying include material, intentional falsification, deception or fraud related to answers or information provided during the employment process for the current or a prior Federal or contract employment (e.g., on the employment application or other employment, appointment or investigative documents, or during interviews.)

(iii) Circumstances relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk include:

(A) The misstated or omitted information was so long ago, was minor, or happened under such unusual circumstances that it is unlikely to recur.

(B) The misstatement or omission was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation.

(4) A CAC will not be issued to a person if there is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of a CAC poses an unacceptable risk.

(i) An individual's abuse of alcohol may put people, property, or information systems at risk. Alcohol abuse can lead to the exercise of questionable judgment or failure to control impulses, and may put people, property, or information systems at risk, regardless of whether he or she is diagnosed as an abuser of alcohol or alcohol dependent. A person's long-term abuse of alcohol without evidence of substantial rehabilitation may indicate that granting a CAC poses an unacceptable safety risk in a U.S. Government facility.

(ii) Therefore, conditions that may be disqualifying include:

(A) A pattern of alcohol-related arrests.

(B) Alcohol-related incidents at work, such as reporting for work or

duty in an intoxicated or impaired condition, or drinking on the job.

(C) Current continuing abuse of alcohol.

(D) Failure to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.

(iii) Circumstances relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk include:

(A) The individual acknowledges his or her alcoholism or issues of alcohol abuse, provides evidence of actions taken to overcome this problem, and has established a pattern of abstinence (if alcohol dependent) or responsible use (if an abuser of alcohol).

(B) The individual is participating in counseling or treatment programs, has no history of previous treatment or relapse, and is making satisfactory progress.

(C) The individual has successfully completed inpatient or outpatient counseling or rehabilitation along with any required aftercare. He or she has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations, such as participation in an alcohol treatment program. The individual has received a favorable prognosis by a duly qualified medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

(5) A CAC will not be issued to a person if there is a reasonable basis to believe, based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of a CAC poses an unacceptable risk.

(i) An individual's abuse of drugs may put people, property, or information systems at risk. Illegal use of narcotics, drugs, or other controlled substances, to include abuse of prescription or over-the-counter drugs, can raise questions about his or her trustworthiness, or ability or willingness to comply with laws, rules, and regulations. For example, a person's long-term illegal use of narcotics without evidence of substantial rehabilitation may indicate that granting a CAC poses an unacceptable safety risk in a U.S. Government facility.

(ii) Therefore, conditions that may be disqualifying include:

(A) Current or recent illegal drug use, serious narcotic, or other controlled substance offense.

(B) A pattern of drug-related arrests or problems in employment.

(C) Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution of illegal drugs, or possession of drug paraphernalia.

(D) Diagnosis by a duly qualified medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence.

(E) Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program.

(F) Failure to successfully complete a drug treatment program prescribed by a duly qualified medical professional.

(G) Any illegal drug use after formally agreeing to comply with rules or regulations prohibiting drug use.

(H) Any illegal use or abuse of prescription or over-the-counter drugs.

(iii) Circumstances relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk include:

(A) The behavior happened so long ago, was so infrequent, or happened under such circumstances that it is unlikely to recur (e.g., clear, lengthy break since last use; strong evidence the use will not occur again).

(B) A demonstrated intent not to abuse any drugs in the future, such as:

(*1*) Abstaining from drug use.

(*2*) Disassociating from drug-using associates and contacts.

(*3*) Changing or avoiding the environment where drugs were used.

(C) Abuse of prescription drugs followed a severe or prolonged illness during which these drugs were prescribed and abuse has since ended.

(D) Satisfactory completion of a prescribed drug treatment program, including but not limited to rehabilitation and aftercare requirements without recurrence of abuse, and a favorable prognosis by a duly qualified medical professional.

(6) A CAC will not be issued to a person if a statutory or regulatory bar prevents the individual's contract employment; or would prevent Federal employment under circumstances that furnish a reasonable basis to believe that issuance of a CAC poses an unacceptable risk.

(i) The purpose of this standard is to verify whether there is a bar on contract employment, and whether the contract employee is subject to a Federal employment debarment for reasons that also pose an unacceptable risk in the contracting context. For example, a person's 5-year bar on Federal employment based on a felony conviction related to inciting a riot or civil disorder, as specified in 5 U.S.C. 7313, may indicate that granting a CAC poses an unacceptable risk to persons, property, and assets in U.S. Government facilities.

(ii) Therefore, conditions that may be disqualifying include:

(A) A debarment was imposed by OPM, DoD, or other Federal agencies when the conduct poses an unacceptable risk to people, property, or information systems.

(B) The suitability debarment was based on the presence of serious suitability issues when the conduct poses an unacceptable risk to people, property, or information systems.

(iii) Circumstances relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk include:

(A) Applicant proves the reason(s) for the debarment no longer exists.

(B) The debarment is job or position-specific and is not applicable to the job currently under consideration.

(7) A CAC will not be issued to a person if the individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

(i) Individuals entrusted with access to U.S. Government property and information systems must not put the U.S. Government at risk.

(ii) Therefore, conditions that may be disqualifying include:

(A) Illegal involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason or sedition against the United States of America.

(B) Association or agreement with persons who attempt to or commit any of the acts in paragraph (d)(7)(ii)(A) of this section with the specific intent to further those unlawful aims.

(C) Association or agreement with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means in an effort to overthrow or influence the U.S. Government.

(iii) Circumstances relevant to the determination of whether there is a reasonable basis to believe there is an unacceptable risk include:

(A) The behavior happened so long ago, was minor, or happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's current trustworthiness.

(B) The person was not aware of the person's or organization's dedication to illegal, treasonous, or seditious activities or did not have the specific intent to further the illegal, treasonous, or seditious ends of the person or organization.

(C) The individual did not have the specific intent to incite others to advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means to engage in illegal, treasonous, or seditious activities.

(D) The individual's involvement in the activities was for an official purpose.

PART 158—OPERATIONAL CONTRACT SUPPORT (OCS) OUTSIDE THE UNITED STATES

Sec.

AUTHORITY: Pub. L. 110–181; Pub. L. 110–417.

SOURCE: 88 FR 26480, May 1, 2023, unless otherwise noted.