



Department of Defense INSTRUCTION

NUMBER 5200.02

March 21, 2014

USD(I)

SUBJECT: DoD Personnel Security Program (PSP)

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive (DoDD) 5200.2 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the authority in DoDD 5143.01 (Reference (b)) to establish policy, assign responsibilities, and prescribe procedures for the DoD PSP consistent with References (c) through (r).

b. Establishes investigation and adjudication policy for the common access card (CAC), which serves as the DoD Federal personal identity verification (PIV) credential in accordance with References (h), (i), (q), (r), and (s) through (x).

c. Incorporates and cancels DoDIs 5210.25 and 5220.28 (References (y) and (z)).

2. APPLICABILITY. This Instruction applies to OSD, 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").

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 References (c) through (r), Intelligence Community Directive (ICD) Number 704 (Reference (aa)), and DoDD 5220.6 (Reference (ab)).

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 sensitive 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 CACs in accordance with the standards of References (s) through (x), 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.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosures 3 and 4.

6. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

7. EFFECTIVE DATE. This Instruction:
 - a. Is effective March 21, 2014.

 - b. Must be reissued, cancelled, or certified current within 5 years of its publication to be considered current in accordance with DoDI 5025.01 (Reference (ac)).

 - c. Will expire effective March 21, 2024 and be removed from the DoD Issuances Website if it hasn't been reissued or cancelled in accordance with Reference (ac).



Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures

1. References
2. Responsibilities
3. National Security Positions
4. CAC Investigation and Adjudication

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....5

ENCLOSURE 2: RESPONSIBILITIES.....7

 UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)).....7

 DIRECTOR FOR DEFENSE INTELLIGENCE (INTELLIGENCE AND SECURITY).....7

 USD(AT&L).....8

 UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)).....8

 GC, DoD.....8

 HEADS OF THE DoD COMPONENTS.....8

ENCLOSURE 3: NATIONAL SECURITY POSITIONS10

 PROCEDURES.....10

 SENSITIVE COMPARTMENTED INFORMATION (SCI) ELIGIBILITY10

 ADJUDICATION.....10

 APPEAL PROCEDURES-DENIAL OR REVOCATION OF ELIGIBILITY11

 POLYGRAPH.....11

 CONTINUOUS EVALUATION.....11

 FINANCIAL DISCLOSURE11

 RECIPROCAL ACCEPTANCE OF ELIGIBILITY DETERMINATIONS11

 NATIONAL SECURITY AGENCY (NSA)/CENTRAL SECURITY SERVICE (CSS)12

 WOUNDED WARRIOR SECURITY AND INTELLIGENCE INTERNSHIP
 PROGRAM.....12

ENCLOSURE 4: CAC INVESTIGATION AND ADJUDICATION.....13

 GENERAL.....13

 INVESTIGATION.....13

 ADJUDICATION.....13

 APPEALS14

 FOREIGN NATIONALS15

 RECORDING FINAL ADJUDICATION.....16

 RECIPROCIY OF CAC DETERMINATIONS.....16

GLOSSARY17

 PART I: ABBREVIATIONS AND ACRONYMS17

 PART II: DEFINITIONS.....17

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5200.2, "DoD Personnel Security Program," April 9, 1999 (hereby cancelled)
- (b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),
November 23, 2005
- (c) Executive Order 12968, "Access to Classified Information," August 2, 1995, as amended
- (d) Executive Order 10865, "Safeguarding Classified Information within Industry,"
February 20, 1960, as amended
- (e) Executive Order 13467, "Reforming Processes Related to Suitability for Government
Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified
National Security Information," June 30, 2008
- (f) Parts 731, 731.101, 732, and 736 of title 5, Code of Federal Regulations
- (g) Executive Order 10450, "Security Requirements for Government Employment," April 27,
1953, as amended
- (h) Executive Order 13526, "Classified National Security Information," December 29, 2009
- (i) Executive Order 12829, "National Industrial Security Program," January 6, 1993, as
amended
- (j) Executive Order 13488, "Granting Reciprocity on Excepted Service and Federal Contractor
Employee Fitness and Reinvestigating Individuals in Positions of Public Trust,"
January 16, 2009
- (k) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as
amended
- (l) Sections 301 and 7532 of title 5, United States Code
- (m) Section 1072 of Public Law 110-181, "National Defense Authorization Act for Fiscal Year
2008," January 28, 2008
- (n) Section 3343. of title 50, United States Code
- (o) Title 10, United States Code
- (p) Title 32, Code of Federal Regulations
- (q) Section 278g-3 of title 15, United States Code
- (r) Section 11331 of title 40, United States Code
- (s) Federal Acquisition Regulation, current edition
- (t) Defense Federal Acquisition Regulation, current edition
- (u) Office of Personnel Management Memorandum, "Final Credentialing Standards for Issuing
Personal Identity Verification Cards under HSPD-12," July 31, 2008
- (v) 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," August 5, 2005
- (w) Homeland Security Presidential Directive-12, "Policy for a Common Identification
Standard for Federal Employees and Contractors," August 27, 2004
- (x) Federal Information Processing Standards Publication 201-2, "Personal Identity
Verification (PIV) of Federal Employees and Contractors," August 2013

- (y) DoD Instruction 5210.25, "Assignment of American National Red Cross and United Service Organizations, Inc., Employees to Duty with the Military Services," May 12, 1983 (hereby cancelled)
- (z) DoD Instruction 5220.28, "Application of Special Eligibility and Clearance Requirements in the SIOP-ESI Program for Contractor Employees," March 8, 1978 (hereby cancelled)
- (aa) Director of National Intelligence, Intelligence Community Directive Number 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 2, 2008
- (ab) DoD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," January 2, 1992
- (ac) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012, as amended
- (ad) DoD Instruction 3305.13, "DoD Security Training," December 18, 2007
- (ae) DoD Directive 5145.01, "General Counsel of the Department of Defense," May 2, 2001
- (af) DoD 5200.2-R, "Personnel Security Program," January 1987
- (ag) DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985
- (ah) DoD 5400.11-R, "DoD Privacy Program," May 14, 2007
- (ai) DoD Instruction 5210.91, "Polygraph and Credibility Assessment (PCA) Procedures," August 12, 2010
- (aj) DoD Directive 5210.48, "Polygraph and Credibility Assessment Program," January 25, 2007
- (ak) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010
- (al) Deputy Under Secretary of Defense for Intelligence and Security Memorandum, "DoD Implementation of Electronic Submission of the Standard SF 714 (SF 714) Financial Disclosure Report," May 11, 2009
- (am) Under Secretary of Defense for Intelligence Memorandum, "Timeline Clarification: Department of Defense implementation of Electronic Submission of the Standard Form 714 Financial Disclosure Report," January 17, 2013
- (an) Office of Management and Budget Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," December 12, 2005
- (ao) Office of Management and Budget Memorandum M-06-21, "Reciprocal Recognition of Existing Personnel Security Clearances," July 17, 2006
- (ap) Office of Management and Budget Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," November 14, 2007
- (aq) DoD Instruction 5210.45, "Personnel Security Policies and Procedures for Sensitive Cryptologic Information in the National Security Agency/Central Security Service," November 14, 2008
- (ar) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- (as) DoD Instruction 1300.24, "Recovery Coordination Program," December 1, 2009

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), pursuant to Reference (b), shall:

a. Develop, coordinate, and oversee the implementation of policy, programs, and guidance for the DoD PSP.

b. In coordination with the Under Secretary of Defense for Personnel and Readiness 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 References (u) through (x), as applicable.

c. 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 References (s) through (x), as applicable.

d. Issue guidance implementing the policy in this Instruction.

2. DIRECTOR FOR DEFENSE INTELLIGENCE (INTELLIGENCE AND SECURITY) (DDI(I&S)). The DDI(I&S), under the authority, direction, and control of the USD(I), shall:

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

b. Develop and publish revisions to Reference (ac).

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

d. Ensure that the Defense Security Service (DSS) provides education, training, and awareness support to the DoD PSP in accordance with DoDI 3305.13 (Reference (ad)).

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

f. 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.

- g. Develop guidance, interpretation, and clarification regarding the DoD PSP as needed.
- h. Conduct oversight inspections of the DoD Components for implementation and compliance with DoD personnel security policy and operating procedures.
- i. 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.

3. USD(AT&L). The USD(AT&L) shall:

- a. Establish acquisition policy, procedures, and guidance, in coordination with the USD(I) that facilitate DoD Component compliance with the DoD PSP.
- b. Establish regulatory requirements within the Federal Acquisition Regulation and Defense Federal Acquisition Regulation (References (s) and (t)) for contracts and agreements that require non-DoD personnel to adhere to personnel security procedures in the performance of a contract or agreement.

4. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) is the approval authority for requests for exceptions to the DoD PSP involving access to NATO classified information.

5. GC, DoD. The GC, DoD shall:

- a. 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.
- b. Perform functions relating to the DoD PSP in accordance with Reference (ad) and DoDD 5145.01 (Reference (ae)), including the maintenance and oversight of the Defense Office of Hearings and Appeals (DOHA).

6. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

- a. Designate a senior agency official, consistent with the provisions of Executive Order (E.O.) 12968, as amended (Reference (c)), who shall direct and administer the DoD PSP consistent with this Instruction.
- b. Comply with the policy and procedures regarding investigation and adjudication for CAC issuance and distribute this guidance to local and regional organizations.
- c. Provide funding to cover Component requirements for PSIs, adjudication, and recording of results to comply with the DoD PSP.
- d. 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.
- e. 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.
- f. Provide requested information and recommendations, as appropriate, on any aspect of this Instruction and the DoD PSP to the USD(I).
- g. Enforce the requirement that DoD personnel security adjudication system(s) of record, within their respective Components, shall only be used as a personnel security system of record and shall not be used as a pre-hiring screening tool.

ENCLOSURE 3

NATIONAL SECURITY POSITIONS

1. PROCEDURES. The objective of the PSP is to ensure persons deemed eligible for national security positions remain reliable and trustworthy.

a. 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 Reference (c), E.O. 10865 (Reference (d)), References (aa), (ab), DoD 5200.2-R (Reference (af)), or DoD 5220.22-R (Reference (ag)). The specific procedures applicable in each case type are set forth in DoD issuances.

b. 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 DoD 5400.11-R (Reference (ah)), may be designated as national security positions within DoD, where such access has the potential to cause serious damage to national security.

2. SENSITIVE COMPARTMENTED INFORMATION (SCI) ELIGIBILITY. Investigative and adjudicative requirements for SCI eligibility shall be executed in accordance with this Instruction and Reference (aa).

3. ADJUDICATION

a. Personnel security criteria and adjudicative standards are described in References (c), (aa), (ab), (af), and (ag) 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.

b. When an unfavorable personnel security determination is rendered:

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

(2) 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.

c. 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.

4. APPEAL PROCEDURES-DENIAL OR REVOCATION OF ELIGIBILITY. Individuals may elect to appeal unfavorable personnel security determinations in accordance with the procedures set forth in References (c), (aa), (ab), (af), and (ag), as applicable, or as otherwise authorized by law.

5. 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. The conditions, requirements, and limitations associated with polygraph use are prescribed in DoDI 5210.91, DoDD 5210.48, and DoDD 5205.07 (References (ai) through (ak)).

6. CONTINUOUS EVALUATION. All personnel in national security positions shall be subject to continuous evaluation.

7. FINANCIAL DISCLOSURE. DoD Components shall implement the annual financial disclosure requirement in accordance with Reference (c), DUSD(I&S) Memorandum (Reference (al)), and USD(I) Memorandum (Reference (am)).

8. RECIPROCAL ACCEPTANCE OF ELIGIBILITY DETERMINATIONS

a. DoD reciprocally accepts existing national security eligibility determinations or clearances from other Government agencies in accordance with E.O. 13467 (Reference (e)), part 731 of title 5, Code of Federal Regulations (Reference (f)), and Office of Management and Budget Memorandums (References (an), (ao), and (ap)).

b. Reciprocity for SCI eligibility shall be executed in accordance with Reference (aa) and associated Director of National Intelligence guidance.

c. 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 Reference (am), 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 Reference (ao).

9. 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 DoDI 5210.45 (Reference (aq)).

10. 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.

a. 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.

b. 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.

ENCLOSURE 4

CAC INVESTIGATION AND ADJUDICATION

1. GENERAL. Individuals entrusted with access to Federal property and information systems must not put the Government at risk or provide an avenue for terrorism.

a. All individuals requiring a CAC must meet credentialing standards of Office of Personnel Management (OPM) Memorandum (Reference (u)). 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.

b. If an individual is found unsuitable for employment in a covered position under part 731.101 of Reference (f), ineligible for access to classified information under Reference (c), 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.

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

a. 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).

b. 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.

c. 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.

d. Existing CAC holders without the requisite background investigation on record must be investigated in accordance with OMB Memorandum M-05-24 (Reference (v)).

3. 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 Reference (u), each of which is to be evaluated in the context of the whole person. These standards shall be evaluated to determine if issuing a CAC to the individual poses an unacceptable risk.

a. 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.

b. Final credentialing standards are:

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

(2) 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.

c. 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.

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

e. 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.

f. 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.

4. APPEALS. CAC applicants or holders may appeal CAC denial or revocation.

a. No separate administrative appeal process is allowed when an individual has been denied a CAC as a result of a negative suitability determination under part 731 of Reference (f), 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 Reference (u). 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.

b. 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.

c. 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 Reference (ab).

d. Decisions following appeal are final.

e. 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.

5. **FOREIGN NATIONALS.** Special considerations for conducting background investigations of non-U.S. nationals (foreign nationals) are addressed in Reference (u). The following criteria shall be met prior to CAC issuance to foreign nationals:

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

b. Foreign nationals are not eligible to receive CAC on an interim basis.

c. At foreign locations:

(1) 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 as stated in DoDD 5230.20 (Reference (ar)).

(2) 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.

d. At U.S.-based locations and in U.S. territories:

(1) 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.

(2) 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.

6. 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 Reference (u) and maintain local records for posting in a DoD repository when available.

7. RECIPROCITY OF CAC DETERMINATIONS

a. The sponsoring activity shall not re-adjudicate CAC determinations for individuals transferring from another Federal department or agency, provided:

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

(2) 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.

(3) 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.

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

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CAC	common access card
DoDD	DoD Directive
DoDI	DoD Instruction
DOHA	Defense Office of Hearings and Appeals
DSS	Defense Security Service
DDI(I&S)	Director for Defense Intelligence (Intelligence and Security)
GC, DoD	General Counsel of the DoD
ICD	Intelligence Community Directive
NACI	National Agency Check with Inquiries
NATO	North Atlantic Treaty Organization
NSA/CSS	National Security Agency/Central Security Service
PIV	personal identity verification
PSI	personnel security investigation
PSP	Personnel Security Program
SCI	sensitive compartmented information
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

PART II. DEFINITIONS

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

continuous evaluation. Defined in section 1.3(d) of Reference (e).

contractor. Defined in Reference (e).

employee. Defined in Reference (c).

limited access authorization: Defined in Reference (af).

national security position. 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. Such positions include those requiring eligibility for access to classified information.

Other such positions include, but are not limited to, those whose duties include: 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; developing defense plans or policies; planning or conducting intelligence or counterintelligence activities, counterterrorism activities and related activities concerned with the preservation of the military strength of the United States; 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; 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; 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; 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 conducting investigations or audits related to the functions described above as "other such positions," where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security. The requirements of this definition 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 definition 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.