SECRETARY OF THE ARMY
WASHINGTON

MAR 0 7 2014

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Directive 2014-05 (Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors)

1. References:

a. Army Directive 2011-08 (Army Implementation of Homeland Security Presidential Directive-12), 26 May 2011.

b. Memorandum, Secretary of the Army, 31 Oct 2013, subject: Uncleared Contractor Common Access Card Credentialing and Installation Access.

2. This directive provides policy and procedures for the unescorted access of uncleared contractor employees to Department of Defense installations, facilities and/or networks for which the Army is responsible for physical security. (This includes Army-managed Armed Forces Reserve Centers, Army Reserve Centers, and Army National Guard facilities subject to Department of the Army jurisdiction or administration.) An uncleared contractor is an individual who falls into one of the following categories:

a. CAC-eligible: An employee of an Army contractor who is eligible for a common access card (CAC), but is not subject to a higher-level vetting (for example, security clearance; Personnel Reliability Program; Arms, Ammunition and Explosives, etc.) that has been favorably adjudicated.

b. Non-CAC eligible: An employee of a Department of Defense contractor who is not eligible for a CAC credential, but requires access to an Army installation or facility.

3. Enclosure 1 provides Army policy for the investigation and adjudication process to support issuance of the CAC credential to eligible uncleared contractors in compliance with Homeland Security Presidential Directive 12 (HSPD-12). Enclosure 2 establishes Army policy for adjudication and screening standards to control the access of unescorted, uncleared contractors to Army installations and facilities.

4. This effort is a priority for the Army and should be provided resources accordingly.

5. This directive applies to Headquarters, Department of the Army; Army Commands; Army Service Component Commands; Direct Reporting Units; field operating agencies; staff support activities; and all Army components, including the Army National Guard/Army National Guard of the United States and U.S. Army Reserve.

6. The Assistant Secretary of the Army (Manpower and Reserve Affairs) provides oversight for these policies. The Deputy Chief of Staff, G-2 provides HSPD-12 investigative and adjudicative guidelines to support issuance of the Army CAC. The Provost Marshal General provides Army policy for adjudication security standards for controlling the entry to Army installations by contractors who are not CAC-eligible.

7. This directive will be reviewed within 60 days of completion of The Inspector General's Armywide inspection directed in reference 1b. The Deputy Chief of Staff, G-2 and the Provost Marshal General will incorporate the provisions of this directive into Army Regulation 380-67 (Personnel Security Program) and Army Regulation 190-13 (The Army Physical Security Program), respectively as soon as practical. This directive is rescinded upon issuance of the revised regulations.

John M. McHugh

Encls

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
- U.S. Army Forces Command
- U.S. Army Training and Doctrine Command
- U.S. Army Materiel Command
- U.S. Army Pacific
- U.S. Army Europe
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Africa/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Cyber Command
- U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Criminal Investigation Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Installation Management Command

Superintendent, United States Military Academy
(CONT)

SUBJECT: Army Directive 2014-05 (Policy and Implementation Procedures Common Access Card Credentialing and Installation Access for Uncleared Contractors)

DISTRIBUTION: (CONT)
Director, U.S. Army Acquisition Support Center
Executive Director, Arlington National Cemetery
Commandant, U.S. Army War College
Commander, U.S. Army Accessions Support Brigade

CF:
Director, Army National Guard
Director, Office of Business Transformation
Commander, U.S. Army Human Resources Command

POLICY AND IMPLEMENTATION PROCEDURES FOR HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12) INVESTIGATIONS AND ADJUDICATIONS

Applicability

The policy and procedures outlined in this document apply to Headquarters, Department of the Army; Army Commands; Army Service Component Commands; Direct Reporting Units; field operating agencies; staff support activities; and all other organizational entities within the Department of Army (including the Army National Guard/Army National Guard of the United States and U.S. Army Reserve), hereafter referred to as "sponsoring activities," responsible for issuance of a common access card (CAC) to uncleared Army contractor personnel.

These policies and procedures do not apply to individuals determined suitable for Federal employment consistent with the provisions of 5 Code of Federal Regulations Part 731 (reference a), or granted eligibility for access to classified information pursuant to Executive Order 12968 (reference b) and Department of Defense (DoD) Regulation 5200.02-R (reference c). (A complete list of references is at attachment 1 to this enclosure.)

Purpose

This document establishes HSPD-12 investigative and adjudicative policy and procedures consistent with references d–h to support credentialing determinations for the issuance of CACs to eligible Army contractor personnel.

CAC Eligibility

Army contractor personnel requiring access to DoD-controlled installations or facilities on behalf of the Department of the Army on a recurring basis for a period of 6 months or more, or an individual requiring both access to a DoD-controlled installation or facility and onsite or remote access to DoD- or Army-controlled information networks are eligible for a CAC.

Background

HSPD-12 mandates a Governmentwide standard for secure and reliable forms of identification issued by the Federal Government for physical access to federally controlled facilities and/or logical access to federally controlled information systems. The CAC is the DoD federal personal identity verification credential.

The DoD Consolidated Adjudications Facility (CAF) will conduct centralized adjudications of favorable HSPD-12 background investigations. The DoD CAF will forward investigations that cannot be favorably adjudicated to the Defense Office of Hearings and Appeals (DOHA) for a final credentialing determination.

Policy

1. Background Investigation

a. Initial issuance of a CAC requires the completion of a Federal Bureau of Investigation (FBI) fingerprint check with favorable results and the successful submission of a National Agency Check with Inquiries (NACI) (equivalent or higher) background investigation to the Army's investigative service provider, the U.S. Office of Personnel Management (OPM), via the U.S. Army Personnel Security Investigation Center of Excellence (reference i).

b. A final CAC determination requires a favorably adjudicated NACI (equivalent or higher) investigation based on the basic and supplemental HSPD-12 credentialing standards listed in attachments 2 and 3 to this enclosure.

2. Reciprocity. Favorable adjudication determinations from another Federal department or agency will be accepted reciprocally in accordance with the enclosed standards. Reciprocity will be based on final favorable adjudication only. Procedures for determining application of reciprocity are described in this directive.

3. Adjudicative Decisions

a. Initial CAC Issuance. Sponsoring activities are responsible for granting interim credentialing decisions to support the initial issuance of a CAC. A determination to issue a CAC on an interim basis is an inherently governmental function and, consistent with reference j, it must be made by a Government official who:

(1) has a favorably adjudicated background investigation or equivalent or higher investigation, and

(2) has successfully completed formal training via the Center for Development of Security Excellence online course "Introduction to HSPD-12 CAC Credentialing[1]."

b. Final CAC Issuance. The DoD CAF will render favorable credentialing determinations except when the background investigation contains unmitigated derogatory information. DOHA will make the final decision on CAC issuance when the DoD CAF is unable to render a favorable determination.

4. Reconsideration (Appeal). Individuals will be notified in writing and provided the opportunity to appeal unfavorable CAC credentialing decisions by DOHA. Notification will be made by an official appointed by the sponsoring activity.

a. The appointed official will receive and process correspondence from DOHA for individuals who have received an unfavorable determination. The official must have knowledge of related security or suitability processes. The contact information for the

[1] http://www.cdse.edu/catalog/elearning/PS112.html

appointed official will be provided by email to the Office of the Deputy Chief of Staff, G-2 (DAMI-CD) no later than 14 days from the date of this directive.

b. Individuals may reapply for a CAC 1 year from the date of the final adjudicative denial or revocation.

5. System of Record. All final credentialing determinations will be annotated in the DoD Case Adjudication Tracking System (CATS) portal, which transmits a record of the determination to the OPM Central Verification System (CVS). The OPM CVS is the system of record for recording final determinations on CAC credentialing.

6. Periodic Reinvestigation. Periodic reinvestigation to support continued possession of a CAC not authorized unless the individual has a 24-month break in Federal service or Army contractor employment.

HSPD-12 Credentialing Procedures

1. Systems Access. Personnel processing HSPD-12 actions for CAC issuance should follow local procedure to access one or more of the following systems to conduct the credentialing process:

a. Joint Personnel Adjudication System (JPAS). JPAS is the DoD master repository for the comprehensive management of all security clearance records and adjudicative determinations for military personnel, DoD civilians and contractors. Currently, JPAS is not a system of record for HSPD-12 determinations, but it will be used in the HSPD-12 credentialing process to determine whether an applicant has already undergone a favorably adjudicated national security investigation for a security clearance or has an open investigation.

b. OPM CVS. OPM CVS is a centralized database at OPM that supports reciprocity and information sharing within the Federal Government. OPM CVS captures and maintains information on all types of investigations and adjudications. OPM CVS may be used to determine if the minimum level of investigation (NACI equivalent/higher) required by HSPD-12 has been conducted and whether it resulted in a favorable adjudication. Personnel processing HSPD-12 CAC credentialing actions are authorized “read-only” access to OPM CVS.

c. Personnel Security Investigation Portal (PSIP). PSIP is an Army system that sponsoring activities use to request background investigations for sponsored applicants.

d. Electronic Questionnaires for Investigations Processing (eQIP). OPM’s eQIP is a Web-based system designed to facilitate the processing of standard investigative forms for conducting background investigations.

e. DoD CATS Portal. A subsystem of CATS, the portal allows for the DoD CAF to share determinations and other correspondence with decision-makers at sponsoring activities.

(1) A “Component Adjudicator” role is required to receive HSPD-12 investigation and adjudication information and record interim credentialing determinations in the portal. The other roles in the portal (“HR” or “Security Manager”) are limited and cannot be used to perform HSPD-12 actions.

(2) The application and instructions for obtaining a Component Adjudicator role to access the portal are at attachment 4 to this enclosure.

2. Validate Need. Army officials processing HSPD-12 actions for CAC issuance must check OPM’s CVS or JPAS before initiating a request for a new investigation. These systems allow the official to determine if the individual already has a favorable adjudication that meets the HSPD-12 credentialing requirement.

a. If no record exists of a favorable adjudication that meets the HSPD-12 credentialing requirement, the sponsoring activity must ensure that the applicant submits an eQIP for an NACI investigation, fingerprint cards and complete Optional Form 306 (OF 306) (Declaration for Federal Employment).

b. If a system shows that an NACI (equivalent or higher) investigation exists that has not been adjudicated (and the individual does not have a 24-month break in Federal service and/or Army contractor employment), sponsoring activities will coordinate with the vendor to review Standard Form 85 (Questionnaire for Non-Sensitive Positions) and OF 306 to determine the individual’s continued Federal service or Army contractor employment. The sponsoring activity may contact the DoD CAF directly or use the portal to request that the DoD CAF to adjudicate the investigation.

c. An individual whose eligibility for a security clearance was denied or revoked within the last 2 years may be CAC eligible. The sponsoring activity may request a copy of the report of investigation from OPM[2]. A review of the report may determine if the CAC may be issued based on the detailed guidelines, including disqualifying and mitigating factors, in attachments 2 and 3.

d. The DoD CAF will not render an HSPD-12 credentialing determination for an individual who has a current security clearance or is eligible for one. The portal will show “close no action,” and a DoD CAF notification will be sent to the sponsoring activity explaining that the “close no action” rationale means that the individual meets HSPD-12 credentialing requirements.

3. Reciprocity. The Army will accept reciprocally a prior NACI (equivalent or higher) investigation that has been favorably adjudicated by another Federal agency.

[2]OPM will send the sponsoring activity an INV Form 79A(Report of Agency Adjudication Action) when a report of investigation is requested. The sponsoring activity must complete and return the form to OPM to update CVS with the determination.

a. Sponsoring activities will not readjudicate credentialing determinations for individuals transferring from another DoD activity, Federal department or agency, provided that the:

(1) individual's former department or agency verifies possession of a valid personal identity verification;

(2) individual has a favorably adjudicated NACI (equivalent or higher) suitability or national security investigation documented in OPM CVS or JPAS;

(3) individual has not had a break in Federal service and/or Army contractor employment greater than 24 months; and

(4) individual has no derogatory information since the date of the last completed investigation.

b. Interim credentialing determinations are not eligible to be transferred or reciprocally accepted.

c. Reciprocity must be based on a favorable adjudication.

4. Credentialing of Non-U.S. Nationals

a. Sponsoring activities are required to apply this CAC credentialing process and adjudication standards (at attachments 2 and 3) to non-U.S. national contractor employees who are eligible for a CAC in accordance with the paragraph entitled "CAC Eligibility" on page 1. However, special considerations apply to non-U.S. nationals who are contractor employees at overseas locations.

(1) U.S.-Based Locations and U.S. Territories Other Than American Samoa and the Commonwealth of the Northern Mariana Islands. (The U.S. territories of American Samoa and the Northern Mariana Islands are not included in the term "United States.")

(a) Non-U.S. national contractor employees who have resided in the U.S. or a U.S. territory for at least 3 or more consecutive years require an NACI (equivalent or higher) investigation after employment authorization is properly verified.

(b) Non-U.S. nationals who have not resided in the U.S. or a U.S. territory for at least 3 or more consecutive years may be issued an alternative facility access identity credential, consistent with Army Regulation 190-13 (The Army Physical Security Program), chapter 8 (reference k), at the discretion of an appropriate agency official. Before an alternative identity credential may be issued:

- the individual's employment authorization must be verified; and

- an FBI fingerprint check[3] and a U.S. Citizenship and Immigration Services Check against the Systematic Alien Verification for Entitlements program must be conducted, with favorable results. The FBI fingerprint Special Agreement Check must be processed on applicable non-U.S. nationals who have not resided in the U.S. or a U.S. territory for 3 or more consecutive years using the form and instructions in attachment 5 to this enclosure, beginning on page 29.

(2) At Foreign Locations

(a) The sponsoring activity must initiate and ensure the completion of a background investigation before applying the CAC credentialing standards. However, the type of background investigation may vary based on standing treaties or other international agreements concerning identity assurance and information exchanges that exist between the United States and its allies, or agency agreements with the host country.

(b) The background investigation must be consistent with an NACI, to the extent possible, and include an FBI fingerprint check (unless prohibited by the status of forces or host nation agreements). Attachment 5 includes the form to request fingerprint processing on applicable non-U.S. nationals at overseas locations who have not resided in the U.S. or a U.S. territory for 3 or more consecutive years.

(c) Installation commanders or activity directors may choose to include additional checks as appropriate, but these checks will not be substituted for the FBI fingerprint check.

(d) As in the United States, for those non-U.S. nationals where an NACI (equivalent or higher) cannot be performed, an alternative facility access identity credential may be issued at the discretion of the installation commander or activity director, as appropriate and consistent with Army Regulation 190-13, chapter 8.

b. Whether at a U.S.-based or foreign location, reciprocity between agencies is not mandatory in the case of alternative identity credentials issued to non-U.S. nationals. Installation commanders or activity directors have the discretion to honor such credentials from other agencies.

5. Processing Background Investigations for CAC Issuance

a. Sponsoring activities will use PSIP to initiate an NACI investigation for the applicant. Select "HSPD-12" from the "Reason for Access" dropdown menu. Annotate "DODH" as the command/sponsoring activity security office identifier.

[3]Fingerprint checks automatically include checks against the FBI criminal history and named based checks, and checks against the terrorist screening database.

b. The applicant will complete Standard Form 85 for an NACI in eQIP, as well as an OF 306. The Personnel Security Investigation Center of Excellence will review the completed forms for accuracy and electronically forward the documents to OPM.

c. Simultaneously, sponsoring activities will electronically submit the applicant's fingerprint cards to OPM.

d. Sponsoring activities that are unable to electronically submit fingerprints must send the fingerprint cards to the Personnel Security Investigation Center of Excellence for electronic processing at:

DEPARTMENT OF THE ARMY
PSI Center of Excellence
ATTN: Fingerprint Team
Bldg 3240, Raritan Ave
Aberdeen Proving Ground, MD 21005-5001

e. Procedures for completing FBI fingerprint checks on applicable non-U.S. nationals are in attachment 5.

f. OPM will forward an advance fingerprint report with the FBI results to the sponsoring activity and conduct the NACI.

6. Initial Determinations for CAC Issuance. Successful scheduling of an NACI (equivalent or higher) by OPM (verified by checking JPAS or contacting OPM) and a favorable FBI fingerprint result is required for initial CAC issuance. Component Adjudicators will review FBI fingerprint results OPM received (or they may check OPM CVS for fingerprint results) and proceed as detailed in the following paragraphs:

a. The OPM FBI fingerprint results will show Record, No Record, No Pertinent Record (NI), or Unclassifiable (UF). "Record" signifies that the applicant's fingerprints are on file with the FBI. Arrest information and disposition of charges are provided, if known. "No Record" signifies no prior arrest data for the applicant in the FBI database. "NI" indicates that the applicant's name appears in the FBI database but without derogatory information. "Unclassifiable" signifies that it could not be determined if the applicant has a criminal history record because of a typographical error, illegible name or fingerprints, or missing information.

(1) If the results are "No Record" or "NI," the sponsoring activity may issue the CAC.

(2) If the results are "Record," the sponsoring activity may adjudicate based on the detailed guidelines, including disqualifying and mitigating factors contained in attachment 3, to determine if it may issue a CAC.

(3) If the results are "Unclassifiable" or "UF," the CAC will not be issued.

b. The Component Adjudicator must annotate favorable interim determinations in the portal.

7. DoD CAF Final Credentialing Determinations

a. Credentialing Determinations. The DoD CAF will enter the results of favorable adjudications (based on basic and supplemental HSPD-12 credentialing standards) in the portal. Appointed officials at sponsoring activities must regularly monitor the portal to get adjudication results.

(1) If the CAC was issued on an interim credentialing determination, the individual is authorized to keep the CAC.

(2) If an initial CAC was not issued on an interim determination, the sponsoring activity may follow local procedures for issuance of a CAC.

b. If the DoD CAF cannot render a favorable determination, it will forward the report of investigation to the Army representative at DOHA and notify the sponsoring activity it has done so. In these instances, DOHA will be responsible for rendering the final CAC credentialing determination and providing written notification to the individual.

c. Post Adjudicative Derogatory Information

(1) If, after issuance of the CAC, the sponsoring activity receives credible derogatory information that raises questions about whether a current CAC holder continues to meet applicable credentialing standards as outlined in attachments 2 and 3, the sponsoring activity will forward the information to DOHA for possible CAC revocation.

(2) In these instances, the sponsoring activity will forward the credible derogatory information via a memorandum on the sponsoring activity's letterhead (event, dates, facts, circumstances, any sponsoring activity actions and recommendations) to DOHA at:

Defense Office of Hearings and Appeals
ATTN: Chief Department Counsel
Post Office Box 3656
Arlington, VA 22203

(3) DOHA is responsible for rendering any revocation determination, conducting any subsequent appeal of such a determination in accordance with reference l, and providing written notification to the individual of its actions.

8. DOHA Credentialing Determinations

a. DOHA will receive the report of investigation from the DoD CAF.

b. DOHA will appoint a department counsel to represent the Government before the DOHA administrative judge.

c. A DOHA administrative judge will review and render a CAC credentialing determination in accordance with the procedures outlined in reference l and the detailed guidelines, including disqualifying and mitigating factors, at attachments 2 and 3.

d. Favorable and unfavorable credentialing determinations by a DOHA administrative judge will be communicated to the sponsoring activity and the DoD CAF via the portal.

e. DOHA will promptly enter final credentialing determinations with the adjudicative rational, including any disqualifying conditions or extenuating or mitigating factors, into the portal. The appointed official at the sponsoring activity will receive a concurrent notification of the final DOHA determination in writing via a memorandum on DOHA letterhead; the appointed official at sponsoring activities may then notify appropriate entities involved in the credentialing process.

f. Unfavorable credentialing determinations by DOHA will result in denial or revocation of the CAC. DOHA will provide written notification to the individual through the appointed official at sponsoring activities.

9. Reconsideration (Appeal)

a. The appeal process does not apply when a CAC is denied or revoked as a result of either an unfavorable DoD civilian suitability determination, a decision to deny or revoke eligibility for access to classified information, or ineligibility to occupy a sensitive position. An individual is already entitled to seek review of these unfavorable determinations in accordance with applicable suitability or national security procedures.

b. The individual has no right to appeal in those situations where the department or agency denies or revokes a CAC based on the results of a determination to disqualify the person from appointment in the excepted service or from working on a classified contract.

c. Individuals who have had their CAC denied or revoked may appeal the unfavorable determination to a DOHA Appeals Board following the policies and procedures in reference l.

d. DOHA will appoint a department counsel to represent the Government before the DOHA Appeals Board.

e. DOHA will promptly annotate the results of the appeal with the adjudicative rationale, including any disqualifying conditions or extenuating or mitigating factors, into the portal.

10. Accountability for Records and Disposition

a. Investigative reports and records will be handled with the highest degree of discretion. Access to such information will be afforded only to process, review, adjudicate and consider appeals associated with the issuance, denial or revocation of a CAC and to persons whose official duties require such information.

b. All records and correspondence related to CAC credentialing determinations will be uploaded to the portal.

c. The sponsoring activity, DoD CAF or DOHA may keep any investigative report that OPM provides only for the period identified in the OPM Privacy Act System of Record Notice[4]. DOHA will retain any file(s) it creates consistent with its responsibility in making credentialing determinations.

[4] http://www.ofr.gov/Privacy/2011/opm.aspx?AspxAutoDetectCookieSupport=1#cent9.

REFERENCES

a. Title 5, Code of Federal Regulations, Part 731.

b. Executive Order 13467 (Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information), July 2, 2008.

c. DoD 5200.2-R (Personnel Security Program), January 1987, Administrative Reissuance Incorporating Through Change 3, February 23, 1996.

d. Homeland Security Presidential Directive 12 (Policy for a Common Identification Standard for Federal Employees and Contractors), August 27, 2004.

e. Memorandum, U.S. Office of Personnel Management, July 31, 2008, subject: Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12.

f. DoD Manual 1000.13, Volume 1 (DoD Identification (ID) Cards: ID Card Life-Cycle), January 23, 2014.

g. Army Directive 2011-08 (Army Implementation of Homeland Security Presidential Directive-12), 26 May 2011.

h. Memorandum, Deputy Secretary of Defense, May 3, 2012, subject: DoD Central Adjudication Facilities (CAF) Consolidation.

i. Memorandum, HQDA, ODCS, G-2, 29 Jan 10, subject: Implementation of the Army Investigative Enterprise Solution (AIES) and Stand Up of the Personnel Security Investigation-Center of Excellence (PSI-CoE).

j. Memorandum, HQDA, SAMR, 26 Nov 13, subject: Adjudicator Requirements for Homeland Security Presidential Directive-12 (HSPD-12), Suitability and Fitness Determinations.

k. Army Regulation 190-13 (The Army Physical Security Program), 25 February 2011.

l. DoD Directive 5220.6 (Defense Industrial Personnel Security Clearance Review Program), January 2, 1992, Administrative Reissuance Incorporating Through Change 4, April 20, 1999.

m. Army Regulation 381-12 (Threat Awareness and Reporting Program), 4 October 2010.

n. Federal Information Processing Standards Publication 201-2 (Personal Identity Verification (PIV) of Federal Employees and Contractors,) September 5, 2013.

o. Title 5, United States Code, section 7313.

BASIC ADJUDICATIVE STANDARDS

1. TERRORISM (DOMESTIC OR INTERNATIONAL)

a. 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.

b. Conditions that could raise concern and may be disqualifying include evidence that the individual has knowingly and willfully been involved with reportable domestic terrorist contacts or foreign intelligence entities, Army counterintelligence activities, indicators, and behaviors such as described in Army Regulation 381-12 (reference m).

c. Conditions that could mitigate these concerns include:

(1) the individual did not knowingly and willfully engage in violent activities designed to overthrow the U.S. Government, or

(2) the organization was not engaged in unlawful or terrorist activities at the time of the individual's involvement.

2. PROBLEMS WITH IDENTITY VERIFICATION

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

b. Conditions that could raise concern and may be disqualifying include:

(1) the individual claimed it was not possible to provide two identity source documents from the list of acceptable documents in Form I-9 (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.

(2) the individual did not appear in person as required by Federal Information Processing Standards Publication 201-2 (reference n).

(3) a substitution occurred during the identity proofing process; the individual who appeared on one occasion was not the same person who appeared on another occasion.

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

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

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

c. No conditions may mitigate the inability to verify the applicant's identity.

3. FRAUDULENT IDENTITY INFORMATION

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

b. No conditions may mitigate submission of fraudulent information in an attempt to obtain a current credential.

4. CONCERNS ABOUT UNAUTHORIZED ACCESS

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

b. 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 that 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.

c. A CAC must not be issued if reasonable basis exists 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.

d. Conditions that could raise concern and may be disqualifying include:

(1) failure to comply with rules or regulations for the safeguarding of classified, sensitive or other protected information; and

(2) any attempt to gain unauthorized access to classified, sensitive or other protected information.

e. Conditions that could mitigate these concerns include:

(1) the person has demonstrated a favorable change in behavior since the last act or activities occurred. 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 properly handle protected information.

(2) 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.

5. UNLAWFUL OR INAPPROPRIATE USE OF IDENTITY CREDENTIALS

a. A CAC must not be issued to a person if reasonable basis exists to believe the individual will unlawfully or inappropriately use an identity credential outside the workplace. An individual's past criminal or dishonest conduct may put people, property or information systems at risk. For example, a person's conviction 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 at a U.S. Government facility.

b. Conditions that could raise concern and may be disqualifying include:

(1) a documented history of fraudulent requests for credentials or other official documentation,

(2) previous incidents during which the individual used credentials or other official documentation to circumvent rules or regulations, and

(3) a history of incidents that put physical assets or personal property at risk.

c. Conditions that could mitigate these concerns include:

(1) 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.

(2) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation.

6. UNLAWFUL, UNAUTHORIZED OR INAPPROPRIATE USE, MODIFICATION, CORRUPTION OR DESTRUCTION OF FEDERALLY CONTROLLED INFORMATION SYSTEMS

a. 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; or corrupt, destroy or engage in inappropriate uses of such systems. A CAC must not be issued to a person if reasonable basis exists to believe the individual will do so or has done so in the past.

b. Conditions that could raise concern and may be disqualifying include:

(1) illegal, unauthorized or inappropriate use of an information technology system or component; and

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

c. Conditions that could mitigate these concerns include:

(1) 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 the use of information technology systems.

(2) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation.

SUPPLEMENTAL ADJUDICATIVE STANDARDS

1. MISCONDUCT OR NEGLIGENCE IN EMPLOYMENT

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

b. Conditions that could raise concern and may be disqualifying include:

(1) history of intentional wrongdoing on the job or other acts that may pose an unacceptable risk to people, property or information systems;

(2) pattern of dishonesty or rule violations in the workplace;

(3) incident or pattern of disruptive, violent or other inappropriate behavior in the workplace;

(4) 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; and

(5) evidence of significant misuse of employer's time or resources.

c. Conditions that could mitigate these concerns include:

(1) 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.

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

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

2. CRIMINAL OR DISHONEST CONDUCT

a. 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.

b. Conditions that could raise concern and may be disqualifying include:

(1) a single serious crime or multiple lesser offenses. 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 at a U.S. Government facility.

(2) charges or admission of criminal conduct, regardless of whether the person was formally charged, prosecuted or convicted.

(3) the commission of dishonest acts (for example, accepting bribes; falsifying claims; committing theft, perjury or forgery; or attempting to obtain identity documentation without proper authorization).

(4) behavior involving 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.

(5) actions involving violence or sexual behavior of a criminal nature that poses an unacceptable risk if access is granted to federally controlled facilities and information systems. For example, convictions for sexual assault may indicate that granting a CAC poses an unacceptable risk to the life and safety of personnel at U.S. Government facilities.

(6) a history of misusing workplace information systems to distribute pornography.

(7) a history of financial irresponsibility, which 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. For example, a person's consistent failure to satisfy significant debts may indicate that granting a CAC poses an unacceptable risk to U.S. Government financial assets and information systems to which he or she will have access.

(8) the 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.

c. Conditions that could mitigate these concerns include:

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

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

(3) the receipt of improper or inadequate advice from authorized personnel or legal counsel significantly contributed to the individual's omission, concealment or

falsification of information. When confronted, the individual provided an accurate explanation and made prompt, good-faith effort to correct the situation.

(4) the individual made prompt, good-faith efforts to correct the omission, concealment or falsification before being confronted with the discrepancy.

(5) 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. MATERIAL, INTENTIONAL FALSE STATEMENT, DECEPTION OR FRAUD IN CONNECTION WITH FEDERAL OR CONTRACT EMPLOYMENT

a. 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 reliability and trustworthiness and put people, property or information systems at risk. He or she must not circumvent hiring procedures created to ensure fair and open competition through a material, intentional false statement, or through deception or fraud in connection with Federal or contract employment.

b. Conditions that could raise concern and 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 (for example, on the employment application or other employment, appointment or investigative documents, or during interviews.)

c. Conditions that could mitigate these concerns include:

(1) the behavior happened so long ago, was minor or happened under such unusual circumstances that it is unlikely to recur.

(2) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation.

4. ALCOHOL ABUSE

a. An individual's abuse of alcohol may put people, property or information systems at risk. Alcohol abuse or excessive alcohol consumption 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 the individual 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 at a U.S. Government facility.

b. Conditions that could raise concern and may be disqualifying include:

(1) a pattern of alcohol-related arrests;

(2) incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

(3) the abuse or excessive consumption of alcohol is current and continuing; and

(4) failure to follow a court order regarding alcohol education, evaluation, treatment or abstinence.

c. Conditions that could mitigate these concerns include:

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

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

(3) 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 licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

5. DRUG USE

a. An individual's abuse of drugs may put people, property or information systems at risk. Illegal use of narcotics, drugs or other controlled substances, including the 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 at a U.S. Government facility.

b. Conditions that could raise concern and may be disqualifying include:

(1) current or recent illegal drug use, or a serious narcotic or other controlled substance offense;

(2) pattern of drug-related arrests or problems in employment;

(3) possession of illegal drugs, including cultivation, processing, manufacture, purchase, sale, or distribution, or possession of drug paraphernalia;

(4) diagnosis by a duly qualified medical professional (for example, physician, clinical psychologist or psychiatrist) of drug abuse or drug dependence;

(5) evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

(6) failure to successfully complete a drug treatment program prescribed by a duly qualified medical professional;

(7) incident of any illegal drug use after formally agreeing to comply with rules or regulations prohibiting drug use; and

(8) incident of any illegal use or abuse of prescription or over-the-counter drugs.

c. Conditions that could mitigate these concerns include:

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

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

- abstaining from drug use,
- disassociating from drug-using associates and contacts, and
- changing or avoiding the environment where drugs were used.

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

(4) 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. STATUTORY OR REGULATORY BAR

a. The purpose of this standard is to verify whether contract employment is barred, or whether the contract employee is subject to a Federal employment debarment for reasons that also pose an unacceptable risk in the contracting context. If a debarment is in place for a Federal applicant, it will typically be addressed through a suitability determination. 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 United States Code section 7313 (reference o), may indicate that granting a CAC poses an unacceptable risk to persons, property and assets in U.S. Government facilities.

b. Conditions that could raise concern and may be disqualifying include:

(1) DoD, OPM or another Federal agency imposed the debarment;

(2) the suitability debarment was based on the presence of serious suitability issues; or

(3) the individual failed to register for the Selective Service, if required.

c. Conditions that could mitigate these concerns include:

(1) the applicant proves that the reason(s) for the debarment no longer exists.

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

7. TREASONOUS ACTS OR ACTIVITIES

a. Individuals entrusted with access to U.S. Government property and information systems must not put the U.S. Government at risk or provide an avenue for terrorism.

b. Conditions that could raise concern and may be disqualifying include:

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

(2) association or agreement with persons who attempt to or commit any of the acts in subparagraph 7b(1) with the specific intent to further those unlawful aims; or

(3) 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.

c. Conditions that could mitigate these concerns include:

(1) 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.

(2) 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.

(3) 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.

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

(5) the involvement in the activities in subparagraphs 7b(1)–(2) occurred for only a short period of time and was attributable to curiosity or academic interest.

HSPD-12/SUITABILITY PORTAL
INSTRUCTIONS FOR COMPLETING DD FORM 2875

a. **TYPE OF REQUEST:**

Initial – Please click this if you do not have an existing portal account.

Modification – Please click this if you currently have portal access and are requesting an additional role(s). You would also use this type of request when modifying any information (phone number/unit identification code (UIC) associated with your existing account. *NOTE: If you are changing your UIC or submitting office number (SON), please include your prior UIC or SON, along with your current UIC or SON, as required in Item 27. Optional Information.*

b. **DATE:** Enter today's date (YYYYMMDD).

c. **SYSTEM NAME:** DOD Gatekeeper Portal.

d. **LOCATION:** DOD CAF, Fort Meade, MD.

PART I (To be completed by requester)

1. **NAME:** Enter name as specified.

2. **ORGANIZATION:** Enter complete agency or company name.

3. **OFFICE SYMBOL/DEPARTMENT:** Enter any additional office information (UIC or SON).

4. **PHONE:** Enter your business phone number, including any extension.

5. **OFFICIAL E-MAIL ADDRESS:** Enter complete email address, please do not use unofficial email addresses, i.e. gmail.com.

6. **JOB TITLE AND GRADE/RANK:** Enter applicable information.

7. **OFFICIAL MAILING ADDRESS:** Enter this information in "Item 27. OPTIONAL INFORMATION" for UIC or SON.

8. **CITIZENSHIP:** Enter country/countries in which you are a current citizen.

9. **DESIGNATION OF PERSON:** Click as appropriate.

10. **IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS:** Complete information about information awareness (IA) training as specified.

11. **USER SIGNATURE:** Type or print your name and then digitally sign as specified.

12. **DATE:** Enter date form was signed.

PART II Endorsement of access by information owner, user supervisor or Government sponsor.

13. **JUSTIFICATION FOR ACCESS:** Enter all roles you are requesting. If you currently have portal access as a Security Manager, you do not need to include this role since you will be submitting a "Modification".

14. **TYPE OF ACCESS REQUIRED:** Click "AUTHORIZED."

15. **USER REQUIRES ACCESS TO:** Click "UNCLASSIFIED."

16. **VERIFICATION OF NEED TO KNOW:** Approving Supervisor will click this box.

16a. **ACCESS EXPIRATION DATE:** Enter as specified.

17. **SUPERVISOR'S NAME:** Type or print approving authority's name.

19. **SUPERVISOR'S SIGNATURE:** Approving authority will digitally sign as specified.

19. **DATE:** Enter date form was signed by approving authority.

20. **SUPERVISOR'S ORGANIZATION/DEPARTMENT:** Enter information, as requested.

20a. **SUPERVISOR'S E-MAIL ADDRESS:** Enter complete email address, please do not use unofficial email addresses (such as gmail.com).

20b. **PHONE NUMBER:** Enter business phone number, including any extension.

21. **SIGNATURE OF INFORMATION OWNER/OPR:** The user's information technology manager will digitally sign as specified.

22. **SIGNATURE OF IAO OR APPOINTEE:** User's information assurance officer (IAO) or appointee will digitally sign as specified.

23. **ORGANIZATION/DEPARTMENT:** Enter IAO or appointee information, as requested.

24. **PHONE NUMBER:** Enter IAO or appointee's business phone number, including any extension.

25. **DATE:** Enter date form was signed by IAO or appointee.

26. **NAME:** Enter user name as specified

27. **OPTIONAL INFORMATION:** Existing users do not have to enter this information unless they are requesting a new role associated with another UIC or SON. New users will have to enter applicable information as specified below. "THRU UIC" and "IMCOM" may not apply. *NOTE: Country is required for all OCONUS addresses.*

27. OPTIONAL INFORMATION *(Additional information)*

If you are requesting a HR Adjudicator or HR Role, please enter the following information in this section:

UIC:
and
SON:

If you are requesting a Security Manager Role, please enter the following information in this section:

UIC:
THRU UIC (higher headquarters):
MACOM:
Supporting IMCOM (if applicable):

All Roles will require a Mailing Address:

CONUS/OCONUS ADDRESS

1st line: ATTN XXXXXXX XXX XXX
2nd Line: Unit or Organization

CONUS ONLY: 3rd Line: Street Address
4th Line: City state Zip+4

OCONUS ONLY: 3rd Line: Unit Number
4th Line: APO/FPO (Country)

PART III – Security Manager Validates the Background Investigation or Clearance Information

Follow guidance as specified in the "INSTRUCTIONS" portion of the form. ***Note: To be approved for a "Component Adjudicator" role within the portal, the user must have a minimum of a favorably adjudicated background investigation or single scope background investigation.***

COMPLETED FORM WILL BE UPLOADED VIA THE "System Authorization Access Request (SAAR) submission site at https://cafregistration.army.mil.

Once the form has been reviewed for completeness, the DOD CATS Portal Team will provide further instructions to continue the registration process. **PLEASE DO NOT ATTEMPT TO REGISTER UNTIL THE SAAR HAS BEEN APPROVED.**

If you require assistance from the DoD Gatekeeper (CATS) portal, please contact:
whs.meade.dodcaf.mbx.dodcaf-gatekeeper-portal@mail.mil
DO NOT SEND PERSONALLY IDENTIFIABLE INFORMATION DATA TO THIS EMAIL ADDRESS

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USES: None.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST ☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID_____	DATE *(YYYYMMDD)*
SYSTEM NAME *(Platform or Applications)* DOD Gatekeeper Portal and UIC/SON Update	LOCATION *(Physical Location of System)* DOD CAF

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*	2. ORGANIZATION	
3. OFFICE SYMBOL/DEPARTMENT	4. PHONE *(DSN or Commercial)*	
5. OFFICIAL E-MAIL ADDRESS	6. JOB TITLE AND GRADE/RANK	
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP ☐ US ☐ FN ☐ OTHER	9. DESIGNATION OF PERSON ☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
☐ I have completed Annual Information Awareness Training. DATE *(YYYYMMDD)* _____

11. USER SIGNATURE	12. DATE *(YYYYMMDD)*

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR *(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)*

13. JUSTIFICATION FOR ACCESS

Requested Portal Roles: (Select all applicable roles)

____ HR Role

____ Component Adjudicator

____ Security Manager

14. TYPE OF ACCESS REQUIRED:
☒ AUTHORIZED ☐ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☒ UNCLASSIFIED ☐ CLASSIFIED *(Specify category)*
☐ OTHER _____

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. ☐	16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)*

17. SUPERVISOR'S NAME *(Print Name)*	18. SUPERVISOR'S SIGNATURE	19. DATE *(YYYYMMDD)*
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE *(YYYYMMDD)*

22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE *(YYYYMMDD)*

DD FORM 2875, AUG 2009 PREVIOUS EDITION IS OBSOLETE. Adobe Designer 9.0

26. NAME *(Last, First, Middle Initial)*
27. OPTIONAL INFORMATION *(Additional information)* If you are requesting a HR Adjudicator or HR Role, please enter the following information in this section: UIC: and SON: If you are requesting a Security Manager Role, please enter the following information in this section: UIC: THRU UIC (higher headquarters): MACOM: Supporting IMCOM (if applicable): All Roles will require a Mailing Address: CONUS/OCONUS ADDRESS 1st line: ATTN XXXXXXX XXX XXX 2nd Line: Unit or Organization CONUS ONLY: 3rd Line: Street Address 4th Line: City state Zip+4 OCONUS ONLY: 3rd Line: Unit Number 4th Line: APO/FPO (Country)

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION			
28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION *(YYYYMMDD)*	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION ☐ LEVEL I ☐ LEVEL II ☐ LEVEL III	
29. VERIFIED BY *(Print name)*	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE *(YYYYMMDD)*

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION		
TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED *(YYYYMMDD)*	PROCESSED BY *(Print name and sign)*	DATE *(YYYYMMDD)*
DATE REVALIDATED *(YYYYMMDD)*	REVALIDATED BY *(Print name and sign)*	DATE *(YYYYMMDD)*

DD FORM 2875 (BACK), AUG 2009

FINGERPRINT SPECIAL AGREEMENT CHECK (SAC) INSTRUCTIONS FOR NON-U.S. CITIZENS

This form will be completed for non-U.S. nationals who have not resided in the U.S. or a U.S. territory for 3 or more consecutive years, if permitted by host nation agreements.

1. Submit an FBI fingerprint SAC on an OFI 86C form. Complete all blocks.

2. If the foreign national does not have a Social Security number, do not complete section 4 (Social Security number).

3. In block 7 (Special Agreement Codes) - place the letter “B” for an FBI fingerprint check and, if applicable, place the letter “I” for a U.S. Citizenship and Immigration Services Check against the Systematic Alien Verification for Entitlements (SAVE) program.

4. If a U.S. Citizenship and Immigration Services Check against the SAVE program must be conducted complete block 13 (Other Information Required by Agreement).

5. If the foreign national does not have a Social Security number, attach a cover letter or memorandum to the OFI 86C that includes a:

   a. statement that the individual is a foreign national without a Social Security number, and

   b. request that OPM assign a pseudo Social Security number.

6. Submit the completed OFI 86C, cover letter/memorandum and the hard card fingerprints to OPM at:

OPM-FIS
PO Box 618
1137 Branchton Road
Boyers, PA 16018-0618
ATTN: Fingerprint SAC Department

SPECIAL AGREEMENT CHECKS (SAC)

OFI FORM 86C
MAY 2010

U.S. OFFICE OF PERSONNEL MANAGEMENT
INVESTIGATIVE SERVICES

Agency Agreement Number	OPM USE ONLY	OPM Codes	Case Number

AGENCY USE ONLY (COMPLETE ITEMS 1 THROUGH 14)

1. SUBJECT'S FULL NAME				2 DATE OF BIRTH
Last Name	First Name	Middle Name	Abbrev.	Month Day Year

3. PLACE OF BIRTH · Use the 2 letter code for the state				4 SOCIAL SECURITY NUMBER
City	County	State	Country	

5. OTHER NAMES AND DATES WHEN USED

Name	Month/Year Month To	Name	Month/Year Month/ To
Name	Month/Year Month To	Name	Month/Year Month To

6. SEX (Mark one box) ☐ Female ☐ Male	7. SPECIAL AGREEMENT CODES	8. POSITION TITLE

9 SON	10 SOI	11 IPAC-ALC NUMBER	12 ACCOUNTING DATA

13 OTHER INFORMATION REQUIRED BY AGREEMENT

(**CODE I**) Citizenship and Immigration information – Complete if Needed.
(Code not required if information is provide for subject or spouse/Co-Hab)
☐ Naturalized U.S. Citizen
☐ U.S. Citizen or national by birth, born outside the U.S. ☐ Not a U.S. Citizen

U.S. PASSPORT *current or most recent passport*			ALIEN REGISTRATION NUMBER *(if applicable)*
Number	Document Number	Expired Y☐N☐	Number

DOCUMENTATION OF U.S. CITIZENS BORN ABROAD (STATE DEPARTMENT FORM (FS) 240, DS 1350, FS 545, etc.)
Report if applicable

Date form was completed	Document Number	Place of Issuance

CITIZENSHIP CERTIFICATE (*if applicable)*

Where was this certificate issued? City/Court	State	Certificate Number	Date Issued

NATURALIZATION CERTIFICATE (*if applicable)*

Where was this certificate issued? City/Court	State	Certificate Number	Date Issued

IMMIGRATION STATUS *Place you entered the U.S.*

City	State	Country(*ies)* of citizenship

Date of entry	Type of document (I-94, etc.)	Document Number

14 Requesting Official Name and Title	Signature	Telephone Number (including area code)	Date

ADJUDICATION STANDARDS AND PROCEDURES FOR USING THE NATIONAL CRIME INFORMATION CENTER AND TERRORIST SCREENING DATABASE FOR INSTALLATION ACCESS CONTROL OF UNESCORTED, UNCLEARED CONTRACTORS

1. References:

a. Under Secretary of Defense (Intelligence) Directive-Type Memorandum (DTM) 09-12 (Interim Policy Guidance for DoD Physical Access Control), December 8, 2009, Incorporating Change 3, March 19, 2013.

b. Memorandum, Secretary of the Army, 31 October 2013, subject: Uncleared Contractor Common Access Card Credentialing and Installation Access.

c. Army Regulation 190-13 (The Army Physical Security Program), 25 February 2011.

d. Army Regulation 600-20 (Army Command Policy), 18 March 2008, incorporating Rapid Action Revision 5, 20 September 2012.

2. Purpose. This document establishes minimum Armywide standards for controlling unescorted access to Army installations for uncleared contractors who are not eligible to be issued a common access card (CAC) or other form of Department of Defense (DoD) identification card. These standards provide the framework for determining the fitness of such individuals for unescorted access to these installations. As used in this enclosure, "Army installations" means DoD installations, facilities and/or networks for which the Army is responsible for physical security. (This includes Army-managed Armed Forces Reserve Centers, Army Reserve Centers, and Army National Guard facilities subject to Department of the Army jurisdiction or administration.) A similar records check will be conducted at OCONUS locations in accordance with status of forces agreements and other theater regulations.

3. Policy

a. References 1a and 1b require that all contractors who do not possess a CAC, another Federal personal identity verification card or other authorized DoD identification card and who request unescorted access to Army installations must (i) have a validated need for such access and (ii) undergo a vetting process to determine their fitness for access.

b. Fitness for unescorted access to Army installations will be determined by an analysis of information obtained through authoritative Government data sources outlined in the references. These references require installations to query, at a minimum, the National Crime Information Center Interstate Identification Index (NCIC-III) and the Terrorist Screening Database (TSDB) to determine if the person

requesting unescorted access presents a potential threat to the good order, discipline, or health and safety on the installation. Implementation of the TSDB query is delayed until the capability becomes available to DoD.

c. Unescorted Access Determination. Army senior commanders (as defined in reference 1d) will, in the absence of an approved waiver (discussed in paragraph 4), deny uncleared contractors unescorted access to installations based on the results of the NCIC-III and TSDB checks that contain credible derogatory information indicating that the individual may present a threat to the good order, discipline, or health and safety on the installation. Such derogatory information includes, but is not limited to, the following:

(1) The NCIC-III contains criminal arrest information about the individual that causes the senior commander to determine that the individual presents a potential threat to the good order, discipline, or health and safety on the installation.

(2) The installation is unable to verify the individual's claimed identity based on the reasonable belief that the individual has submitted fraudulent information concerning his or her identity in the attempt to gain access.

(3) The individual has a current arrest warrant in NCIC, regardless of the offense or violation.

(4) The individual is currently barred from entry or access to a Federal installation or facility.

(5) The individual has been convicted of crimes encompassing sexual assault, armed robbery, rape, child molestation, production or possession of child pornography, trafficking in humans, drug possession with intent to sell or drug distribution.

(6) The individual has a U.S. conviction for espionage, sabotage, treason, terrorism or murder.

(7) The individual is a registered sex offender.

(8) The individual has a felony conviction within the past 10 years, regardless of the offense or violation.

(9) The individual has been convicted of a felony firearms or explosives violation.

(10) The individual has engaged in acts or activities designed to overthrow the U.S. Government by force.

(11) The individual is identified in the TSDB as known to be or suspected of being a terrorist or belonging to an organization with known links to terrorism or support of terrorist activity. When this capability becomes available to DoD, installation access

control personnel will strictly follow the Federal Bureau of Investigation's published engagement protocols.

d. Only Government officials whom the senior commander designates will perform fitness determinations. Designations will be in writing by duty position and codified in local guidance.

4. Access Denial Waiver Process. In cases where an uncleared contractor is denied access based on derogatory information obtained from an NCIC or NCIC-III check, senior commanders will offer the following process only if the individual requests a waiver.

a. Personnel at the access control point or visitor control center will issue the denied individual instructions on how and where to submit a waiver . The instructions will direct the individual to:

(1) obtain a certified copy of their complete criminal history, which must include all arrests and convictions.

(2) obtain a letter of support from their Government sponsor. The letter must indicate that the sponsor requests that the individual be granted unescorted access to accomplish a specific purpose, as well as the anticipated frequency and duration of such visits. If a contractor employee is terminated, the sponsor must inform the senior commander so that unescorted access to the installation is no longer authorized.

(3) complete an Installation Access Control Denial Waiver Application and provide the packet to the Government sponsor, who will be responsible for submitting the waiver application to the senior commander. All offenses must be listed, along with an explanation why the conduct should not result in denial of access to the installation. Other factors the sponsor/applicant should address are the:

- nature and seriousness of the conduct,
- circumstances (in specific) surrounding the conduct,
- length of time elapsed since the conduct,
- age of the individual at the time of the incident or conduct, and
- proof of efforts toward rehabilitation

(4) provide a current physical or email address to enable the senior commander to transmit a copy of his/her determination on the waiver request.

b. The Government sponsor will review the individual's packet for completeness and determine whether or not to endorse the request for a waiver.

c. If the Government sponsor decides to endorse the waiver, he/she must provide a letter of recommendation for the individual that addresses the conduct that caused the denial and indicate why the conduct should not prohibit the individual from being granted unescorted access to the installation. The Government sponsor will submit the packet and letter to the senior commander.

d. The senior commander will review the waiver application and render a determination that ensures proper protection of good order, discipline, and health and safety on the installation. The senior commander will provide the individual with a copy of the determination.

e. The results of the senior commander's decision will be provided to the installation Director of Emergency Services/Provost Marshal Office to ensure that applicable access control databases are updated.

f. Individuals who have had a waiver request denied may request reconsideration from the senior commander 1 year after the date of the commander's decision. Individuals may request reconsideration earlier if they can present significant information that was not available at the time of the original request or show that the basis for the original denial was overturned, rescinded or expired.