

**BY ORDER OF THE COMMANDER
HILL AIR FORCE BASE**

HILLAFB INSTRUCTION 36-812

5 SEPTEMBER 2012



Personnel

**ISSUE OF COMMON ACCESS CARDS
TO CONTRACTORS (CONTRACTOR
VERIFICATION SYSTEM)**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-Publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 75 SFS/S5

Certified by: 75 ABW/CC
(Col Sarah Zabel)

Pages: 24

This instruction implements and provides detailed instructions on the usage of the Contractor Verification System (CVS). Installation Points of Contact (IPOC), Trusted Agent Security Managers (TASM), Trusted Agents (TA), Government Program Managers (PM) Contracting Officers (CO), Contracting Officer Representatives (COR) and Contractors may find guidance throughout this instruction guiding them on what processes, policies and procedures to follow to obtain or renew a Common Access Card (CAC) identification. The policies within this instruction apply to all personnel employed, visiting or otherwise working on Hill Air Force Base (AFB). Ensure that all records created as a result of the processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with (IAW) the Air Force Records Disposition Schedule (RDS) at <https://www.my.af.mil//afrims/afrims/afrims/rims/ctm>. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Air Force (AF) Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command.

This instruction requires the collection and maintenance of information protected by the Privacy Act of 1974. The authority to collect and maintain the records prescribed by this instruction is 10 USC 8013. Each form, format, or form letter prescribed by this instruction that requires a Privacy Act Statement (PAS), in accordance with AFI 33-332, *Air Force Privacy Act Program*, must have the PAS incorporated thereon or the PAS will be prominently posted and be provided to the requester prior to collecting this information. Privacy Act information taken from an existing privacy act system of records, which authorizes blanket use of this information for this purpose, doesn't require a PAS. Collected information is "For Official Use Only." Requests to

release privacy act information to persons or agencies outside the Department of Defense (DoD) must be in accordance with AFI 33-332. Privacy Act System of Records Notices F031 AF SP M, *Personnel Security Access Records*, and F031 AF SP O, *Documentation for Identification and Entry Authority apply*. Access at: <http://privacy.defense.gov/notices/usaf>.

- 1. General: 2
- 2. Commanders/Directors Responsibilities. 3
- 3. Service Point of Contact (SPOC) Responsibilities. 4
- 4. Installation Point of Contact (IPOC). 4
- 5. Trusted Agent Security Manager (TASM). 5
- 6. Trusted Agent (TA). 6
- 7. Government Program Manager/Contracting Officer Representative (PM/COR). . 8
- 8. Contracting Officer (CO). 9
- 9. Issuing Official Responsibilities. 10
- 10. Contractor Personnel (Applicants). 10
- 11. The 75th Air Base Wing (75 ABW) Information Protection (75 ABW/IP) office responsibilities. 10

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 12

Attachment 2—CONTRACTOR COMMON ACCESS CARD ISSUE PROCESS 15

Attachment 3—LIST OF ACCEPTABLE DOCUMENTS 23

1. General: The intent of the Contractor Verification System (CVS) is to create a secure, on-line, streamlined application process for requesting and approving the issuance of Common Access Cards (CAC) to contractor personnel while simultaneously eliminating undue government paperwork and complying with Homeland Security Presidential Directive (HSPD) 12. The Defense Manpower Data Center (DMDC) manages and provides oversight for the CVS.

1.1. HSPD 12, signed by the President on August 27, 2004, established the requirements for a common identification standard for identification credentials issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to federally controlled facilities and logical access to federally controlled information systems. The CVS supports HSPD-12’s requirements by facilitating issuance of a CAC for logical access to federally controlled information systems.

1.2. Additionally, HSPD-12 established control objectives for secure and reliable identification of Federal employees and contractors. The CVS meets these control objectives through the following procedures.

1.2.1. Common Access Cards (CAC) are issued:

1.2.1.1. To individuals whose true identity has been verified.

- 1.2.1.2. After proper authority has authorized issuance of the credential.
- 1.2.2. Only an individual with a background investigation on record is issued a credential.
- 1.2.3. An individual is issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or State government issued picture identification (ID).
- 1.2.4. Fraudulent identity source documents are not accepted as genuine and unaltered.
- 1.2.5. A person suspected or known to the government as being a terrorist is not issued a credential.
- 1.2.6. No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued.
- 1.2.7. No credential is issued unless requested by proper authority. See [Paragraph 7](#) of this instruction.
- 1.2.8. A credential remains serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked.
- 1.2.9. A single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential. This means there will be more than one government official/agency involved in the issue process so that one individual cannot request, process, clear, approve and issue an identification credential.
- 1.2.10. An issued credential is not modified, duplicated, or forged.
- 1.3. The procedures, requirements and processes in this instruction are designed to ensure the above mentioned federally mandated control objectives are met consistently. All persons appointed to positions responsible for meeting these control objectives must comply with this instruction or military or civilian punitive actions shall be taken, as appropriate.
- 1.4. It is not the intent of this instruction to duplicate the efforts of other trusted agencies that are following the approved DoD process for vetting an employee. For example, contractors who employ Facility Security Officers (FSO) with appropriate clearances and access to the Joint Personnel Access System (JPAS) are assumed to have identity proofed employees prior to creating records for them in JPAS.

2. Commanders/Directors Responsibilities.

- 2.1. Appoint Trusted Agents (TA) for his/her unit utilizing a DD Form 2875, *System Authorization Access Request (SAAR)*. Affected commanders and directors must appoint sufficient TAs to prevent any single TA from having to manage more than 100 active applicants/cardholders. **NOTE:** DMDC requires that TAs not manage more than 100 active applicants/cardholders per TA. However, exceptions can be applied for to the Service Point of Contact (SPOC) through the Installation Point of Contact (IPOC).
- 2.2. Reverify TA appointment status/eligibility every 2-years with a newly executed DD Form 2875.

2.3. Forward a memorandum or e-mail to the Trusted Agent Security Manager (TASM) revoking a TA's appointment anytime the TA:

2.3.1. Is under investigation (or has been convicted) for any offense punishable by the Uniform Code of Military Justice (UCMJ) or equivalent civilian law.

2.3.2. Has been relieved of duty.

2.3.3. Has left the military or civil service or has otherwise become disassociated with the USAF.

2.3.4. Has transferred out of the organization.

3. Service Point of Contact (SPOC) Responsibilities.

3.1. The SPOC for Hill AFB is the AF CVS Program Manager, Headquarters, Air Force Personnel Center, Chief, Defense Enrollment Eligibility Reporting System (DEERS)/Real-time Automated Personnel Identification System (RAPIDS)/Contractor Verification System (CVS) Branch (HQ AFPC/DPSIZ).

3.2. The SPOC manages the CVS for the United States Air Force, to include the following responsibilities/actions:

3.2.1. Coordinates with the DMDC and establishes sites with CVS capability.

3.2.2. Oversees TASM registration and provides other field support.

3.2.3. Works with the DMDC Security Team (DST) to register and/or remove site identifications and TASMs.

3.2.4. Creates policies, operating procedures and other supporting documentation in support of service/agency specific implementation.

4. Installation Point of Contact (IPOC).

4.1. The IPOC shall be the 75th Security Forces Squadron (75 SFS) Chief, Plans and Programs (75 SFS/S5) unless otherwise designated by the 75th Air Base Wing Commander (75 ABW/CC). Additionally, the IPOC shall:

4.1.1. Have a minimum of a favorably completed National Agency Check (NAC).

4.1.2. Be uniformed service member or Hill AFB civil servant.

4.1.3. Be a United States citizen.

4.1.4. Have not been convicted of a felony.

4.1.5. Be responsible for oversight of CVS for all of Hill AFB.

4.2. IPOC Responsibilities. The IPOC shall:

4.2.1. Appoint a primary and alternate TASM for Hill AFB.

4.2.2. Be the Hill AFB main focal point for TASMs for issues related to the CVS.

4.2.3. Be responsible for garnering advice and guidance from higher headquarters and those directly involved in policy making decisions regarding the CVS. This information shall be provided to all Hill AFB TASMs in a timely manner.

4.2.4. Provide needed advice, assistance, and training to all Hill AFB TASMs when the training is not already addressed on the CVS website.

4.2.5. Coordinate the TASM's appointment with CVS program managers. Use the customized DD Form 2875 and related SPOC instructions, ensuring the TASM is afforded appropriate access and rights to CVS in order to fulfill the requirement of the TASM position.

4.2.6. Contact the SPOC to terminate TASM access when appropriate.

4.2.7. Notify the SPOC upon appointment and/or revocation of TASM.

5. Trusted Agent Security Manager (TASM).

5.1. The TASM shall be a uniformed service member or civil servant assigned to the 75 SFS Plans and Programs Section (75 SFS/S5) unless otherwise designated by the 75 ABW/CC. Additionally, the TASM shall:

5.1.1. Be a United States (U.S.) Citizen.

5.1.2. Be a uniformed service member or Hill AFB civil servant (cannot be a contractor).

5.1.3. Be capable of sending and receiving encrypted e-mail.

5.1.4. Be a CAC holder.

5.1.5. Have a working knowledge of Hill AFB, including the base's mission.

5.1.6. Been the subject of a favorable NAC or higher investigation.

5.1.7. Complete the CVS TASM on-line training within 3-months of appointment.

5.1.8. Have not been convicted of a felony.

5.1.9. Have not knowingly been denied a security clearance or had a security clearance revoked.

5.1.10. Be trustworthy.

5.1.11. Be retainable in the TASM position for a minimum of 12-months.

5.2. TASM Responsibilities. The TASM shall:

5.2.1. Act as a TA when needed.

5.2.2. Troubleshoot CVS questions/issues for the TAs.

5.2.3. Provide training to TAs that is not already provided on the CVS website.

5.2.4. Update newly appointed individuals to DMDC Security online for TA access. Ensure only those appointed by the Unit Commanders/Directors are given access to the CVS.

5.2.5. Immediately remove TA access to CVS upon request by the Unit Commanders/Directors.

5.2.6. Monitor the number of applicants/cardholders each TA manages.

5.2.6.1. The DMDC requires that TAs not manage more than 100 active applicants/cardholders per TA. Waivers to this limit must be requested through the IPOC to the SPOC.

5.2.6.2. The DMDC recommends that TASM's control no more than 200 TAs per site.

5.2.7. Provide TAs with all the required information in order to have his/her account activated by the DMDC Support Center.

5.2.8. Transfer applicants/cardholders between TAs within the TASM's assigned site (Hill AFB), when appropriate. Appropriate reasons for transfer include:

5.2.8.1. Oversight of a specific contract permanently transfers outside of the TA's purview. In this case the TASM should wait to receive acknowledgement from the original TA prior to making the change. Regardless, the CVS will generate an automatic notice to ensure the gaining, original, and applicants/cardholders are aware of the change.

5.2.8.2. One TA is willing to temporarily cover for another TA who is not available (sick, temporary duty (TDY), leave, etc.). The key concern in this situation is whether the gaining TA is willing to accept responsibility. The TAs need not necessarily belong to the same organization. But if not, the applicants/cardholders should be transferred back to the appropriate TA upon their return. The CVS will generate an automatic notice to ensure the gaining TA, original TA, and applicants/cardholders are aware of the change.

5.2.8.3. A TA no longer works in a TA capacity.

5.2.8.4. A TA has an unmanageable number of applicants/cardholders. The DMDC requires that TAs not manage more than 100 active applicants/cardholders. See [paragraph 5.2.6.1](#) of this instruction for waiver process.

5.2.8.5. The TASM will contact the SPOC to request transfer of applicants/cardholders outside of the TASM's site.

5.2.9. Verify through a security manager or other individual with JPAS access that mandated investigative requirements have been completed before loading personnel into CVS to act as TAs.

6. Trusted Agent (TA).

6.1. A TA shall be a uniformed service member or civil servant (TA cannot be contractor). Additionally, a TA:

6.1.1. Must be a U.S. Citizen.

6.1.2. Must be in possession of a valid operational CAC.

6.1.3. Must complete the on-line TASM/TA CVS Certification Training at <http://learning.dmdc.osd.mil> within 3-months of appointment.

6.1.4. Must not have been convicted of a felony.

6.1.5. Must have favorable or higher adjudication based on a National Agency Check with Inquiries (NACI) or higher investigation.

6.1.6. Must be appointed via a DD Form 2875 by the individual's unit Commander or Director. The DD Form 2875 will be electronically processed with digital signatures.

6.1.6.1. Parts I, II, and III on the DD Form 2875 will be completed as follows.

6.1.6.1.1. Part I, blocks 1-9, 11 and 12.

6.1.6.1.2. Part II, blocks 13 and 15-20b.

6.1.6.1.2.1. The phrase, "Execute CVS TA responsibilities IAW Hill Instruction 36-812," will be typed in block 13. Also in block 13, type the TA's Social Security Account Number (SSAN). The SSAN is required to initiate the User Account.

6.1.6.1.2.2. Check "Other" in block 15 of the DD Form 2875 and type "CVS Trusted Agent" in the blank following.

6.1.6.1.3. After completion of Part II, the DD Form 2875 will be electronically forwarded via encrypted email to the 75 SFS Security Manager (75 SFS/S1S).

6.1.6.1.4. Part III, blocks 28-32 will be completed by 75 SFS/S1S.

6.1.6.2. The 75 SFS/S1S will then forward the DD Form 2875 via encrypted email to the TASM.

6.1.7. Is appointed for 24 months, unless sooner rescinded. At the 24th month anniversary a newly executed DD Form 2875 must be submitted to the TASM in order to retain access to CVS. On the 1st day of the 25th month, if an updated DD Form 2875 is not received, the TASM will revoke the TAs access to CVS.

6.2. TA Responsibilities:

6.2.1. Create contractor accounts in CVS.

6.2.2. Provide contractors with account information to log into the CVS.

6.2.3. Review completed contractor applications.

6.2.4. Approve, return (for modification), or reject the CAC ID application, as applicable.

6.2.5. Before approving a CAC application, the TA shall:

6.2.5.1. Establish the validity of the application.

6.2.5.2. Ensure accuracy of the application.

6.2.5.3. Verify, through the PM, the individual's affiliation with DoD through contract requirements.

6.2.5.4. Verify, through the PM, an established requirement to access military facilities and installations in execution of the contract.

6.2.5.5. Verify, through the PM, the need for the contractor to access DoD networks and information systems. **NOTE:** Possession of a CAC does not constitute authority

to access DoD networks or information systems. A CAC is a tool for accessing them, when authorized. Authorization for access to DoD networks or information systems is a separate process and must not be confused with this process or used in lieu of this process to issue a CAC.

6.2.5.6. If access is only needed to military facilities or installations, and not to networks and information systems, a CAC will not be issued. Contractors who do not require access to DoD networks or information systems will be issued a Defense Biometric Identification System (DBIDS) credential. Contact 75 SFS Pass and Registration (75 SFS/S5P) for instructions on applying for a DBIDS credential.

6.2.6. Conduct six month contractor reverifications as prompted by CVS.

6.2.7. Revoke CAC identifications as appropriate.

6.2.8. Approve, return or reject applications as quickly as possible; recommend this be completed within five (5) business days. The TA may approve exceptions. **NOTE:** The CVS will reject the application if not completed with 90 days.

6.2.9. Act as the unit focal point for all matters pertaining to issuance of contractor CACs and the Contractor Verification System.

6.2.10. Immediately bring any security issues or CVS access matters to the TASM's attention.

6.2.11. After being entered into the CVS as a TA, the TA shall contact the DMDC Support Center at 1-800-372-7437 and have his/her account activated and anytime thereafter when his/her account is suspended due to inactivity.

6.2.12. Ensure only contractor personnel are entered into the CVS. Separate policies, procedures and systems exist for the issuance of ID cards to civil servants, military personnel, retirees, etc. This does not preclude an individual with an additional status in DEERS from being entered into CVS as a contractor, for example a military retiree with a job as a contractor. However, never use the CVS to issue a CAC to an individual who is not a contractor.

6.2.13. All TAs shall immediately notify the TASM of any suspected compromise with the TA's account. The TASM will immediately disable the TA's account and notify the IPOC.

6.2.14. All TA accounts go inactive after 45 days of no activity. After this point, the TA will need to contact the DMDC Support Center to re-activate the TA's account.

6.2.15. All TAs shall comply with any additional Military Personnel Element (MPE), formerly known as Military Personnel Flight, requirements insofar as they do not violate existing higher echelon instructions.

6.2.16. A TA is frequently also the unit Security Manager (SM). In those cases where the TA is not the SM, the TA must develop a close working relationship with the SM to ensure information regarding contractor CAC holders is shared appropriately.

7. Government Program Manager/Contracting Officer Representative (PM/COR).

7.1. The PM/COR is the individual assigned by the agency/Contracting Officer who is responsible for oversight of a contract that provides goods or services to the U.S. Government. This individual must not be confused with the program manager assigned by the contractor. Responsibilities in this instruction are assigned to, and the responsibility of, the government PM/COR.

7.2. The government PM/COR will:

7.2.1. Ensure CAC(s) are collected from all contractor personnel upon termination of employment or contract completion. The PM/COR will ensure CAC(s) are returned to the issuing agency through the TA.

7.2.2. Ensure the TA and the appropriate contracting officer are notified if the contractor fails to turn in/account for all identification media upon completion or termination of the contract. The contracting officer is authorized to delay final payment under the contract. Ensure coordination with Wide Area Work Flow (WAWF) personnel.

8. Contracting Officer (CO).

8.1. The CO is the person with the authority to enter into, administer, and/or terminate contracts.

8.2. The CO shall:

8.2.1. Ensure AFFARS 5352.242-9000, *Contractor Access to Air Force Installations* is included in all solicitations and contracts that require contractor personnel to make frequent visits to or perform work on Air Force installations(s).

8.2.2. Ensure AFFARS 5352.242-9001, *Common Access Cards (CACs) for Contractor Personnel* is included in solicitations and contracts that require contractor personnel to meet one or both of the following criteria:

8.2.2.1. Require logical access to Department of Defense computer networks and systems in either the unclassified environment or the classified environment where authorized by governing security directives; and/or;

8.2.2.2. Perform work which requires the use of a CAC for installation entry control or physical access to facilities and buildings.

8.2.3. Ensure verification of the applicant's affiliation with DoD through contract requirements.

8.2.4. Ensure verification of an established requirement to access military facilities and installations in execution of the contract. Can be delegated. **NOTE:** At Hill AFB, CACs are only issued to contractors for logical access, i.e. access to information systems. CACs are not issued strictly for access to information systems for training purposes.

8.2.5. Ensure verification of the need for the applicant to access DoD networks and information systems. See [paragraph 6.2.5.6](#)

8.2.6. Ensure issuance of a CAC to a contractor is requested via email or memorandum to the TA IAW [Attachment 2](#) to this instruction.

8.2.7. Provide a complete listing of all contractor personnel who have been issued a CAC to the appropriate contracting officer for official file documentation. The listing will

include as a minimum: the Contract Number, Contractor Name, Contract Period of Performance, and Employee Name.

8.2.8. Maintain open communication with government PM/COR and WAWF personnel ensuring work that is invoiced has been accomplished and that CAC issues have been resolved prior to issuance of final payment in WAWF.

8.2.9. The CO shall withhold final payment if CAC(s) of contractor employees who no longer require access to the physical or logical access are not returned to the issuing office.

9. Issuing Official Responsibilities.

9.1. The CAC Issuer for Hill AFB is the 75th Force Support Squadron, Military Personnel Section Customer Support Element (75 FSS/FSMPS). The CAC Issuer is also referred to as the RAPIDS or CAC Issuing Official. The Issuing Official will:

9.1.1. Identity proof the applicant prior to issuing a CAC.

9.1.2. Verify the applicant's personnel status in DEERS.

9.1.3. Follow procedures for issue, renewal, reissuance, retrieval, duplication, and restrictions as specified in paragraph A2.5 through A2.5.7 of this instruction.

10. Contractor Personnel (Applicants).

10.1. Contractor personnel (also referred to as applicant(s) and cardholder(s)) shall provide TAs all required information in order to accomplish actions required to obtain a CAC ID. If information is denied/refused, a CAC ID will not be issued.

10.2. When a contractor does not have an e-mail address, he or she must maintain contact with the TA through the employer's FSO, Human Resource or Administrative Office.

10.3. As a general rule, contractors have seven (7) days to log into CVS from the date the TA creates the contractor's account. Unit TAs can require contractors to log in sooner, however the system will automatically disable the application after seven days.

10.4. Contractors complete and submit the on-line application to the TA within five (5) business days. The TA may approve exceptions. The maximum time allowed by the CVS is 30 days.

10.5. Upon notification of approval to receive a CAC, contractors have three (3) business days to report to an ID card facility and receive their card. TAs may approve exceptions. **NOTE:** If the card is not issued within 90 days, it will be dropped from the system.

10.6. Contractor personnel are required to notify the TA any time there is a change in status (employment terminated, new position not requiring access to a computer, etc.).

10.7. Contractor personnel are required to turn in all identification media upon termination of employment, expiration of media, or contract completion. Failure to do so could result in withholding of final payment.

11. The 75th Air Base Wing (75 ABW) Information Protection (75 ABW/IP) office responsibilities.

11.1. The 75 ABW/IP will:

- 11.2. Conduct oversight on processes in this instruction by:
 - 11.2.1. Developing a compliance checklist covering the key elements of this instruction within 30 days of publication.
 - 11.2.2. Provide the checklist to the IPOC who will disseminate it to the TASM and all TAs for use as a self-inspection checklist.
 - 11.2.3. Inspect TA processes during Information Security and Industrial Security Staff Assistance Visits (SAV) and surveys, where applicable.
 - 11.2.4. Provide commanders, directors, and staff agency chiefs with the results of inspections within the context of other reports produced covering the SAV and/or survey.
- 11.3. Conduct quality control checks on Personnel Security Questionnaires (PSQ) prior to forwarding to the Office of Personnel Management (OPM).
- 11.4. Fingerprint applicants when requested.
- 11.5. Provide a list of favorable fingerprint results as retrieved from the Case Adjudication Tracking System (CATS) to SMs weekly when possible.

SARAH E. ZABEL, Colonel, USAF
Commander, 75th Air Base Wing

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFFAR Supplement Clause 5352.242-9000, *Contractor Access to Air Force Installations*, August 2007

AFFAR Supplement Clauses 5352.242-9001, *Common Access Cards (CACs) for Contractor Personnel*, August 2004

AFI 31-101, *Integrated Defense*, 20 September 2010

AFI 31-113, *Installation Perimeter Access Control*, 26 January 2012

AFI 31-501, *Personnel Security Program Management*, 27 January 2005

AFI 33-332, *Air Force Privacy Act Program*, 16 May 2011

AFMAN 33-363, *Management of Records*, 01 March 2008

FIPS PUB 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006

Homeland Security Presidential Directive 12, 27 August 2004

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

AF IMT 1168, *Statement of Suspect/Witness/Complainant*, 01 April 1998

AF IMT 2583, *Request for Personnel Security Action*, 01 March 1987

DD Form 2875, *System Authorization Access Request (SAAR)*, 01 August 2009

Form I-9, *OMB No. 1115-0136, Employment Eligibility Verification*, 21 November 1991

INS Form I-94, *Arrival/Departure Blank Record Card*, May 2008

INS Form I-327, *Reentry Permit*, 13 February 2007

INS Form I-551, *Permanent Resident Card*, May 2010

INS Form I-571, *Refugee Travel Document*, 24 March 2006

INS Form I-688, *Temporary Resident Card*, May 1987

INS Form I-688A, *Employment Authorization Card*, May 1987

INS Form I-688B, *Employment Authorization Document*, January 1989

INS Form N-550, *Certificate of U.S. Naturalization*, April 2004

INS Form N-560, *Certificate of U.S. Citizenship*, 1 November 1987

INS Form N-561, *Certificate of U.S. Citizenship*, April 2004

INS Form N-570, *Certificate of U.S. Naturalization*, 1 November 1987

Abbreviations and Acronyms

AFB—Air Force Base

AFCAF—Air Force Central Adjudication Facility

AFFAR—Air Force Federal Acquisition Regulation

AF IMT—Air Force Management Information Tool

AFMAN—Air Force Manual

CAC—Common Access Card

CAGE—Commercial and Government Entity Code

CATS—Case Adjudication Tracking System

CO—Contracting Officer

COR—Contracting Officer Representative

CVS—Contractor Verification System

DBIDS—Defense Biometric Identification System

DEERS—Defense Enrollment Eligibility Reporting System

DMDC—Defense Manpower Data Center

DoD—Department of Defense

DST—DMDC Security Team

FSO—Facility Security Officer

HSPD—Homeland Security Presidential Directive

IAW—In Accordance With

ID—Identification

IPOC—Installation Points of Contact

JPAS—Joint Personnel Access System

MPE—Military Personnel Element

NAC—National Agency Check

NACI—National Agency Check with Inquiries

OPR—Office of Primary Responsibility

PAS—Privacy Act Statement

PIV—Personal Identity Verification

PM—Program Manager (Government)

PSQ—Personnel Security Questionnaire

RAPIDS—Real-time Automated Personnel Identification System

RDS—Records disposition Schedule
SAV—Staff Assistance Visit
SM—Security Manager
SPOC—Service Point of Contact
SSAN—Social Security Account Number
SSM—Site Security Manager
TA—Trusted Agents
TASM—Trusted Agent Security Managers
TDY—Temporary Duty
UCMJ—Uniform Code of Military Justice
U.S.— United States
USPS—United States Postal System
URL—Uniform Resource Locator
WAWF—Wide Area Work Flow

Terms

Access Control— The process of granting or denying specific requests: 1) obtain and use information and related information processing systems; and 2) enter specific physical facilities (e.g. Federal buildings, military establishments, border crossing entrances). A function or a system that restricts access to authorized persons only.

Fitness— Level of character and conduct determined necessary for the basis of access control decisions.

Identity— The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

Identity Proofing— The process of providing or reviewing federally authorized acceptable documentation for authenticity.

NACI— A personnel security investigation combining a National Agency Check and written inquiries to law enforcement agencies, former employers, and supervisors, references and schools. All NACIs conducted for the DoD shall include a credit check.

Revocation— The process by which an issuing authority renders an issued credential useless.

Vetting— An evaluation of an applicant's or a card holder's character and conduct for approval, acceptance or denial for the issuance of an access control credential for physical access.

Attachment 2

CONTRACTOR COMMON ACCESS CARD ISSUE PROCESS

A2.1. General: The following process is a role based model for issuance of a Common Access Card (CAC) to a contractor whose duties require access to government information systems at Hill AFB. This process is based on the model provided in Federal Information Processing Standards (FIPS) Publication (PUB) 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Appendix A.

A2.2. Roles and Responsibilities: The critical roles associated with the CAC identity proofing, registration and issuance process are defined below. These roles may be additional duties assigned to personnel who have other primary duties. The following roles shall be employed for identity proofing and CAC issuance:

A2.2.1. Contractor – The individual to whom a CAC needs to be issued. Also referred to as applicant(s) and cardholder(s).

A2.2.2. Government's Program Manager (PM)/Contracting Officer (CO) – The individual who substantiates the need for a CAC to be issued to the Contractor. The PM/CO requests the issuance of a CAC to the Contractor. These duties can be delegated.

A2.2.3. Trusted Agent (TA) – The entity responsible for identity proofing of the Contractor and ensuring the successful completion of the background checks. The TA provides the final approval for the issuance of a CAC to the Contractor.

A2.2.4. CAC Issuer – The entity that performs credential personalization operations and issues the CAC to the Contractor after all identity proofing, background checks, and related approvals have been completed. The CAC Issuer is also responsible for maintaining records.

A2.3. Identity Proofing and Vetting of Contractors

A2.3.1. The PM/CO shall request CAC issuance to a contractor via email or memorandum to the TA. This can be delegated. The request for issuance shall include the following:

A2.3.1.1. Name, date of birth, position, and contact information of the applicant, contract number, contract expiration, and projected CAC expiration date.

A2.3.1.2. Signature of the PM/CO (digitally signed email or memorandum acceptable).

A2.3.2. The TA, through the SM or FSO, will check JPAS to determine if a record already exists for the applicant. If a record exists, the applicant can be considered identity proofed.

A2.3.3. If no JPAS record exists, it is the TA's responsibility to ensure the applicant is identity proofed. The importance of this step cannot be overstated.

A2.3.3.1. If the contract has an assigned FSO, the TA may contact them to initiate identity proofing. It can be assumed that an FSO is properly completing this process.

A2.3.3.2. If there is no record of the applicant in JPAS, the TA or FSO must take the following steps:

A2.3.3.2.1. Meet with the applicant in person, who will produce two forms of identity in original form. At least one shall be valid state or federal government-issued picture ID. The other must be one of the forms listed at Attachment 3.

Additionally, the TA must verify applicant's SSAN and citizenship via originally issued SSAN card and birth certificate, or some other assured source. The purpose of SSAN and citizenship verification is to facilitate creating a record of the applicant in JPAS. **NOTE:** The list at **Attachment 3** comes from the list of acceptable documents included in Form I-9, *OMB No. 1115-0136, Employment Eligibility Verification*, as required by FIPS PUB 201-1.

A2.3.3.2.2. The TA shall visually inspect the identification documents and authenticate them as being genuine and unaltered.

A2.3.3.2.3. The TA shall electronically verify the authenticity of the source document where possible.

A2.3.3.2.4. If electronic verification is not possible or available, the TA shall use other available tools, such as the *U.S. Identification Manual*, to verify the integrity of the identity source documents.

A2.3.3.2.5. The TA shall compare the picture on the identity source document with the applicant.

A2.3.3.3. If the TA cannot meet with the applicant in person due to geographic separation, seek to make arrangements with an authorized TA, SM, or IP office in proximity to the applicant. Coordinate this attempt with the internal SM, as the SM will ultimately need to be satisfied that the ID, SSAN, and citizenship verifications were properly completed by a trustworthy source in order to create a JPAS record of the applicant.

A2.3.3.4. If the above checks are successful, the SM will record the following data for each of the two identity source documents presented, to include the documentation used to verify citizenship in the remarks block on the AF IMT 2583, *Request for Personnel Security Action*, and sign it: The AF IMT 2583s will be retained on file for the length of the contract.

A2.3.3.4.1. Document Title.

A2.3.3.4.2. Document issuing authority.

A2.3.3.4.3. Document number.

A2.3.3.4.4. Document expiration date (if any).

A2.3.3.4.5. Any other information used to confirm the identity of the applicant.

A2.3.3.4.6. When verification is not completed by the SM (in most cases the TA and SM are the same person), record the name of the person who verified they completed the above requirements on behalf of the SM, i.e. the local TA or the name/organization of the person at a remote location as described in **paragraph A2.3.3.3**

A2.3.4. The TA shall compare the applicant's information contained in the CAC request (i.e., full name, date of birth, contact information) with the corresponding information provided by the applicant.

A2.3.5. Favorably Adjudicated or Submitted National Agency Check (NACI) or higher.

A2.3.5.1. The TA, through the SM or FSO, shall verify a favorably adjudicated NACI or higher investigation is recorded in JPAS.

A2.3.5.2. To verify favorable NACI through JPAS, contact the SM, who will:

A2.3.5.2.1. Review the “Adjudication Summary” section in JPAS.

A2.3.5.2.2. If eligibility states “No Determination Made,” verify if “IT” or “Public Trust” is marked “Yes” or “IT 3” under the “Suitability and Trustworthiness” section.” If so, the NACI is favorable based on the unit commander’s suitability determination.

A2.3.5.2.3. If the “Public Trust” and “IT” links are marked “N/A”, contact 75 ABW/IP for further guidance. The 75 ABW/IP office will send a Contractor Suitability package to the applicable commander/civilian leader for review and suitability determination. The Contractor Suitability package includes detailed actions to be taken by unit Commanders/Directors in making suitability assessments and provides instructions for maintaining required suitability documentation.

A2.3.5.3. If favorable adjudication cannot be verified, the SM or FSO must initiate the process by submitting an AF IMT 2583 on the applicant following applicable Personnel Security procedures.

A2.3.5.3.1. Once the investigation package is initiated, a CAC cannot be issued until JPAS reflects verified submission of the NACI. Verified submission means 75 ABW/IP has forwarded the Personnel Security Questionnaire (PSQ) to the Office of Personnel Management (OPM). The SM must monitor the investigation to ensure it opens at OPM.

A2.3.5.3.2. There are three fields within the JPAS Person Summary which can be used to verify the NACI was submitted: PSQ Sent, Open Investigation, and Adjudication Summary.

A2.3.5.3.2.1. PSQ Sent Date: This field verifies the NACI was submitted when 75 ABW/IPP or another authorized submitter has populated it with the date the investigation was sent to OPM.

A2.3.5.3.2.2. Open Investigation: This field verifies the NACI was submitted when OPM has populated it with the date the investigation was opened.

A2.3.5.3.2.3. Adjudication Summary: This field verifies the NACI was submitted when the Air Force Central Adjudication Facility (AFCAF) populates it with an entry indicating the NACI is pending adjudication, or adjudication of “favorable” or higher is provided.

A2.3.6. Favorable Fingerprinting.

A2.3.6.1. If a favorable adjudicated NACI is verified through JPAS, the assumption can be made that fingerprints have been submitted with no issues noted.

A2.3.6.2. If this cannot be verified, the TA, through the SM or FSO, shall either:

A2.3.6.2.1. Direct the applicant to schedule an appointment for fingerprinting through the 75th Air Base Wing Information Protection, Personnel Security office (75 ABW/IPP).

A2.3.6.2.2. Or, provide the applicant a blank FD 258, *Applicant Fingerprint Card*, and have the fingerprinting completed at 75 SFS/S5P or their local police department.

A2.3.6.3. Verification of favorable fingerprint results must be made before initiation of the CVS application process. To meet this requirement, the 75 ABW/IP will:

A2.3.6.3.1. Provide a list of favorable fingerprint results as retrieved from the CATS to SMs weekly when possible.

A2.3.6.3.2. The list will include the names of individuals who have been cleared in CATS for CAC issuance.

A2.3.6.3.3. The SM will be responsible for searching the list for applicant's names to ensure a issuance of an interim CAC is authorized, pending final adjudication of the NACI (or higher).

A2.3.6.3.4. The 75 ABW/IP is not authorized to release unfavorable results or determine why an individual is not showing up on the list.

A2.3.7. If the TA cannot verify favorable NACI submission and favorable fingerprint results, the CAC cannot be issued prior to favorable adjudication of the NACI as verified in JPAS.

A2.3.8. Once identity proofing and vetting (submitted or favorably adjudicated NACI or higher) is complete, the TA will initiate the CAC application process in CVS.

A2.4. Contractor Verification System (CVS) Application Process

A2.4.1. The TA will ensure the applicant is not registered as a CVS TASM or TA.

A2.4.2. The TA will complete the CAC application process following the on-screen prompts in the CVS system. Refer to the Defense Manpower Data Center (DMDC) CVS Trusted Agent User Guide.

A2.4.3. Once the application is completed, the TA uses a secure means to provide the applicant his or her user ID and temporary password and the CVS weblink Uniform Resource Locator (URL).

A2.4.3.1. Full information can be sent via encrypted email or United States Postal Service (USPS) mail to the applicant, FSO, or the PM. The PM must provide the information to the applicant via a secure means or in person.

A2.4.3.2. If other means are not practical, the weblink URL and user ID can be sent via unencrypted email. The applicant will be contacted and provided the temporary password telephonically or in person.

A2.4.4. The applicant logs on to CVS and completes his or her portion of the application following the on-screen prompts. Upon completion, the CVS will automatically notify the TA.

A2.4.4.1. As a general rule, applicants have seven (7) days to log into CVS from the date the TA creates the contractor's account. Unit TAs can require contractors to log in sooner, however the system will automatically disable the application after seven days.

A2.4.4.2. Once an initial logon is successful, the applicant must complete the application within seven (7) business days. The TA may approve exceptions. The applicant can logon and off the system as many times as necessary during this time limit. NOTE: The CVS will lock the applicant out if not completed in 30 days.

A2.4.4.3. If changes are needed once the applicant submits the completed application, the applicant must request the TA return the application.

A2.4.5. The TA will review the application in CVS. The TA can reset the password, approve the application, return it to the applicant for changes, reject, or disable it.

A2.4.6. If the TA approves the application, the CVS will automatically notify the applicant to report to the nearest RAPIDS. The notification includes a URL to find the nearest RAPIDS.

A2.4.6.1. Applicants using the Hill AFB RAPIDS (75 FSS/FSMPS) should use the following URL to schedule an appointment to avoid a potential long wait for issue: .

A2.5. CAC Issuance Process

A2.5.1. The applicant will present two forms of identification in their original form to the CAC Issuing Official to verify identity. The identity source document must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, "Employment Eligibility Verification." At least one document from the Form I-9 list shall be a valid (unexpired) State or Federal Government-issued picture identification. The identity documents will be inspected for authenticity and scanned and stored in the DEERS.

A2.5.2. The CAC Issuing Official will verify the applicant's personnel status in DEERS and issue the CAC to the expiration date established by the verified CVS record.

A2.5.3. Renewals. A CAC holder shall be allowed to apply for a renewal starting 90 days prior to the expiration of the current CAC provided a new CAC expiration date was established. The CAC Issuing Official will verify the cardholder's identity against the biometric information stored in DEERS. The applicant is required to provide two forms of identity source documents in original form as noted in [Paragraph A2.5.1](#)

A2.5.4. Reissuance. A CAC will be reissued when:

A2.5.4.1. Printed information requires change or when any of the media (including printed data, magnetic stripe, bar codes, chip, or contactless chip) becomes illegible or inoperable. The CAC Issuing Official will verify the cardholder's identity against the biometric information stored in DEERS. The applicant is required to provide two forms of identity source documents in original form as noted in paragraph A2.5.1.

A2.5.4.2. The CAC is reported lost or stolen. (Refer to [Paragraph A2.9](#))

A2.5.5. Multiple Cards. There are individuals within the DoD who have multiple personnel category codes in DEERS (e.g., an individual that is both a reservist and a contractor). These individuals shall be issued a separate CAC for each personnel category for which they are

eligible. Multiple CACs will not be issued for an individual under a single personnel category code.

A2.5.6. Retrieval. Unauthorized possession of a CAC can be prosecuted criminally under section 701 of Title 18, United States Code, which prohibits photographing or otherwise reproducing or possessing DoD identification cards in an unauthorized manner, under penalty of fine, imprisonment, or both. Invalid, inaccurate, inoperative, terminated, or expired CACs shall be returned to the CAC Issuer for disposition. The CAC is the property of the U.S. Government and shall not be retained by the cardholder upon expiration, replacement, or when the DoD affiliation of the employee has been terminated.

A2.5.7. Restrictions. The CAC shall not be amended, modified, or overprinted by any means. No stickers or other adhesive materials are to be placed on either side of the CAC. Holes shall not be punched into the CAC. The chip or laminate shall not be removed from the CAC.

A2.6. Applicant Reverification

A2.6.1. The CVS will automatically notify the TA and CAC holder when reverification is due. The TA can also check the "Reverification" tab in CVS. Reverification is directed by CVS every 180 days.

A2.6.2. The TA must contact the PM/COR or FSO and verify the contractor is still working on the contract and still requires a CAC.

A2.6.3. If the PM/COR does not verify the contractor still requires a CAC, the TA must revoke the credential.

A2.6.4. If the PM/COR verifies the contractor still requires CAC access, the TA must double-check the cardholder's favorable or higher adjudication. If all is in order, the TA follows on-screen prompts in CVS to reverify.

A2.7. Card Expiration

A2.7.1. As the card expiration date approaches and continued CAC requirement exists, the contractor must contact the government PM/CO to initiate the reissue process.

A2.7.2. Before the TA initiates the process for a new CAC to be issued, the PM/CO must verify the applicant's continued employment under the contract and valid requirement for a new CAC.

A2.8. Revocation

A2.8.1. The CAC is the property of the U.S. Government and as such the contract employee (cardholder) has no rights to retain the CAC when not required to perform on a Government contract or the U.S. Government requests its return. Hence once the U.S. Government requests the CAC be returned (through the PM/CO/COR, TA, contracting officer, or other appropriate agent) the CAC can be seized by military or civilian police, the employer, TA, PM/CO/COR, or contracting officer. However, these entities must fully understand the limitations of their legal authority in cases where the cardholder refuses or resists verbal instructions during attempts to seize the CAC. Such cases will normally be turned over to Security Forces and/or other law enforcement agencies to be resolved.

A2.8.2. The cardholder must return the government credential to the issuing agency within seven working days of one of the following: Completion or termination of employment, completion or termination of the contract, when the credential is no longer needed for contract performance, or when directed to return the CAC.

A2.8.2.1. The normal and preferred method of returning the CAC to the U.S. Government is for the cardholder to personally turn it into a RAPIDS. At Hill AFB other options include:

A2.8.2.1.1. Collection by the company and returned within seven days to the RAPIDS, PM/CO/COR, or TA. The PM/CO/COR or TA will ensure the CAC(s) are subsequently provided to the RAPIDS.

A2.8.2.1.2. The contractor can turn in the CAC(s) to the Visitor Centers located at South and West Gates, who will ensure CAC(s) are forwarded to the RAPIDS.

A2.8.2.1.3. The contractor can turn in the CAC(s) to any Security Forces post or patrol, who will ensure CAC(s) are forwarded to the RAPIDS.

A2.8.2.1.4. Upon seizure, whoever possesses the CAC will ensure it is forwarded to the RAPIDS.

A2.8.3. Contractors must notify the PM/CO/COR if a cardholder fails to comply with these requirements. In cases where the PM/CO/COR is not immediately available or situations involving misuse, refusal to return the CAC, violence, or criminal behavior, the company must also notify the TA directly. In extreme cases the company must also notify Security Forces.

A2.8.4. The PM notifies the TA and the appropriate contracting officer who is authorized to delay final payment under the contract if the contractor fails to comply with these requirements.

A2.8.5. Upon notification that a contractor has failed to comply with these requirements, the TA must:

A2.8.5.1. Immediately revoke the CAC in CVS. This triggers a series of events which include updating the DEERS to indicate the cardholder is no longer authorized and terminating the cardholder's certificates associated with electronic systems access and verification.

A2.8.5.2. Notify Security Forces so they can notify posts and patrols as well as mark the CAC in DBIDS to be seized upon contact.

A2.9. Lost CAC Procedures

A2.9.1. Operational security is every cardholder's responsibility. To prevent potential misuse or criminal activity, the following specific actions are required in order to replace a lost or stolen CAC.

A2.9.2. The cardholder must immediately report the incident to their supervisor. They must also report to their sponsoring agency security manager to complete an AF Information Management Tool (IMT) 1168, *Statement of Suspect/Witness Complainant*, or a memorandum that explains when and where the cardholder believes they lost their CAC and what actions were taken to find the card and rectify the situation.

A2.9.3. The AF IMT 1168 or memorandum must be presented to the CAC Issuing Official before the individual will be issued a new CAC.

A2.9.4. Applicants should use the following URL to schedule an appointment to avoid a potential long wait for replacement: .

A2.9.5. The CAC Issuing Official will verify the cardholder's identity against the biometric information stored in DEERS and confirm the expiration date of the missing CAC. The applicant is required to provide two forms of identity source documents in original form as noted in paragraph A2.5.1.

A2.9.6. The replacement CAC will have the same expiration date as the lost or stolen CAC.

A2.9.7. If no identity documentation is available but the picture and biometric data stored in the DEERS database can be verified by the CAC Issuing Official, a CAC can be re-issued upon additional approval of the DEERS Site Security Manager (SSM). The SSM's approval may only be given for reissuance of a lost or stolen CAC. If the picture and biometric data cannot be verified, the requirements for initial issuance apply.

A2.9.8. The CAC Issuer is responsible for keeping a copy of all lost/stolen CAC reports.

Attachment 3**LIST OF ACCEPTABLE DOCUMENTS****A3.1. Identity Proofing**

A3.1.1. U.S. Passport (unexpired).

A3.1.2. Driver's license or ID card issued by a state or outlying possession of the U.S. provided it contains a photograph or information such as name, or information such as name, date of birth, sex, height, eye color, and address.

A3.1.3. ID Card issued by federal, state, or local government agencies or entities provided it contains a photograph or information such as name, date of birth, sex, height, eye color, and address.

A3.1.4. School ID card with a photograph.

A3.1.5. Voter's registration card.

A3.1.6. U.S. Military card or draft record.

A3.1.7. Military dependent's ID card.

A3.1.8. U.S. Coast Guard Merchant Mariner Card.

A3.1.9. Native American tribal document.

A3.1.10. Driver's license issued by a Canadian government authority.

A3.1.11. INS Form N-560, *Certificate of U.S. Citizenship*, or INS Form N-561, *Certificate of U.S. Citizenship*.

A3.1.12. INS Form N-550, *Certificate of U.S. Naturalization*, or INS Form N-570, *Certificate of U.S. Naturalization*.

A3.1.13. Unexpired foreign passport, with I-551, *Permanent Resident Card*, stamp or attached INS Form I-94, *Arrival/Departure Blank Record Card*, indicating unexpired employment authorization.

A3.1.14. Unexpired INS Form I-688, *Temporary Resident Card*.

A3.1.15. Unexpired INS Form I-688A, *Employment Authorization Card*.

A3.1.16. Unexpired INS Form I-327, *Reentry Permit*.

A3.1.17. Unexpired INS Form I-571, *Refugee Travel Document*.

A3.1.18. Unexpired INS Form I-688B, *Employment Authorization Document*, issued by the INS which contains a photograph.

A3.2. SSAN Verification

A3.2.1. Originally issued SSAN card from U.S. Social Security Administration.

A3.2.2. U.S. Military ID (including family member ID and U.S. Coast Guard Merchant Mariner). **NOTE:** SSAN is being phased out from these types of IDs, leaving the U.S. Social Security Administration card as the only valid proof in the future.

A3.3. Citizenship Verification

- A3.3.1. Record in JPAS when citizenship information is included.
- A3.3.2. U.S. Passport (unexpired).
- A3.3.3. INS Form N-560 or INS Form N-561.
- A3.3.4. INS Form N-550 or INS Form N-570.
- A3.3.5. Unexpired foreign passport, with I-551 stamp or attached INS Form I-94, indicating unexpired employment authorization.
- A3.3.6. Unexpired INS Form I-551 with photograph.
- A3.3.7. Unexpired INS Form I-688.
- A3.3.8. Unexpired INS Form I-688A.
- A3.3.9. Unexpired INS Form I-327.
- A3.3.10. Unexpired INS Form I-571.
- A3.3.11. Unexpired INS Form I-688B issued by the INS which contains a photograph.