BY ORDER OF THE COMMANDER
HILL AIR FORCE BASE

HILL AIR FORCE BASE INSTRUCTION
36-3026

24 MAY 2023
Certified Current, 16 October 2023
Personnel

TRUSTED ASSOCIATE
SPONSORSHIP SYSTEM (TASS)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 75ABW/IP

Certified by: 75ABW/IP
(Mr. David W. Koontz)

Supersedes: HILLAFBI36-812, 5 September 2012

Pages: 16

This Hill Air Force Base Instruction (HILLAFBI) implements Department of the Air Force Manual (DAFMAN) 36-3026, *Air Force Trusted Associate Sponsorship System.* This publication applies to all Hill Air Force Base (AFB) host and tenant unit civilian employees, uniformed members of the Regular Air Force, Air Force Reserve, Air National Guard, United States Space Force, and those with a contractual obligation to abide by the terms of Hill AFB issuances. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using the Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level; however, all supplements must be routed to the OPR of this publication for coordination prior to certification and approval. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Department of the Air Force.

SUMMARY OF CHANGES

This document has been completely revised and must be reviewed in entirety. Major changes include series and control number changed from 36-812 to 36-3026.

1. Overview: The Trusted Associate Sponsorship System (TASS) is a secure, on-line, streamlined application process for requesting and approving the issuance of Common Access Cards (CAC) to qualifying contractors, volunteers, interns, and other eligible personnel per DoDM 1000.13 Volume 1.

1.1. TASS is managed by the Defense Manpower Data Center (DMDC) and complies with Homeland Security Presidential Directive (HSPD) 12 requirements for a common identification standard for credentials issued by the Federal government to its employees to include contractors and contractor employees.

1.2. Federal Information Processing Standards identify TASS issued Common Access Cards (CACs) serve two purposes: To provide authorization for physical access to federally controlled installations/facilities and to obtain logical access to federally controlled information systems and networks.

1.3. The Air Force TASS program is administered based on authorities derived from DoDM 1000.13, Volume 1. These authorities include a program hierarchy with the following duty positions: Air Force Service Point of Contact (SPOC), Installation Point of Contact (IPOC), Trusted Agent Security Manager (TASM) and the Trusted Agent (TA).

1.4. The TASS program is an integral component to ensuring installation physical and cyber security. Unauthorized CAC issuance or CAC retention creates an increased security risk to personnel, resources, and sensitive information. Security risks associated with the TASS program must be addressed in a time sensitive manner. The IPOC must be notified of any TASS related security incident involving Hill TASS site #174496.

2. Responsibilities.

2.1. The Service Point of Contact (SPOC) shall:

2.1.1. Establish and oversee the Hill AFB TASS site #174496 for the United States Air Force.

2.1.2. Provision Hill Trusted Agent Security Managers (TASMs) and provide TASS field support.

2.1.3. Conduct transfers of applicants/cardholders between the Hill TASS site #174496 and other Air Force TASS sites.

2.1.4. Create policies, operating procedures, and other documentation in support of service/agency specific implementation.

2.2. The Installation Point of Contact (IPOC) shall:

2.2.1. Be appointed in writing by the 75th Air Base Wing Commander (75 ABW/CC) or designated representative and serve as the Hill AFB primary manager for TASS site identification #174496.

2.2.2. Meet Trusted Agent Security Manager standards per DoDM 1000.13-M-V1, para 4b, DAFMAN36-3026, para 3.3.2, Air Force TASS SOP, Sections 8.7 & 8.9 and complete TASM certification requirements within 30 days of appointment and annually until deprovisioned.

2.2.3. Maintain DD Form 2875 appointments for all active TASM and TAs; notify the SPOC of appointment and termination of installation TASMs and TAs.

2.2.4. Direct and maintain the Hill AFB TASS training program.

2.2.5. Establish an installation TASS inspection program and accomplish program assessments as directed to include:

2.2.5.1. Publish and maintain a Hill TASS compliance checklist covering the MICT and local elements of this instruction for use as a self-inspection checklist.

2.2.5.2. Provide commanders/directors feedback of unit TASS program assessment results within 15 business days.

2.2.6. Conduct periodic reviews of Trusted Agent records and remove those with no applicant/contractors assigned after 30 days.

2.3. The Unit Commander/Director shall:

2.3.1. Ensure sufficient unit Trusted Agents (TA) are assigned to comply with DMDC standards for active applicant/cardholder account limits and exceptions to policy are submitted per DAFMAN36-3026, para 1.2, in the approved waiver format to the Service Point of Contact (SPOC) and copy the Installation Point of Contact (IPOC).

2.3.2. Ensure unit oversight of TASS program requirements in coordination/cooperation with the respective Contracting Officer/Program Manager, Security Officer/Manager, and Trusted Agent. TASS oversight requirements are multi-disciplinary and not exclusively the responsibility of a single functional representative (contracting, security, personnel, etc).

2.3.3. Provide a memorandum or e-mail notification to the IPOC and applicable TASMs when a unit TA is revoked due to the following:

2.3.3.1. Has been relieved of TA duties for cause due to an investigation or conviction for any offense punishable by the Uniform Code of Military Justice (UCMJ) or equivalent civilian law.

2.3.3.2. Has left the unit or has otherwise become disassociated with the US Air Force.

2.4. The Trusted Agent Security Manager (TASM) shall:

2.4.1. Meet Trusted Associate Sponsorship System qualifications per DoDM 1000.13-M-V1, para 4b, DAFMAN36-3026, para 3.3.2, Air Force TASS SOP, Sections 8.7 & 8.9 and local requirements as follows:

2.4.1.1. Complete the TASS TASM on-line DMDC training within 30 days of appointment and annually until deprovisioned.

2.4.2. Perform TASM duties and responsibilities per DAFMAN36-3026, para 2.5 and local requirements as follows:

2.4.2.1. Act as a TA when needed.

2.4.2.2. Troubleshoot TASS questions/issues for the TAs.

2.4.2.3. Provide refresher training to TAs for TASS site/installation specific policy or requirements not provided on the TASS website or DMDC annual training.

2.4.2.4. Use Enterprise Management and Monitoring of Accounts (EMMA) to update newly appointed individuals to DMDC Security online for TA access.

2.4.2.5. Remove TA access to TASS upon request by authorized Commanders/Directors.

2.4.2.6. Monitor the number of applicants/cardholders each TA manages; coordinate on waiver requests sent to the IPOC/SPOC.

2.4.2.7. Provide TAs with required information to activate their account by the DMDC Support Center.

2.4.2.8. Verify newly appointed TAs meet security investigative requirements before provisioning them in TASS.

2.4.2.9. Transfer applicants/cardholders between TAs within the Hill TASS site to include:

2.4.2.9.1. When a TA is willing to temporarily cover for another TA who is not available (sick, temporary duty (TDY), leave, etc.). In these situations, the gaining TA must be 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 TASS will generate an automatic notice to ensure the gaining TA, original TA, and applicants/cardholders are aware of the change.

2.4.2.9.2. When a TA no longer works in a TA capacity.

2.4.2.9.3. When a TA has an unmanageable number of applicants/cardholders.

2.4.2.10. Notify the IPOC as soon as practicable in advance when they are unable to perform TASS duties due to scheduled absences (leave, TDY, etc) and immediately for any unscheduled absences.

2.5. The Trusted Agent (TA) shall:

2.5.1. Meet Trusted Agent qualifications per DoDM 1000.13-M-V1, para 4c, DAFMAN363026, para 3.3.3, Air Force TASS SOP, Sections 8.7 & 8.9 and local requirements as follows:

2.5.1.1. Complete the TASS TA on-line DMDC training within 30 days of appointment and annually until deprovisioned.

2.5.1.2. Be appointed by the unit Commander/Director and submit a completed/approved DD Form 2875 to the IPOC (the DD Form 2875 is the only approved appointment method).

2.5.2. TA Responsibilities:

2.5.2.1. In coordination/cooperation with the designated Contracting Officer, Program Manager, and Security Officer/Manager, ensure applicants meet TASS program requirements to include:

2.5.2.1.1. Establish the validity of the application.

2.5.2.1.2. Ensure accuracy of the application.

2.5.2.1.3. Verify, through the PM/COR/Government Official, the individual's affiliation with the DoD through contract requirements prior to CAC issuance to include:

2.5.2.1.3.1. Verify, through the PM/COR/Government Official, an established requirement to access a military installation in execution of the contract. If physical access is only required for Hill AFB and no logical access to DoD networks/information systems will be granted, a CAC will not be issued. Contact 75 SFS Pass and Registration (75 SFS/S5P) for instructions on applying for a Defense Biometric Identification System (DBIDS) credential.

2.5.2.1.3.2. Verify, through the PM/COR/Government Official, an established requirement to access a military installation and DoD networks/information systems in execution of the contract. If physical and logical access to a military installation and DoD networks/information systems are both required, a CAC will be issued based on justification identified in the contract Performance Work Statement (PWS), Statement of Work (SOW), or DD Form 254. NOTE: Contractors who are exclusively remote workers and only require access to DoD networks/information systems may be issued a CAC based on justification identified in the contract Performance Work Statement (PWS), Statement of Work (SOW), or DD Form 254.

2.5.2.1.3.3. Verify, through PM/COR/Government Official, an established requirement to access multiple military installations in execution of the contract. If physical access is required for multiple military installations, with or without logical access to DoD networks/information systems, a CAC may be issued based on justification identified in the contract Performance Work Statement (PWS), Statement of Work (SOW), or DD Form 254.

2.5.2.2. Conduct 180-day contractor reverifications as prompted by TASS.

2.5.2.3. Revoke CAC identifications as appropriate.

2.5.2.4. Act as the unit focal point for all matters pertaining to issuance of contractor CACs and the Trusted Associate Sponsorship System.

2.5.2.5. Immediately bring any security issues or TASS access matters to the TASM's attention.

2.5.2.6. Log into TASS every 30 days to maintain TA account; if locked out/suspended contact the DMDC Support Center to reactivate the account. Accounts suspended longer than 120 days, except for NIPRNet Enterprise Alternative Token System (NEATS), will be terminated.

2.5.2.7. Disable approved CAC applications older than 120 days.

2.5.2.8. Process a change request for mismatches to an applicant's personnel information in TASS utilizing the change form instructions; possible changes include Date of Birth, Gender, Name, Place of Birth, and Social Security Number.

2.5.2.9. Notify a TASM immediately of any suspected compromise to the TASS TA account. The TASM will immediately disable the TA's account and notify the IPOC.

2.5.2.10. Notify the IPOC as soon as practicable when no longer performing TASS duties (separation, termination, etc).

2.6. TASS Applicants/Contractor Personnel shall:

2.6.1. Provide TAs information required to obtain a CAC; if information is denied/refused, a CAC will not be issued.

2.6.2. Maintain contact with the TA through an e-mail address.

2.6.3. As a rule, log into TASS within seven (7) days from the date the TA creates their account. Unit TAs can require contractors to log in sooner, however the system will automatically disable the application after seven days.

2.6.4. 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 TASS is 30 days.

2.6.5. Upon notification of approval to receive a CAC report to a Real-Time Automated Personnel Identification System (RAPIDS) office and receive their CAC. TAs may approve exceptions.

2.6.6. Notify the TA any time there is a change in status (employment terminated, new position not requiring access to a computer, etc.).

2.7. The Government Program Manager/Contracting Officer Representative (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 who shall:

2.7.1. Ensure CAC(s) are collected from all contractor personnel upon termination of employment or contract completion and ensure CAC(s) are returned to the issuing agency through the TA.

2.7.2. 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.

2.7.3. Provide verification to the TA in accordance with paragraphs **2.5.2.4** - **2.5.2.6**.

2.8. The Contracting Officer (CO) is the person with the authority to enter, administer, and/or terminate contracts, who shall:

2.8.1. 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).

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

2.8.2.1. 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;

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

2.8.3. Ensure verification of an established requirement to access military facilities and installations in execution of the contract.

2.8.4. Ensure a complete listing of all contractor personnel who have been issued a CAC includes as a minimum: the Contract Number, Contractor Name, Contract Period of Performance, and Employee Name.

2.8.5. 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.

2.8.6. Withhold final payment if CAC(s) of contractor employees who no longer require physical and logical access are not returned to the issuing office.

2.9. The CAC Issuing Official or RAPIDS for Hill AFB is the 75th Force Support Squadron, Military Personnel Section Customer Support Element (75 FSS/FSMPS) who shall:

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

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

2.9.3. Follow procedures for issue, renewal, reissuance, retrieval, duplication, and restrictions as specified in this instruction. ANCE

3. Installation Trusted Associate Sponsorship System Management.

3.1. General: The following procedures are utilized to manage the Hill TASS Site #174496 for Common Access Card (CAC) issuance to a contractor.

3.2. Identity Proofing and Vetting of Contractors

3.2.1. Trusted Agents will verify the CAC applicant meets the following requirement: an FBI fingerprint check with favorable results has been completed and a National Agency Check with Inquiries (NACI)/or T-1, or a DoD determined equivalent investigation, or greater, has been submitted to the Office of Personnel and Management (OPM) or designated agency. This is normally accomplished via Defense Information System for Security (DISS) or replacement security system. TA's may work with Government Security personnel to check the system. If no favorable fingerprint record is on file, terminate the application/revoke the CAC and contact 75 ABW Information Protection office to schedule a fingerprint appointment.

3.2.2. RAPIDS personnel will verify the applicant's identity with 2 valid forms of identification. list of valid forms of identification can be found on the RAPIDS website.

3.3. Trusted Associate Sponsorship System (TASS) Application Process

3.3.1. The Applicant will complete Section 1 of TASS FM 1 and send to a Government official.

3.3.2. A Government official (COR, Program Manager, etc) will check one or both blocks in Section II and sign. The Government official will send the TASS FM 1 to the TA.

3.3.3. The TA will coordinate with a Security Manager (SM) to complete Section III of the TASS FM 1.

3.3.3.1. The SM will verify the Applicant meets the following:

3.3.3.1.1. SM will verify the Applicant has at least a favorable FBI fingerprint check completed. The Applicant has at least a T1 (previously a NACI) submitted to the Office of Personnel Management within the last 10 years; then complete Section III.

3.3.3.1.2. Security Manager will initiate a T1 investigation if the Applicant does not meet the requirement in 3.3.3.1.1.

3.3.4. The TA will sign or coordinate with a COR to sign Section IV of TASS FM 1. Signing Section IV confirms the Applicant is on an Air Force Contract and is authorized a CAC. There must be at least two different government personnel to sign the different Sections of TASS FM 1. At no time can a TA or any other person sign all the Sections of the TASS FM 1.

3.3.5. The TA will Create New Application Account in TASS using the information on the TASS FM 1.

3.3.5.1. Once the application is created, in TASS, the TA will communicate the Username, Password, and a link to the TASS log-in page securely to the Applicant. Examples of, but not limited to, secure communication includes direct email, separate username and password emails, telephone call or text, or DOD SAFE site.

3.3.5.1.1. The TA can reset the password upon request of the Applicant if the situation warrants.

3.3.6. The Applicant will log into the TASS site with the username and password supplied by the TA. They will then complete all steps required by the TASS site.

3.3.7. TASS will notify the TA when the Applicant has completed their steps. The TA will perform a final check, per the TASS site, then approve the application in TASS.

3.3.8. TASS will notify the Applicant once the application is approved. The Applicant will proceed to a RAPIDS facility to obtain their CAC. Appointments and the list of required documents can be found on the RAPIDS website.

3.4. CAC Issuance

3.4.1. The Site Security Manager/Verifying Official at the RAPIDS Issuing site will verify the applicant’s personnel status in DEERS and issue the CAC to the expiration date established by the verified TASS record.

3.4.2. 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.

3.4.3. 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.

3.4.4. 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 previously noted**.**

3.5. CAC Reissuance

3.5.1. A CAC will be reissued when:

3.5.1.1. Printed information needs to be updated to include when an applicant has a change to name or gender.

3.5.1.2. When any of the media (including printed data, magnetic stripe, bar codes, chip, or contactless chip) becomes illegible or inoperable.

3.5.1.3. The CAC has been amended, modified, or overprinted by any means to include: stickers 325 or other adhesive materials placed on either side of the CAC, holes punched in the CAC, or when 326 the chip/laminate has been removed.

3.5.1.4. The CAC is reported lost or stolen.

3.5.1.4.1. If lost/stolen, the cardholder must immediately report the incident to their supervisor and TA. The TA will immediately revoke the CAC. The TA will process a CAC application in TASS.

3.6. Reverification

3.6.1. Every six months (after the CAC was approved in TASS) the Trusted Agent will receive an email from the TASS requesting reverification of the CAC. NOTE: If the CAC has not been issued, the TA will the determine the cause. This might result in the CAC application being disabled or the Contractor getting a CAC issued.

3.6.2. The Trusted Agent will coordinate with the CO, COR, PM, or Government Official to determine if the Contractor is still on contract and still requires a CAC. In addition, the TA may verify the Contractor's security eligibility/status with an approved security representative; Unit Security Manager, Facility Security Officer, Installation IP Office, etc., based on unit mission requirements.

3.6.2.1. If the Contractor is still on contract and needs a CAC, the Trusted Agent will reverify them in TASS.

3.6.2.2. If the Contractor is not on contract, the Trusted Agent will revoke the CAC in TASS.

3.6.3. Trusted Agents will track reverification utilizing any of the following methods: email, Excel spreadsheet, word document, or the AHRC TASS FORM 2.1.

3.6.4. Failure to reverify the CAC within the time limit will result in TASS automatically revoking the CAC.

3.6.5. As prescribed in AFFARS 5342.490-2, para (b)(1), contractors shall provide a listing of personnel who require a CAC to the contracting officer. The government will provide the contractor instruction on how to complete the TASS application and then notify the contractor when approved.

3.7. Revocation & Recovery of CACs

3.7.1. The Trusted Agent is notified when contractor CACs are no longer required because of six-month revalidations of issued cards reported in the TASS, the CAC is expired, or termination actions by the contractor, sponsoring organization, or contracting officials.

3.7.2. Upon notification, Trusted Agent will update the status of the card in TASS to "Revoked," if not expired, and enter information in an internally developed tracking spreadsheet to indicate the contractor CAC needs to be tracked for collection and turn-in. Trusted Agent will turn-in collected CACs to a Real-time Automated Personnel Identification System (RAPIDS) center within seven duty days.

3.7.3. If the CAC is not turned-in to the Trusted Agent, the Trusted Agent will use all reasonable methods to obtain the CAC. NOTE: If the contractor is a threat to the installation or personnel, immediately notify 75th Security Force and/or AFOSI Det 113.

3.7.3.1. Reasonable efforts include, but not limited to: Contacting the CAC holder via the contact info on TASS FM 1 and requesting the CAC be delivered to the TA, via mail or other means; contacting the Company the CAC holder was employed by and requesting the CAC be delivered to the TA, via mail or other means; or contacting the COR, PM or Government personnel to work with the Company the CAC holder was employed by, or the CAC holder, and requesting the CAC be delivered to the TA, via mail or other means.

3.7.3.2. Contractors not living in the local area can mail CACs to 75 ABW/IP at the following address: 7981 Georgia Street, Hill AFB, UT 84056.

3.7.4. Trusted Agents will notify their IT/Cyber Liaison to ensure contractor logical access is removed/terminated.

3.8. Transfer of personnel

3.8.1. CACs are linked to the person. A Contractor can keep their CAC if they are transferring to another company. Trusted Agents may request a transfer of a person's CAC (Subject) if the following is met:

3.8.1.1. The CAC has not expired, and the Subject will stay with an Air Force contractor company. NOTE: Transfer of CACs can only be done within the Air Force.

3.8.1.2. A COR/PM or Government Sponsor of the gaining contract verifies the Subject will need a CAC on that contract and a new Trusted Agent has been identified.

3.8.1.3. The losing Company agrees the Subject may retain their CAC.

3.8.2. Once the requirement has been met the Trusted Agent will:

3.8.2.1. Within the same Site ID: Contact the TA's TASM and request the transfer. The TA will provide the following: gaining TA's first and last name, and the subject's first and last name. The gaining TA will update the Subject's contract number and other information in TASS.

3.8.2.2. Outside the current Site ID: Contact the TA's TASM and request the transfer. The TA will provide the following: The gaining Site ID, gaining TA's first and last name, the losing TA's first and last name, and the subjects first and last name and social security number. The gaining TA will update the Subject's contract number and other information in TASS.

3.8.2.3. The gaining TA might request any TASS Form 1 or documentation from the losing TA.

3.8.3. TASM will:

3.8.3.1. Within the same Site ID: execute the transfer in TASS.

3.8.3.2. Outside the current Site ID: Contact the SPOC and request the transfer. The TASM will provide the following: The gaining Site ID, gaining TA's first and last name, the losing TA's first and last name, and the subjects first and last name and social security number.

3.8.4. TASM's and TA will keep a record of the transfer for 2 years. Records may be, but not limited to, email, Excel spreadsheet, word document, or the AHRC TASS FORM 2.1.

3.9. Waiver Requirements

3.9.1. Trusted Agents can only oversee 100 CAC accounts. Waivers are required over 100 CAC accounts.

3.9.2. To request a waiver, the TA or TASM will provide a letter with justification signed by the unit Commander/Director to the SPOC and copy the IPOC.

3.9.3. Trusted Agents will submit waiver requirements for any exception to DoD/AF/Hill AFB TASS policy requirements to the IPOC for review and processing.

3.10. Logical Access

3.10.1. Contractors requiring logical access to Air Force Networks will complete a DD Form 2875 during unit in processing for each system/program and submit to their unit cyber liaison.

3.10.2. Contractors will submit an updated DD Form 2875 for each approved system/program upon expiration of their CAC or not to exceed 3 years.

3.10.3. Contractors leaving Air Force employment will have their logical access to all Air Force systems/programs disabled/terminated upon notification.

3.10.4. Units will develop procedures for logical access accountability and publish them in unit policy.

3.11. Records Management

3.11.1. Trusted Agents/Program Managers will ensure all records created due to processes prescribed in this publication are maintained in accordance with Air Force Instruction (AFI) 33-322, Records Management and Information Governance Program, and disposed in accordance with Air Force Records Information Management System (AFRIMS) Table 33-42, Rule 10.00 or ga unit developed filing system.

3.11.2. Trusted Agents will ensure hard copies of TASS Form(s) with PII are properly labeled using CUI/privacy designations and are appropriately restricted to authorized unit personnel. Electronic records will be stored in a properly marked CUI folder.

3.11.3. Trusted Agents/Program Managers will ensure TASS documentation being used to support findings in a security inquiry or investigation are retained until the inquiry or investigation is closed.

3.11.4. TASS forms and documentation will utilize unit approved standardized naming conventions unless designated by higher authorities.

JEFFREY G. HOLLAND, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

Federal Information Processing Standards Publication (FIPS PUB) 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, January 2022

DoDI 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals,* 23 January 2014

DoDI 1341.02, *Defense Enrollment Eligibility Reporting System (DEERS) Program and Procedures,* 18 August 2016

DoDM 1000.13, Volume 1, *DoD Identification (ID) Cards: ID Card Life-Cycle*, 23 January 2014 DoDM 1000.13, Volume 2, *DoD Identification (ID) Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Members*, 23 January 2014

DoDM 5200.02_AFMAN 16-1405, *Air Force Personnel Security Program*, 31 July 2018

DoDM 5200.08, Volume 3, *Physical Security Program: Access to DoD Installations*, 2 January 2019

DAFI 31-101, *Integrated Defense (ID),* 24 March 2020

DAFMAN 36-3026, *Air Force Trusted Associate Sponsorship System*, 11 January 2022

AFFAR Supplement Clause 5352.242-9000, *Contractor Access to Air Force Installations*, October 2019

AFFAR Supplement Clauses 5352.242-9001, *Common Access Cards (CACs) for Contractor Personnel*, October 2019

AFI 33-322, *Records Management and Information Governance Program,* 27 July 2021

AFI 33-332, *Air Force Privacy and Civil Liberties Program, 9 March 2020*

AFI 36-3026, Volume 1, *Identification Cards For Members Of The Uniformed Services, Their Eligible Family Members And Other Eligible Personnel*, 4 August 2017

AFI 36-3026, Volume 2, *Common Access Card*, 17 May 2018

Air Force *TASS Standard Operation Policy and Procedures (SOP)*

Assistant Secretary of the Air Force Manpower and Reserve Affairs (SAF/MR), *Appointment of Headquarters and Installation Trusted Associate Sponsorship System Administrator and Installation Point of Contact (IPOC),* 12 January 2021

Prescribed Forms

None

Adopted Forms

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

DAF Form 847, *Recommendation for Change of Publication*

AHRC TASS Form 1, *TASS Applicant Registration Request*

AHRC TASS Form 2, *CAC Reverification/Retrieval Form*

Abbreviations and Acronyms

AFB—Air Force Base

AFFAR—Air Force Federal Acquisition Regulation

AHRC—Army Human Resources Command

AFI—Air Force Instruction

AFMAN—Air Force Manual

CAC—Common Access Card

CAGE—Commercial and Government Entity Code

CO—Contracting Officer

COR—Contracting Officer Representative

DAF—Department of the Air Force

DAFI—Department of the Air Force Instruction

DAFMAN—Department of the Air Force Manual

DBIDS—Defense Biometric Identification System

DEERS—Defense Enrollment Eligibility Reporting System

DISS—Defense Information System for Security

DMDC—Defense Manpower Data Center

DoD—Department of Defense

DoDI—Department of Defense Instructions

DoDM—Department of Defense Manual

EDPI—DoD Identification Number

EMMA—Enterprise Monitoring and Management of Accounts

FSO—Facility Security Officer

HILLAFBI—Hill Air Force Base Instruction

HSPD—Homeland Security Presidential Directive

IAW—In Accordance With

ID—Identification

IPOC—Installation Point of Contact

NAC—National Agency Check

NACI—National Agency Check with Inquiries

NEATS—NIPRNet Enterprise Alternative Token System

OPR—Office of Primary Responsibility

PAS—Privacy Act Statement

PIV—Personal Identity Verification

PM—Program Manager (Government)

RAPIDS—Real-Time Automated Personnel Identification System

SM—Security Manager

SPOC—Service Point of Contact

SSAN—Social Security Account Number

SSM—Site Security Manager

TA—Trusted Agents

TASS—Trusted Associate Sponsorship System

TASM—Trusted Agent Security Managers

TDY—Temporary Duty

UCMJ—Uniform Code of Military Justice

USID—Uniformed Services Identification Card

USPS—United States Postal System

URL—Uniform Resource Locator

VoLAC—Volunteer Logical Access Card

WAWF—Wide Area Work Flow

Office Symbols

75ABW—75th Air Base Wing

75ABW/CC—75th Air Base Wing Commander

75ABW/IP—75th Air Base Wing Information Protection

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.

Camera Ready—A term used to identify that a document is fully formatted and ready for printing or posting. I.e., the document is formatted by the OPR to look like an AFDPO formatted publication.

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.