Unified Washington Military Department and National Guard Policy
No. 15-01

Title:	Washington Military Department Trusted Associate Sponsorship System (TASS) - CAC/AKO Enrollment
References	Homeland Security Presidential Directive-12 (HSPD-12), The White House Federal Information Processing Standards Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors DoD Regulation 5200.2-R, Personnel Security Program Department of Defense Manual (DoDM) 1000.13, Volume 1 - DoD Identification (ID) Cards: ID Card Life-Cycle Trusted Associate Sponsorship System (TASS) Overview Guide, Defense Manpower Data Center (DMDC)
Cross-Reference Number	HR-234-10
Information Contact:	NGWA Security Specialist Building #18 (253) 512-8091
Effective Date	1 January 2015
Revised:	This Policy replaces the Washington Army National Guard Contractor Verification System SOP dated 18 August 2008 and the Washington State Employee Department of Defense Automation System Requirement Policy – CAC/AKO (HR-234-10) dated 1 October 2010.
Approved by:	Bret D. Daugherty, Major General The Adjutant General Washington Military Department Director

Purpose

This Policy establishes the procedures by which the Washington National Guard (NGWA) will implement and conduct the Trusted Associate Sponsorship System (TASS) as mandated by and in accordance with the references listed above.

Scope

This policy applies to all state and federal civilian employees of the Washington Military Department (WMD) and all members of the NGWA.

Policy

For the program to be successful and meet the enabling mandates, a concerted effort by all commanders, directors, agency heads, and supporting staff within the WMD/NGWA is required.

The TASS application, initially established in 2003 as the Contractor Verification System (CVS), was designed to standardize and automate the paper application process using DD Form 1172-2, *Application for Department of Defense (DoD) CAC Defense Enrollment Eligibility Reporting System (DEERS) Enrollment*. TASS allows the following populations within the WMD/NGWA to apply for a Common Access Card (CAC) or other government credential electronically through an approved DoD web application:

a. Affiliated Volunteers (requiring DoD Network access)

b. DoD and Uniformed Service Contractors

c. Non-Federal Agency Civilian Associates (State Employees)

1. TASS Program Background and Overview.

a. **Background.**

1) The TASS Program is a DoD initiative developed to implement the Homeland Security Presidential Directive-12 requirement to create a standard form of identification for eligible personnel. Under this program, personnel requiring "physical" access to DoD facilities or "logical" access to DoD computer networks (to include the NGWA network) in order to perform their assigned duties must be issued a CAC. The CAC serves as both a "standard form of identification" for personnel and their means of accessing a secure network.

2) CAC issuance to appropriate personnel is required to access DoD facilities and computer networks. To be issued a CAC, DoD policy requires that an appropriate authorizing official within DoD sponsor each individual and approve issuance of the CAC to him/her. TASS supports various types of government credentials such as the Volunteer Logical Access credential and the Uniformed Services ID (USID) card.

b. **Overview.**

1) TASS is a secure, web-based application hosted on a Defense Manpower Data Center (DMDC) server that allows for updating the DEERS database with DoD or other supporting agency personal data.

2) TASS updates the DEERS Person Data Repository (PDR) with personnel data and uses the DEERS Enterprise Monitoring and Management of Accounts (EMMA) website to authenticate the validity of designated and certified program managers within the TASS system.

3) It is necessary for an organization to obtain a Site ID and identify a Service or Agency Point of Contact in order to participate in the TASS system. For the purposes of TASS program implementation and operation within the NGWA, a single Site ID (175173) exists for the entire NGWA and it applies to any eligible personnel supporting NGWA activities statewide.

2. Roles and Responsibilities.

a. This section lists each of the roles within TASS. To manage the phases of the TASS process within the NGWA, three TASS user roles exist:

1) Service or Agency Point of Contact **(SPOC)**

2) Trusted Agent Security Manager **(TASM)**

3) Trusted Agent **(TA)**

b. The TASS SPOC, TASM, or TA must fulfill the responsibilities and comply with the position requirements listed for his/her role or the TASS role may be revoked. Appendix A contains a detailed discussion of duties, roles, and responsibilities of TASS critical actors in the NGWA.

3. **SPOC, TASM, and TA TASS Certification Training.** All new SPOCs, TASMs, and TAs must complete and pass the TASS Certification Training via the DMDC Learning Management System (LMS) prior to accessing the TASS system. All active SPOCs, TASMs, and TAs must complete and pass TASS Certification Training on an annual basis. When the annual training date draws closer and the SPOCs, TASMs, or TAs log in to the TASS website, they will see a notification to complete the training requirement. SPOCs, TASMs, and TAs receive notification 30 days prior to the beginning of the 30-day recertification period. Once the 30-day notification has lapsed, SPOCs, TASMs, and TAs have 30 days to complete the certification training. If they do not meet the training requirement within 30 days, TASS locks them out of the application, preventing them from performing their duties within TASS until they satisfy the training requirement. See Appendix B for a discussion of training requirements for TASS users in the NGWA.

4. **Applicant Background Vetting.** Prior to an Applicant being entered into the TASS, he or she must first be vetted by a DoD-approved process.

a. For **State Employees and Affiliated Volunteers**, a background investigation shall be initiated by the NGWA sponsoring organization's Security Manager (Army or Air) before the Applicant may be enrolled in the TASS and a CAC issued. Prior to a State Employee being approved to apply for a CAC they are required to provide the TA with a completed CAC Approval and Justification Form that will be signed by the Employee, his/her Supervisor, Division Director and Human Resources Officer (WMD Form #2022-14). The employee will work directly with the respective Security Manager for the necessary documentation and processing of their background investigation.

b. For **Contractors** with "in-state" contracts, the organization requesting the Contractor will coordinate with the appropriate Security Manager (Army or Air) for proper vetting. Contractor employees who work for a Parent Contracting company, the organization will contact the company's Facility Security Officer (FSO) to coordinate the process for the company to initiate a requisite background investigation.

c. The background security investigation documentation is considered confidential and is treated as such by all involved in processing. Personnel information contained on forms will not be shared with anyone other than the employee and Security Manager processing the paperwork. Completed documents will not be provided or retained by the employee's TA or supervisor(s). Information of this nature sent via email will be sent digitally signed and encrypted to prevent loss of personally identifiable information (PII).

d. The following criteria will apply before input into the TASS:

1) All CAC holders must at a minimum have an initiated National Agency Check with Inquiries (NACI) and a favorable completion of an FBI fingerprint check, or a DoD-

determined equivalent investigation, or greater. However, NGWA Affiliated Volunteers requiring network access are only required to have an initiated National Agency Check (NAC), and a favorable completion of an automated FBI National Criminal History Check (fingerprint check).

2) Personnel who require an ID card for physical access to a DoD Installation (e.g. ESGR Field Committee Volunteers) are eligible only for the DD Form 2765 (self-sponsored Civilian ID card) and do not require background vetting.

3) The FBI fingerprint check adjudication process may take up to four weeks to complete. The TA must confirm the favorable completion of the FBI fingerprint check before he or she creates or approves the TASS application.

Note: If a background investigation uncovers unfavorable or derogatory information, the respective NGWA Security Manager will work with the affected employee and their Human Resource Office (HRO) to process any required waivers or responses to the background investigation. If it is determined that the employee is ineligible for TASS input and CAC issuance, the employee's HRO will follow their own internal policies regarding the outcome of the employee.

e. The TA must verify through the Primary or Alternate TASM that the Applicant has initiated an appropriate background investigation. For Applicants who have had a previous background investigation, the Primary or Alternate TASM will utilize the Joint Personnel Adjudication System (JPAS) to verify the status of the background investigation. To ensure compliance, the NGWA TASMs will routinely check their assigned TAs to ensure that the Applicant verification has been completed according to DoD and DMDC guidelines.

5. CAC Application Processing.

a. Before a TA can create a new application, he or she must meet the following prerequisites:

1) Ensure the Applicant is not registered as a TASS TASM or TA.

2) Determine and verify the Applicant has a valid requirement for a CAC (WMD Form 2022-14 for State Employees).

3) Verify that the Applicant has been properly vetted.

4) Obtain the following Applicant information.

– Last Name.

– First Name.

– Middle Name.

– Person Identifier (Social Security Number).

– Email Address (Applicant's work email address, if available).

– Date of Birth.

– Personnel Category (e.g. Contractor, Non-Federal Agency Civilian Associate, Affiliated Volunteer etc...)

– Sponsoring Organization (Army or Air).

– Eligibility Expiration Date (Contract or service end date. For State Employees and Affiliated Volunteers without a known end date, the expiration date will be 3 years from the date of input.)

– Contract information (contract number and end date), if the Applicant is a Federal or State Contractor.

a. Once the TA submits a new application, a user name and password will be generated that will require the Applicant to log into the TASS website and provide further information to include the Applicant's home address and work location. The TA needs to communicate using a secure means, i.e. in person or encrypted email, to the Applicant with his or her user ID and temporary password and the TASS website URL. The Applicant can then log in to TASS to complete his or her portion of the application and submit for final review. The Applicant has seven days to complete an initial log in to TASS and begin his/her portion of the application process, or TASS will automatically disable the application.

b. When the Applicant has logged in for the first time, he or she has 30 days to complete the application process. The Applicant can save a partially completed application; however, the TA cannot process the application until the Applicant submits the complete form. Once the Applicant submits a completed application, the system automatically sends an email notification to the TA. The TA has 30 days to approve the application, otherwise the application automatically will disable. The Applicant cannot make changes to a submitted application unless the TA returns the application to the Applicant for correction.

c. After the TA receives notification that the Applicant has submitted his or her application, the TA logs in to TASS and reviews the application for final review. Upon final review, the TA can reset the Applicant's password, approve the application, return it to the Applicant for changes, reject, or disable it. Once the TA approves the application, the Applicant needs to obtain a CAC from a Real-Time Automated Personnel Identification System (RAPIDS) Issuing Facility within 90 days; otherwise, the system automatically disables the application. If the TA rejects or disables the application, the system notifies the Applicant by email and updates the appropriate status in the Applicant record. If the TA approves the application, the system updates DEERS with the Applicant information, and TASS reflects this status change in the Applicant's record.

6. **Card issuance.** Once the TA approves the application, the Applicant has 90 days to obtain a government credential from a RAPIDS Issuing Facility. Allow over 24-hours (one business day) from when the application was approved by the TA before a CAC can be issued.

7. **DEERS Updates.** TASS runs a nightly offline process to provide DEERS updates to TASS regarding government credentials and card statuses. After the RAPIDS Issuing Facility has issued a card to the Applicant, the TASS application status for the Applicant will change from "Approved" to "Issued."

8. **Applicant Reverification.** Once Applicants have received a government credential, TASS requires the TA to either reverify or revoke active Applicant records every 6 months (180 days). In addition to confirming the Applicant's personal information and continued affiliation with the NGWA for reverification, the TA must confirm the Applicant has a continued need for a government credential. TASS notifies TAs and Applicants by email when reverification is due, however, TAs should regularly access the TASS website to keep track of this requirement. A TA may also revoke an Applicant's government credential at any time. If the application is not reverified in 180 days, the application will be automatically revoked, which in turn will update DEERS and terminate the associated credentials.

9. **Eligibility Expiration.** Government credentials typically expire after 3 years or the length of an Applicant's contract as in the case of contacted personnel. If a continued need for a government credential exists as the expiration date approaches, the Applicant must contact the TA and be input into the TASS for a new CAC. Before the TA initiates the application process for a new CAC, he/she must verify the Applicant's continued employment or contract to the NGWA, and the Applicant's valid ongoing requirement for a new CAC according to applicable policies and procedures.

10. **Applicant Revocation.** The TA can revoke an active TASS Applicant record at any time. The TA performs the revocation process within TASS by selecting the "Revoke" action on the Manage Applicants screen. TASS simultaneously updates DEERS and terminates the personnel record, and DEERS subsequently terminates the card and updates the Certificate Authority (CA). The CA revokes the Applicant's certificates. The Applicant, TA, and TASM receive notice of revocation by email. At the time of revocation, the TA needs to coordinate the collection and return of the government credential and they will return it to the nearest RAPIDS Issuing Facility for proper disposal. If the TA fails to collect the government credential, the TA will notify the appointed NGWA TASM.

11. **TA Sponsorship Transfer.** The NGWA TASM can transfer Applicant sponsorship between TAs. The TASM may need to transfer sponsorship because the assigned TA is not available due to military training, illness, the TA no longer works in a TA capacity, or the TA has an unmanageable number of Applicants. The system notifies the TASMs, TAs, and affected Applicants of the TA reassignments by email. Applicant transfer requests to agencies outside of the NGWA must be submitted to the NGWA SPOC to coordinate the request appropriately with the TASS Program Office.

12. **DoD Automation Systems or Website Sponsorship.** Personnel who require access to DoD automation systems or websites in support of the NGWA, such as Army Knowledge Online (AKO), will be sponsored for these applications by their respective TA.

Appendix A.

1. **Roles and Responsibilities.**

   a. **Service or Agency Point of Contact (SPOC).**

      1) SPOCs handle the day-to-day TASS management and operation. The TASS SPOC ensures that assigned TASMs and TAs meet TASS requirements. Therefore, they should be familiar with the requirements for each role. A SPOC fulfills the following key roles:

         – Oversees TASS for NGWA.

         – Liaison between DMDC and other TASS roles.

         – Creates TASS sites.

         – Manages TASM registration and revocation.

         – Coordinates other program support/requirements.

      2) SPOC Responsibilities:

         – Administer the TASS program within the NGWA, including establishing and updating Site ID numbers and Trusted Agent Security Manager (TASM) appointments.

         – Coordinate requests for new or additional TASS capabilities between the NGWA and DMDC.

         – Use the Enterprise Monitoring and Management of Accounts (EMMA) application to register and remove Site IDs and TASMs, and ensure the currency of site and TASM information.

         – Ensure that TASMs and TAs complete all required TASS training, including both the TASS Certification Web-based Training (WBT) and the TASS training specified by the NGWA.

         – Transfer Applicants from an existing TASM/TA to another TASM/TA within the TASS website.

         – Create policies, operating procedures, and other supporting documentation in support of service- or agency-specific implementation.

         – Manage and oversee an internal Management Service that includes the following; The NGWA TASS program, all responsible TASS sites, all responsible TASM accounts, and contact information for all TASM and TA personnel.

         – Ensure assigned TASM and TA personnel have met all requirements for their roles.

         – Provide documented policies and guidelines for assigned TASMs to provide training on how TAs are to complete and maintain the sponsorship process and their responsibilities.

      (3) SPOC Position Requirements:

         – U.S. citizen.

– DoD uniformed service member, DoD Civilian, or Contractor working for the NGWA.

– CAC holder.

– Capable of sending and receiving digitally signed and encrypted email.

– Working knowledge of service or agency structure, including populations and missions of service or agency posts and sites.

– Familiar with Public Key Infrastructure (PKI), the CAC issuance process, and the NGWA TASS site account management.

– No convictions of a felony offense.

– Federal Bureau of Investigation (FBI) fingerprint check with favorable results.

– At minimum, a National Agency Check with Inquiries (NACI) background investigation performed.

– Completed the required TASS Certification Training.

– Unknowingly been denied a security clearance or had a security clearance revoked.

– Appointed in writing by the NGWA Adjutant General.

b. **Trusted Agent Security Manager (TASM).**

1) The SPOC appoints TASMs for the NGWA. This site must have a minimum of two TASMs. A TASM fulfills the following key roles:

– Administrates activities at their TASS site.

– Manages users at their TASS site.

– Oversees TAs at their TASS site.

2) TASM Responsibilities:

– Act as a TA, if required.

– Troubleshoot TASS questions and issues for his or her site.

– Manage TA users for his or her site.

– Train all TAs operating TASS.

– Provide visibility for TASS at his or her site. The TASM may accomplish this via staff call, newsletter or weblink, or another effective means. Information should include the TASS location, hours of operation, telephone numbers, and other pertinent data.

– Submit requests through his or her SPOC for new or additional TASS capability.

– Coordinate all TASS matters with his or her SPOC.

– Notify the SPOC and DMDC Support Center (DSC) of the following: TASS outages and suspected or known TASS system compromise.

– Provision, appoint, or authorize TAs in EMMA.

– Ensure positive identification of all site TAs.

3) TASM Position Requirements:

– U.S. citizen.

– DoD uniformed service member or DoD Civilian (Federal Technician) working for the NGWA.

– CAC holder.

– Capable of sending and receiving digitally signed and encrypted email.

– Working knowledge of the structure and the populations within the NGWA.

– FBI fingerprint check with favorable results.

– At minimum, a NACI background investigation performed.

– Completed the required annual TASS Certification Training.

– No convictions of a felony offense.

– Unknowingly been denied a security clearance or had a security clearance revoked.

– Not enrolled in TASS as a Contractor.

– Retainable for a minimum of 12 months.

– Appointed in writing by the SPOC.

Note: TASMs may not be Contractors. If a TASM who is also a Contractor attempts to log in to TASS as a TASM or TA, TASS will lock him or her out of the system and send an email notification to his or her SPOC, TASM, and TA.

c. **Trusted Agent (TA).**

1) A TA is a government sponsor to TASS Applicants who establishes the service or agency affiliation for registration of a CAC. TASMs identify and approve appointed TAs and then register them in TASS through the EMMA application. A TA fulfills the following key roles:

– Establishes sponsorship of the Applicant under the NGWA.

– Verifies, through the Applicant's supervisor, the need for logical or physical access to either a DoD network or facility, both initially and ongoing through semiannual re-verifications.

– Initiates the process of application for registration of a CAC.

2) TA Responsibilities:

– Establish sponsorship of Applicants under the NGWA.

– Notify the TASM or SPOC (if the TASM is unavailable) of site capability (TASS) outages.

– Notify the TASM, SPOC, or DMDC Support Center (DSC) of any suspected or known TASS system compromise.

– Be current with the TASS Certification Training requirement, which allows access to TASS to perform the duties of the TA role.

3) TA Position Requirements:

– U.S. citizen.

– DoD uniformed service member or DoD Civilian (Federal Technician) working for the NGWA.

– FBI fingerprint check with favorable results.

– At minimum, a NACI background investigation performed.

– CAC holder.

– Capable of sending and receiving digitally signed and encrypted email.

– Completed the required annual TASS Certification Training.

– No convictions of a felony offense.

– Unknowingly been denied a security clearance or had a security clearance revoked.

– Not enrolled in TASS as a Contractor.

– Appointed in writing by the SPOC.

Note: TAs may not be Contractors. If a TA who is also a Contractor attempts to log in to TASS as a TA, TASS will lock him or her out of the system and send an email notification to his or her SPOC, TASM, and TA.

Appendix B.

1. **SPOC, TASM and TA TASS Certification Training.** The NGWA TASS SPOC and all appointed TASMs and TAs within the NGWA upon their initial appointment must complete the required TASS certification training within 30 days. Re-certification will take place annually. The training is completed at the TASS DMDC learning website: https://learning2.dmdc.osd.mil/Atlas2/faces/page/login/DMDCIntro.seam?cid=4327. Once you log into the TASS DMDC learning website, the required courses will be shown under the "My Training" window.

   a. The **SPOC** must complete and pass the following training courseware on the DMDC Learning Site:

      1) TASS 001, Introduction to Web-based Training on the DMDC Learning Site.

      2) TASS 002, Trusted Associate Sponsorship System (TASS) Training Overview.

      3) TASS 005, Trusted Associate Sponsorship System (TASS) Service/Agency Point of Contact (SPOC) Training.

      4) EMMA 001, Enterprise Monitoring and Management of Accounts (EMMA) Overview.

      5) EMMA 002, Organization Functions in EMMA.

      6) EMMA 003, Role and User Functions in EMMA.

   b. The **TASM** must complete and pass the following training courseware on the DMDC Learning Site:

      1) TASS 001, Introduction to Web-based Training on the DMDC Learning Site.

      2) TASS 002, Trusted Associate Sponsorship System (TASS) Training Overview.

      3) TASS 003, Trusted Associate Sponsorship System (TASS) Trusted Agent (TA) Training.

      4) TASS 004, Trusted Associate Sponsorship System (TASS) Trusted Agent Security Manager (TASM) Training.

      5) EMMA 001, Enterprise Monitoring and Management of Accounts (EMMA) Overview.

      6) EMMA 003, Role and User Functions in EMMA.

   c. The **TA** must complete and pass the following training courseware on the DMDC Learning Site:

      1) TASS 001, Introduction to Web-based Training on the DMDC Learning Site.

      2) TASS 002, Trusted Associate Sponsorship System (TASS) Training Overview.

      3) TASS 003, Trusted Associate Sponsorship System (TASS) Trusted Agent (TA) Training.

   d. Successful completion of the training updates the SPOC, TASM or TAs profile in DEERS. If TASMs and TAs do not successfully complete the training, the TASS application does not allow them to log in. A user is given five (5) attempts to pass a

TASS certification course post-test. A failed fifth attempt locks them out of the course. To resume training, the user must call the DSC Help Desk at 1-800-372-7437 to have his or her test reset.

2. TASS Website: When the authorized user completes their required training, the TASS website can be accessed using the URL: https://www.dmdc.osd.mil/tass/.

Appendix C.

1. TASS Site Account Management.

a. Site Creation. The NGWA has a single TASS account. This TASS account is assigned a site ID (175173) which is used to manage all TASS users assigned to or employed by the WAARNG, WAANG, and WA Military Department.

b. Designating/Revoking TASMs within TASS.

1) The NGWA SPOC has two active TASMs for the Site ID at all times to ensure management of all active TA accounts and associated Applicant records.

2) The NGWA SPOC is responsible for requesting and revoking the designation of individuals to serve as TASMs for the NGWA TASS Site ID. A SPOC can remove TASM/TA accounts on the Enterprise Monitoring and Management of Accounts (EMMA) website.

3) When a new TASM is registered in EMMA, the TASM will receive an email notification prompting them to redeem their EMMA token. The TASM must redeem his or her EMMA token within the allotted time of 30 days. If the 30 day time frame is elapsed, the SPOC must log in to EMMA to provision the TASM again and generate another token email. When the EMMA token is redeemed, the TASM's TASS account is automatically activated.

4) The SPOC should immediately revoke a TASM's application and privileges if the TASM meets any of the following conditions:

– TASM is under investigation (or has been convicted) for any offense punishable by the Uniformed Code of Military Justice (UCMJ) or equivalent civilian law.

– TASM has been relieved of their full-time or military assignment.

– TASM has left military service or civil service or has otherwise become disassociated with the NGWA.

– TASM has transferred out of the organization.

c. **Activating/Deactivating TAs within TASS.**

1) The NGWA TASS TASMs are responsible for activating and deactivating individuals to serve as TAs for the NGWA TASS Site ID. To activate a new TA, the TASM will access the EMMA application and complete the on-line TA registration process. When the TASM registers a TA's account in EMMA, the TA will receive an email prompting them to redeem their EMMA token which will activate their TASS account. TAs must redeem the EMMA token within the allotted 30 days. If the 30 day time frame has elapsed, the TASM must log in to EMMA to provision the TA again, and generate another token email. To deactivate an existing TA within TASS, the TASM will log-in to the EMMA application, locate the TA in the drop-down menu, and select "remove user."

2) The TASM is the TA's primary point of contact. If a TA's account is in an inactive state, he or she will need to contact the TASM to have the account unlocked in EMMA.

3) TAs must notify the TASMs prior to departure for an extended time (one month or longer) so they can determine whether any personnel assigned to the TA within the TASS website should be temporarily reassigned to another TA.

d. **General TASS Website Account Management Procedures**.

1) CAC enabled login is the only means to access the TASS and EMMA websites by SPOCs, TASMs and TAs.

2) TASMs and TAs must ensure that they **always safeguard** the personally identifiable information (PII) of the personnel they manage within the TASS system.