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

Title:	Washington Military Department Mission Partner Identity, Credential, and Access Management (MP-ICAM)
Former Number:	Washington Military Department Trusted Associate Sponsorship System (TASS) dated 21 April 2020
References:	Homeland Security Presidential Directive-12 (HSPD-12), The White House Federal Information Processing Standards Publication 201-3, 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 Lifecycle Mission Partner Identity, Credential and Access Management (MP-ICAM) User Guide August 2023
Information Contact:	NGWA Security Specialist (253) 512-7717
Effective Date:	January 1, 2015
Mandatory Review Date:	January 15, 2029
Revised:	January 15, 2025
Approved by:	Gent Welsh, Major General The Adjutant General Washington Military Department Director

Purpose

This Policy establishes the procedures by which the Washington Military Department (WMD) will implement and conduct the Mission Partner Identity, Credential, and Access Management (MP-ICAM) system as mandated by and in accordance with the references listed above.

Scope

This policy applies to all state, federal, military, contractor, and volunteer employees of the WMD, to include members of the Washington State Guard.

Policy

For the program to be successful and meet the enabling mandates, a concerted effort by all commanders, directors, supervisors, and supporting staff within the WMD is required. MP-ICAM allows for the sponsorship and management of Department of Defense (DoD) credentials for DoD physical and/or logical (network) access for mission partners. MP-ICAM allows the following populations within the WMD to apply for a Common Access Card (CAC) or other

government credential electronically through an approved DoD web application:

(a) DoD-affiliated Volunteers

(b) DoD and Uniformed Service Contractors

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

1. MP-ICAM Program Background and Overview.

(a) **Background**.

1) The MP-ICAM application, established in 2023, is the replacement for the previously utilized Trusted Associate Sponsorship System (TASS).

2) The MP-ICAM application 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 installations/facilities or logical access to DoD computer networks to perform their assigned duties may be issued a CAC. The CAC serves as both a 'standard form of identification' for personnel and provides means of accessing a secure network.

3) To be issued a CAC, DoD policy requires that an appropriate authorizing official within the DoD sponsor each individual and approve issuance of the CAC to him/her following a routine federal background investigation.

(b) **Overview**.

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

2) MP-ICAM 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 MP-ICAM system.

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

2. Roles and Responsibilities.

(a) This section lists each of the roles within MP-ICAM. To manage the phases of the MP-ICAM process within the organization, three MP-ICAM user roles exist:

1) Service or Agency Point of Contact (SPOC)

2) Mission Partner Affiliation Sponsor Manager (MPASM)

3) Mission Partner Affiliation Sponsor (MPAS)

(b) The MP-ICAM SPOC, MPASM, or MPAS must fulfill the responsibilities and comply with the position requirements listed for his/her role or the MP-ICAM role may be

revoked. Appendix A contains a detailed discussion of roles and responsibilities of MP-ICAM critical actors in the WMD.

3. SPOC, MPASM, and MPAS MP-ICAM Certification Training.

(a) All new SPOCs, MPASMs, and MPASs must complete and pass the MP-ICAM Certification Training via the Joint Knowledge Online (JKO) website prior to accessing the MP-ICAM system.

(b) All active SPOCs, MPASMs, and MPASs must complete and pass MP-ICAM Certification Training on an annual basis. When the annual training date draws closer and the SPOCs, MPASMs, or MPASs log in to the MP-ICAM website, they will see a notification to complete the training requirement. SPOCs, MPASMs, and MPASs receive notification 30 days prior to the beginning of the 30-day recertification period. Once the 30-day notification has lapsed, SPOCs, MPASMs, and MPASs have 30 days to complete the certification training. If they do not meet the training requirement within 30 days, MP-ICAM locks them out of the application, preventing them from performing their duties within MP-ICAM until they satisfy the training requirement.

(c) See Appendix B for a discussion of training requirements for MP-ICAM users in the NGWA.

4. Applicant Background Investigation. Prior to an applicant being entered into the MP-ICAM application, they must first be vetted by a DoD-approved background investigation. In most cases, this requirement is fulfilled by a Federal Tier 1 background investigation.

(a) **State Employees and DoD-affiliated Volunteers** will provide the MPAS with a completed CAC Application-Justification of Need (WMD Form #2022-14) that will be signed by the applicant as well as their supervisor, division director, and human resources officer. A background investigation will be initiated by the sponsoring organization's Security Manager (Army or Air) before the applicant may be enrolled in MP-ICAM and a CAC issued. The applicant 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 following criteria will apply before input into the MP-ICAM:

1) Applicants must at a minimum have an initiated a Federal Tier 1 background investigation with FBI fingerprint check showing a favorable determination, or a DoD-determined equivalent investigation, or greater.

2) The FBI fingerprint check determination may take up to four weeks to complete. The MPAS must confirm the favorable completion of the FBI fingerprint check before they create or approve the applicant's MP-ICAM application.

(d) 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 applicant and security manager processing the paperwork. Completed documents will not be provided or retained by the applicant's MP-ICAM sponsor. Information of this nature will be sent via official email and digitally signed or encrypted to prevent loss of personally identifiable information (PII), if applicable.

(e) The MPAS must verify through the respective security manager that the applicant has initiated an appropriate federal background investigation. For applicants who have had a previous federal background investigation, the security manager will utilize the DoD security clearance database of record to verify the status of the background investigation. To ensure compliance, the appointed MPASMs will routinely check the MP-ICAM application to ensure the applicant vetting has been initiated/completed according to DoD guidelines.

(f) If a background investigation uncovers unfavorable or derogatory information, the respective security manager will work with the applicant and their HRO to process any required waivers or responses to the background investigation. If it is determined that the employee is ineligible for MP-ICAM input and CAC issuance, the applicant's HRO will follow their own internal policies regarding the outcome.

5. CAC Application Processing.

(a) Before a MPAS can create a new application, they must meet the following prerequisites:

1) Ensure the applicant is not registered as a MP-ICAM, MPASM, or MPAS.

2) Verify the applicant has a valid requirement for a CAC (WMD Form 2022-14 for State Employees).

3) Verify that the applicant has a background investigation.

4) Obtain the following applicant information (may be provided at the time of MP-ICAM input):

– 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, DoD-affiliated Volunteer, etc..)

– Sponsoring Organization (Army or Air)

– Eligibility Expiration Date. The end date must be before the contract end date or whatever date the sponsorship will end, up to 5 years. The sponsorship begin date is defaulted to the date of input.

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

(b) Once the MPAS submits a new application, a username and password will be generated that will require the applicant to log into the MP-ICAM website and provide further information to include the applicant's home address and work location. The MPAS 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 MP-ICAM website URL. The applicant can then log in to MP-ICAM 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 MP-ICAM and begin their portion of the application process, or MP-ICAM will automatically disable the application.

(c) When the applicant has logged in for the first time, they have 30 days to complete the application process. The applicant can save a partially completed application; however, the MPAS 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 MPAS. The MPAS has 30 days to approve the application, otherwise the application automatically will disable. The applicant cannot make changes to a submitted application unless the MPAS returns the application to the applicant for correction.

(d) After the MPAS receives notification that the applicant has submitted their application, the MPAS logs in to MP-ICAM and reviews the application for final review. Upon final review, the MPAS can reset the applicant's password, approve the application, return it to the applicant for changes, reject, or disable it. Once the MPAS 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 MPAS rejects or disables the application, the system notifies the applicant by email and updates the appropriate status in the applicant record. If the MPAS approves the application, the system updates DEERS with the applicant information, and MP-ICAM reflects this status change in the applicant's record.

6. **Card issuance.** Once the MPAS 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 MPAS before a CAC can be issued.

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

8. **Applicant Reverification.** Once applicants have received a government credential, MP-ICAM requires the MPAS to either reverify or revoke active applicant records every six months (180 days). In addition to confirming the applicant's personal information and continued affiliation with the NGWA for reverification, the MPAS must confirm the applicant has a continued need for a government credential. MP-ICAM notifies MPASs and applicants by email when reverification is due, however, MPASs should regularly access the MP-ICAM website to keep track of this requirement. A MPAS 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 contracted personnel. If a continued need for a government credential exists as the expiration date approaches, the applicant must contact the MPAS and be input into the MP-ICAM for a new CAC. Before the MPAS initiates the application process for a new CAC, he/she must verify the applicant's continued employment or contract to the organization, and the applicant's valid ongoing requirement for a new CAC according to applicable policies and procedures.

10. **Applicant Revocation.** The MPAS can revoke an active MP-ICAM applicant record at any time. The MPAS performs the revocation process within MP-ICAM by selecting the 'revoke' action on the 'manage applicants screen.' MP-ICAM 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, MPAS, and MPASM receive notice of revocation by email. At the time of revocation, the MPAS needs to coordinate the collection and return of the government credential, and return it to the nearest RAPIDS issuing facility for proper disposal. If the MPAS fails to collect the government credential, the MPAS will notify the appointed MPASM.

11. **MPAS Sponsorship Transfer.** The MPASM can transfer applicant sponsorship between MPASs. The MPASM may need to transfer sponsorship because the assigned MPAS is not available due to military training, illness, the MPAS no longer works in a MPAS capacity, or the MPAS has an unmanageable number of applicants. The system notifies the MPASMs, MPASs, and affected applicants of the MPAS reassignments by email. Applicant transfer requests to agencies outside of the WMD must be submitted to the SPOC to coordinate the request with the National Guard Bureau MP-ICAM program office.

12. **Other DoD Website or Application Sponsorship.** Personnel who require access to other official DoD websites or applications should be sponsored for these by their respective MPAS. The requirements for each may vary.

13. **Misuse of a CAC.** If an employee misuses a CAC or fails to follow the rules for access or use of federal installations or systems, the employee may be subject to disciplinary action in coordination with their HRO. If a contractor misuses a CAC or fails to follow the rules for access or use of federal installations or systems, the contractor may be subject to disciplinary action in coordination with their Contracting Officer's Representative.

Appendix A.

1. Roles and Responsibilities.

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

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

– Oversees MP-ICAM for WMD.

– Liaison between DMDC and other MP-ICAM roles.

– Creates MP-ICAM sites.

– Manages MPASM registration and revocation.

– Coordinates other program support/requirements.

2) SPOC Responsibilities:

– Coordinate requests for new or additional MP-ICAM capabilities between the National Guard and DMDC.

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

– Ensure that MPASMs and MPASs complete all required MP-ICAM training, including both the MP-ICAM Certification Web-based Training (WBT) and the MP-ICAM training specified by the WMD.

– Transfer applicants from an existing MPASM/MPAS to another MPASM/MPAS within the MP-ICAM website.

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

– Ensure assigned MPASM and MPAS personnel have met all requirements for their roles.

– Provide documented policies and guidelines for assigned MPASMs to provide training on how MPASs 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 WMD.

– 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 WMD MP-ICAM site account management.

– No convictions of a felony offense.

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

– At minimum, a Tier 1 (T1) background investigation performed.

– Completed the required MP-ICAM Certification Training.

– Has not been denied a security clearance or had a security clearance revoked.

(b) **Mission Partner Affiliation Sponsor Manager (MPASM)**.

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

– Administrates activities at their MP-ICAM site.

– Manages users at their MP-ICAM site.

– Oversees MPASs at their MP-ICAM site.

2) MPASM Responsibilities:

– Act as a MPAS, if required.

– Troubleshoot MP-ICAM questions and issues for his or her site.

– Manage MPAS users for his or her site.

– Train all MPASs operating MP-ICAM.

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

– Submit requests through their SPOC for new or additional MP-ICAM capability.

– Coordinate all MP-ICAM matters with his or her SPOC.

– Notify the SPOC and DMDC Support Center (DSC) of the following: MP-ICAM outages and suspected or known MP-ICAM system compromise within 4 hours.

– Ensure positive identification of all site MPASs.

3) MPASM Position Requirements:

– U.S. citizen.

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

– CAC holder.

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

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

– FBI fingerprint check with favorable results.

– At minimum, a Tier 1 background investigation performed.

– Completed the required annual MP-ICAM Certification Training.

– No convictions of a felony offense.

– Has not been denied a security clearance or had a security clearance revoked.

– Not enrolled in MP-ICAM as a contractor.

– Retainable for a minimum of 12 months.

Note: MPASMs may not be contractors. If a MPASM who is also a contractor attempts to log in to MP-ICAM as a MPASM or MPAS, MP-ICAM will lock him or her out of the system and send an email notification to his or her SPOC, MPASM, and MPAS.

(c) **Mission Partner Affiliation Sponsor (MPAS).**

1) A MPAS is a government sponsor to MP-ICAM applicants who establishes the service or agency affiliation for registration of a CAC. MPASMs identify and approve appointed MPASs and then register them in MP-ICAM through the EMMA application. A MPAS fulfills the following key roles:

– Establishes sponsorship of the applicant under the WMD.

– 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) MPAS Responsibilities:

– Establish sponsorship of applicants under the WMD.

– Notify the MPASM or SPOC (if the MPASM is unavailable) of site capability (MP-ICAM) outages.

– Notify the MPASM, SPOC, or DMDC Support Center (DSC) of any suspected or known MP-ICAM system compromise within 4 hours.

– Be current with the MP-ICAM Certification Training requirement, which allows access to MP-ICAM to perform the duties of the MPAS role.

– Complete applications by proxy when the applicant is unable to do so.

– Initiate new credential applications.

3) MPAS Position Requirements:

– U.S. citizen.

– DoD uniformed service member or DoD civilian (Federal Technician) working for the WMD.

– FBI fingerprint check with favorable results.

– At minimum, a Tier 1 background investigation performed.

– CAC holder.

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

– Completed the required annual MP-ICAM Certification Training.

– No convictions of a felony offense.

– Has not been denied a security clearance or had a security clearance revoked.

Appendix B.

1. **SPOC, MPASM and MPAS MP-ICAM Certification Training.** The WMD MP-ICAM SPOC and all appointed MPASMs and MPASs within the WMD upon their initial appointment must complete the required MP-ICAM certification training within 30 days. Re-certification will take place annually. The training is completed on the Joint Knowledge Online (JKO) website. Once you log into the JKO 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 JKO:

      1) DMDC-US1430-MPICAM; Mission Partner Identity, Credential and Access Management (MP-ICAM) Training Overview.

      2) DMDC-US1431-MPICAM; Privileged Users Functions

      3) DMDC, Mission Partner Identity, Credential and Access Management (MP-ICAM) Service/Agency Point of Contact (SPOC) Training.

      4) DMDC-US1378-EMMA, Enterprise Monitoring and Management of Accounts (EMMA) Overview.

      5) DMDC-US1379-EMMA, Organization Functions in EMMA

      6) DMDC-US1380-EMMA, Role and User Functions in EMMA

   (b) The **MPASM** must complete and pass the following training courseware on the DMDC Learning Site:

      1) DMDC-US1431-MPICAM; Privileged Users Functions

      2) DMDC-US1430-MPICAM; Mission Partner Identity, Credential and Access Management (MP-ICAM) Training Overview.

      3) DMDC-US1378-EMMA, Enterprise Monitoring and Management of Accounts (EMMA) Overview.

      4) DMDC-US1380-EMMA, Role and User Functions in EMMA.

      5) DMDC-US1379-EMMA, Organization Functions in EMMA

   (c) The **MPAS** must complete and pass the following training courseware on the DMDC Learning Site:

      1) DMDC-US1430-MPICAM; Mission Partner Identity, Credential and Access Management (MP-ICAM) Training Overview.

   (d) Successful completion of the training updates the SPOC, MPASM or MPASs profile in DEERS. If MPASMs and MPASs do not successfully complete the training, the MP-ICAM application does not allow them to log in. A user is given five (5) attempts to pass a MP-ICAM certification course post-test. A failed fifth attempt locks them out of the course. To resume training, the user must call the DMDC Help Desk to have his or her test reset.

2. MP-ICAM Website: When the authorized user completes their required training, the MP-ICAM website can be accessed using the URL: mpartnerspnrweb-pki.dmdc.osd.mil

Appendix C.

1. MP-ICAM Site Account Management.

(a) Site Creation. The WMD has a single MP-ICAM account. This MP-ICAM account is assigned a site ID (175173) which is used to manage all MP-ICAM users assigned to or employed by the WMD.

(b) Designating/Revoking MPASMs within MP-ICAM.

1) The WMD SPOC has two active MPASMs for the site ID to ensure management of all active MPAS accounts and associated applicant records.

2) The WMD SPOC is responsible for requesting and revoking the designation of individuals to serve as MPASMs for the WMD MP-ICAM Site ID. A SPOC can remove MPASM/MPAS accounts on the Enterprise Monitoring and Management of Accounts (EMMA) website.

3) When a new MPASM is registered in EMMA, the MPASM will receive an email notification prompting them to redeem their EMMA token. The MPASM 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 MPASM again and generate another token email. When the EMMA token is redeemed, the MPASM's MP-ICAM account is automatically activated.

4) The SPOC should immediately revoke a MPASMs application and privileges if the MPASM meets any of the following conditions:

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

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

– MPASM has left military service or civil service or has otherwise become disassociated with the WMD.

– MPASM has transferred out of the organization.

(c) **Activating/Deactivating MPASs within MP-ICAM**.

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

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

3) MPASs must notify the MPASMs prior to departure for an extended time (one month or longer) so they can determine whether any personnel assigned to the MPAS within the MP-ICAM website should be temporarily reassigned to another MPAS.

(d) **General MP-ICAM Website Account Management Procedures**.

1) CAC enabled login is the only means to access the MP-ICAM and EMMA websites by SPOCs, MPASMs and MPASs.

2) MPASMs and MPASs must ensure that they **always safeguard** the personally identifiable information (PII) of the personnel they manage within the MP-ICAM system.

WASHINGTON MILITARY DEPARTMENT

EMPLOYEE/EMPLOYER INQUIRY SHEET – CAC CARD APPLICATION – JUSTIFICATION OF NEED

EMPLOYEE APPLICATION FOR CAC CARD

EMPLOYEE NAME: Click here to enter text.

DATE REQUESTED: Click here to enter text.

POSITION NUMBER: Click here to enter text.

E-MAIL ADDRESS: Click here to enter text.

TELEPHONE NUMBER: Click here to enter text.

SUPERVISOR NAME: Click here to enter text.

INQUIRY DETAILS

SUPERVISORS: COMPLETE THIS FORM FOR YOUR EMPLOYEE AND ROUTE TO DEPARTMENT HEAD FOR SIGNATURE.

IN THE SPACE BELOW, IDENTIFY WHY YOU OR YOUR EMPLOYEE NEED TO BE AUTHORIZED TO APPLY FOR A CAC CARD AND ANSWER THE FOLLOWING QUESTIONS IN YOUR RESPONSE:

1. **DO YOU OR YOUR EMPLOYEE WORK ON A STATE COMPUTER WITH A CAC CARD READER OR WORK ON A FEDERALLY PROVIDED COMPUTER?**
   Click here to enter text.

2. **WHAT SPECIFIC JOB DUTY DO YOU OR YOUR EMPLOYEE PERFORM THAT REQUIRES THE NEED FOR A CAC CARD AND ENTRY INTO THE FEDERAL NETWORK?**
   Click here to enter text.

3. **HAVE WORKAROUNDS BEEN EXPLORED? IF SO, ARE THE WORKAROUNDS EFFICIENT?**
   Click here to enter text.

NOTE: ATTACH ALL SUPPORTING DOCUMENTATION TO INCLUDE A CURRENT COPY OF THE POSITION DESCRIPTION FORM WHICH OUTLINES YOUR DUTIES AS DESCRIBED ABOVE. PRIOR TO SUBMISSION TO HR, ALL PDFS MUST BE APPROPRIATELY UPDATED AND REVIEWED BY THE STATE HRO CLASSIFICATION AND COMPENSATION POC.

FOR DIVISION MANAGEMENT/HUMAN RESOURCE APPROVAL ONLY

DIVISION MANAGEMENT SIGNATURE: _____ **DATE:** _____

HR SIGNATURE: _____ **DATE:** _____

HUMAN RESOURCE CHECKLIST:

1. **APPROPRIATE BACKGROUND CHECK IDENTIFIED ON PDF?** ☐ **Y** ☐ **N**
2. **ARE DUTIES REQUIRING CAC NOTED ON PDF?** ☐ **Y** ☐ **N**
3. **IS IMPACT BARGAINING REQUIRED?** ☐ **Y** ☐ **N**

JAG SIGNATURE: _____ **DATE:** _____

CC: POSITION DESCRIPTION FILE – STATE HRO
SUPERVISORY FILE – STATE
TRUSTED AGENT – FEDERAL