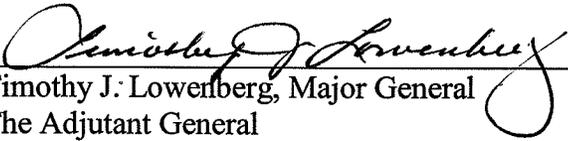




Washington State
Military
Department

Department Policy No. HR-234-10

Title:	Washington State Employee Department of Defense Automation System Requirement Policy – CAC/AKO
Authorizing Source:	Army Regulation AR 25-2 Information Assurance Air Force Instruction AFI-31-501; 5-13
References	Army Regulation AR 25-2 Information Assurance Air Force Instruction AFI-31-501; 5-1 Homeland Security Presidential Directive 12
Information Contact:	Laura Drybread, Human Resources Director Bldg # 33, 253-512-7941 Military Department, Camp Murray
Effective Date:	10/01/2010
Mandatory Review Date:	10/01/2012
Revised:	New
Approved By:	 Timothy J. Lowenberg, Major General The Adjutant General Washington Military Department Director

Purpose

To provide guidelines for issuing a Common Access Card (CAC) to Washington Military Department (WMD) state employees who require access to Department of Defense (DoD) automation systems or programs. To provide sponsorship to state employees who require an AKO/DKO (Army Knowledge Online/Defense Knowledge Online) or Air Guard Network account in order to perform significant duties and responsibilities assigned to their position.

Scope

This policy applies to all WMD state employees who require access to DoD networks or CAC enabled programs to complete some aspect of their position's normal duties in support of the WMD. It provides guidance to state employees and managers on the eligibility requirements and account access processes. Employees who do not have a State Military Department email address (predominantly AIR support employees) are advised

that any personal email sent from the AKO account address is subject to State Public Disclosure laws.

Definitions

Army Knowledge Online/Defense Knowledge Online (AKO/DKO) State Employee Account: An account established for a WMD state employee whose position requires access to a DoD CAC enabled network in order to do their job.

AKO/DKO Sponsor – A WAARNG or WA ANG federal employee the State Agency Chief Information Officer has approved to sponsor a state employee or contractor who has been authorized an AKO/DKO account.

Common Access Card (CAC): The US DoD ID Card containing an imbedded chip of an individual's credentials that is required to log on to a computer connected to a DoD CAC enabled network or program.

CAC Enabled Programs: Tracking and reporting systems operating on DoD web pages that require the CAC.

Required Access for Normal Duties: Employees having state duties as assigned in their Position Description Form (PDF) that cannot be completed without access to a program on a DoD CAC enabled network. Required access does not mean for convenience or ease and indicates that Information Technology has been contacted in regards to appropriate cost-effective, efficient workarounds.

Defense Eligibility Enrollment Reporting System (DEERS): The DoD database that issues the CAC.

Department of Defense (DoD): The federal department responsible for coordinating and supervising all agencies and functions of the government relating directly to national security and the military.

National Agency Check and Inquiries (NACI): The background investigation required in order for authorized state employees and contractors to use a DoD CAC for accessing a CAC enabled DoD computer network or program.

State Employee Database (SED): Input method for State Employees information to be uploaded into DEERS.

The Federal Office of Personnel Management (OPM): The Designated Centralized Personnel Headquarters for rules and regulations affecting Federal Technicians and those Military Department Employees who serve in a federal capacity.

The Washington Army National Guard Personnel Security Manager (WAARNG-PSM): Individual responsible for receipt, processing, and notification to the State Human Resources Office of the results of the NACI background check once completed.

The Washington Air National Guard Installation Security Program Manager (ANG-ISP): Individual responsible for fingerprinting, receipt, processing, and notification of the results to the NACI Federal Program Manager once completed.

The Washington Air National Guard Unit Security Manager (USM): Individual in the work unit responsible for initiating employees requiring a NACI, providing a blank Form 85P for employee use in gathering required information, and assisting employees with questions related to completing Form 85P prior to submission.

Policy

- A. NACI/CAC standards for issuing, maintaining and utilizing DoD networks shall ensure adherence to the network requirements associated with the Army or Air National Guard programs supported by the state civilian employees requiring CAC related network access.
- B. Division Directors shall work in coordination with the Federal Program Manager to ensure that NACI/CAC access is limited to appropriate state civilian employees.
- C. NACI/CAC cards are issued to civilian state employees for use exclusively in the performance of their assigned duties and responsibilities. Failure to maintain CAC standards or misuse of CAC cards will result in cancelation of CAC related network access.
- D. Employee probationary and/or trial service periods may be extended up to an additional six months (not to exceed twelve months total) when the NACI/CAC requests and application process can not be completed within the original six month probationary or trial service period.

NACI/CAC Request Procedures

Responsibilities

- A. WMD Division Directors
 - 1. Approve validation of requirements for CAC access to a DoD network/program by state employees in coordination with the Federal Program Manager.
 - 2. Communicate requirements to the State Human Resources Office.
- B. State Human Resources Office (HRO)
 - 1. Notifies Information Technology Representatives (State and Federal Help Desk) of approved authorization to provide instructions for the completion of the required Federal application/paperwork.
 - 2. Maintains, identifies and tracks positions required for DoD Network Program Access as identified in Position Description Forms (PDF).
 - 3. Ensures job postings reflect NACI background requirements for continued employment.
 - 4. Notifies employees who are not approved by Division Directors to have CAC access.
- C. Army Support Employees

1. WMD Supervisors

- a) Verifies operational requirements of state employee CAC access to DoD network programs by:
 - i. Identifying state employees with positions requiring DoD network/program access and providing a list of those personnel/positions to Division Directors in their respective areas. Identifies the need in order to perform job duties.
 - ii. Suggesting potential workarounds after consultation with IT Division.
 - iii. Notifying HRO of position requirements/changes to position requirements.
 - iv. Updating PDF to reflect NACI background check requirements.
- b) Secures the CAC card upon employee's separation, transfer to another state agency, retirement, or when it is determined that the CAC access is no longer needed.

2. State IT Division Help Desk

In coordination with the Washington Army National Guard – Personnel Security Manager (WAARNG-PSM)

- a) Provides WMD state employees appropriate paperwork and resources to obtain a DoD user account (AKO/DKO) and/or CAC.
- b) Processes and records the applicant's required information into the State Employee Database (SED) after required documents are submitted to and accepted by the WAARNG-PSM.
- c) Activates the account pending the results of the NACI.
- d) Cancels the DoD network account if the NACI results include derogatory information that cannot be waived.
- e) Cancels the DoD network account for employees who no longer require DOD network access.

3. Army National Guard Personnel Security Manager

- a) Receives the Request for Suitability Trustworthiness Form from State IT for any state employee who has been identified as not having a proper background investigation according to the Joint Personnel Adjudication System (JPAS).
- b) Initiates an Electronic Questionnaire for Investigations Processing (eQIP) application through JPAS for individuals requiring a NACI and emails the individual the instructions on completing the application.
- c) Reviews the application for errors, fingerprints the subject, approves the eQIP application and forwards it to OPM.
- d) Forwards OPM results of the NACI to the WMD State HRO Director.

- e) Assists the employee and State HRO Director in processing required waivers.

D. Air Support Employees

1. Federal Program Manager

- a) Verifies operational requirements of state employee CAC access to a DoD network.
- b) Coordinates any local approval that may be required with the Information System Owner (ISO).
 - i. When local authority is required for a WMD employee who has NACI results with no determination; or
 - ii. When a WMD employee is an office staff member or other staff member that requires temporary computer access through a user name and password setup to perform the essential functions of their duties.

Note: Dependent upon which military branch the state employee supports and works will determine their technology system and the process by which they obtain authorization and approval for a CAC and/or AKO Account.

2. Air IT Division Help Desk

- a) The Unit Security Manager (USM) provides the WMD employee with a Standard Form (SF) 85 for data collection and any other paperwork or resources necessary to complete the NAC.
- b) The WMD employee completes the SF85 and is encouraged to keep a file copy and any other documents used to gather necessary information secure.
- c) Upon completion and verification of the SF85, the USM completes the Office of Personnel Management (OPM) cover sheet and attaches it to the SF85.
- d) Using FD 258, the ISPM fingerprints the employee and forwards the fingerprint card with copies of the signed SF85 to OPM. Upon completion of OPM review, investigation and adjudicating authority, investigation results will appear in the JPAS personal summary and are forwarded to the ISPM.
 - i. If the results are favorable, the SED may be initiated in issuing the CAC.
 - ii. If the results are no determination, ISPM gives the packet to the State HRO Director who will confer with the Employee's Manager and Federal Program Manager to determine if local authority permission should be requested.

3. Air National Guard Installation Security Program Manager (ISPM)

When favorable or local authority approval is received:

- a) The ISPM forwards a copy of the local authority approval memorandum as written confirmation to 194 MSG/CF (Air West), or 141MSG/CF (Air East), to enable set up of an ANG network account and to State HRO for their records.

- b) 194 MSG/CF (Air West) or 141 MSG/CF (Air East) provides the WMD employee with temporary network access to complete required SED request information under the supervision of Communication staff located in Bldg 113 (Air West), or Communication staff located in Bldg in 2285 (Air East).
- c) Completed SED WMD employee information is forwarded to the State IT Technician at MILDLCAC@Mil.wa.gov.
- d) Upon receipt of confirmation from the State IT Technician that SED input has been completed, the WMD employee will schedule an appointment with one of the following: 194 Force Support Flight (194 FSF) at (253) 512-3331 in building 107 (Air West), or 141 FSF (Air East) at (509) 247-7310, to obtain CAC. It may take up to 10 working days before the WMD employee's information is uploaded into DEERS from the SED.
- e) The employee will provide two forms of government issued identification (one must be photo identification) and their social security number at their scheduled appointment.
- f) The employee shall provide a confidential six to eight digit numeric PIN each time the employee gains access to a computer using the CAC.

Network Access

- A. Authorized employees granted network access to DoD automation systems or programs include:
 1. WMD employees who must use DoD programs or reports as part of their normal duties in support of the WNG. This does not include access strictly for convenience; only those duties for which there are no reasonable workarounds.
 2. WMD employees who work in remote WNG Armories or facilities where the DoD network is the only available internet connection and must gain access to WMD Email or other programs.
 3. State Contract employees such as the Family Support Group, who work in direct support of the WNG.
 4. A signed computer user agreement:
 - a) Acceptable Use Policy (AUP) (Army)
 - b) Form AF-4394 (Air)
 5. Complete initial DoD Information Assurance Awareness computer based training (CBT):
 - a) DoD Information Assurance Awareness through website <https://ia.signal.army.mil> (Army)
 - b) Advanced Distributed Learning Service (ADLS) through website https://golearn.csd.disa.mil/kc/login/asp?kc_ident=kc0001 (Air)

6. Annual completion of DoD Information Assurance Awareness CBT (Army and Air)

Eligibility and Processing

- A. WMD employees identified by supervisors and documented by HRO as requiring DoD network access must follow the steps outlined in the NACI/CAC Application Procedures section of this policy. To be allowed access to a DoD network, a WMD employee must complete a similar process as a DoD employee. The process may include the application for a DoD user account, completion of initial Annual Computer User Training and test and/or other user requirements, acknowledgement of the DoD Acceptable Use of the DoD automation system, and the initiation of the NACI, federal background investigation.
- B. The background investigation documentation is considered confidential and is treated as such by all involved in processing. Personal information contained on forms will not be shared with anyone other than the employee and the WAARNG-PSM/ WANG ISPM processing the packet. Completed documents **will not** be provided to the employee's supervisor(s).
- C. If a background investigation uncovers unfavorable or derogatory information, the WMD State HRO Director will work with the employee and the Military Personnel Security Manager to process any required waivers.
 1. If an employee cannot be issued a CAC because of personal history that cannot be waived, the appropriate IT Division Representative will cancel the employee's DoD network account.
 2. The State HRO Director and Supervisor of the employee will work to establish an alternative work process not requiring DoD network/program access if available.
 3. If an alternate workaround is not available, and the essential functions of the job are affected, employees hired on or after September 30, 2010 who have been given conditional job offers based on the successful outcome of a screening will be terminated. Employees hired prior to September 30, 2010, will work with their supervisor and State HRO Director to determine alternative work assignments.
- D. Once an employee no longer needs to connect to a DoD network/program, the CAC must be turned in immediately and the network access account revoked.
 - a) If the employee with DoD access is terminated for any reason, the CAC is collected during the out processing with the State Supervisor.
 - b) If the employee no longer requires access to a DoD network, and remains employed by the WMD, the supervisor will collect the CAC and deliver the unaltered CAC to WMD State HRO. The unaltered CAC will be returned to the point of issuance or closest issuing source.

- c) The WMD State HRO will inform the appropriate WMD IT Division who will inform the DoD network manager and the network privileges will be revoked.

NACI/CAC Application Procedures

Upon determination that an employee requires access to the DoD network/program, a NACI is required as part of the process to issue a CAC. The following items need to be completed as soon as possible but take no longer than 14 days to facilitate the NACI/CAC application. Employees who have had a NACI investigation in the past should notify WMD State HRO Director. If the previous background check can be verified, the employee may not have to complete the NACI portion of the CAC process.

A. Army Support Employees

1. Create an Army Knowledge Online (AKO) User Account
 - a) Go to <https://www.us.army.mil> and select "Register for AKO".
 - b) Select "Create a Sponsored Account". A non federal employee must be sponsored by a DoD member. The State Human Resources representative will identify a federal sponsor point of contact for the employee applicant.
 - c) Select "Federal Civilian Agencies" as the Account Type. The AKO username of the sponsor account will be entered in the Sponsor field. After the employee is issued a CAC, AKO email should be forwarded to their WMD email account. Users can register their CAC to simplify logging on to AKO.
2. Complete the CAC Spreadsheet which will be provided by the IT Division and return to them at the designated place within a designated time frame.
3. Complete the following forms in order to have your eQIP application initiated online:
 - a) Suitability Trustworthiness Form
 - b) Optional Form 612 – Application for Federal Employment or a completed resume.

The OF612 may be obtained at the below website to be completed and printed out for signing. The Suitability Trustworthiness Form can be obtained from the State IT. Save a copy for your records. Notify the Human Resources Director that you have completed the process.

<http://www.opm.gov/forms/html/sf.asp>

Applications must be completed on-line and submitted in a typed format.

Hand written documents will not be accepted.

- c) eQIP application – Once the Suitability Trustworthiness Form is received by WAARNG-PSM from State IT, an email with instructions and a weblink to the application will be provided to the employee. The application has a timeline of

30 days to initially login and 60 days to be completed. Once the employee completes the application, three signature pages are printed out and the employee clicks on the Release/Transmit to Agency button at the bottom of the application to complete the process. Once the release/transmit button is clicked, the employee can no longer go in and make any changes until the WAARNG-PSM unlocks their eQIP. The three signature forms need to be signed, dated and either scanned or emailed to the WAARNG-PSM or hand delivered. **Faxed copies are not accepted.** The WAARNG-PSM will review the application once it shows in JPAS as Ready for Review. The WAARNG-PSM will review the application and send back any necessary corrections to the employee. The employee will make corrections and print three new signature pages and release/transmit the application to the agency again. The new signature pages will be given to the WAARNG-PSM. The eQIP application will be reviewed again, and if there are no corrections to be made, the WAARNG-PSM will approve the application through JPAS.

- d) FD 258 - Fingerprint Card – Employees processing the NACI documentation should contact the WAARNG- PSM located in Bldg 18, Camp Murray by calling (253)512-8135 to schedule a fingerprinting appointment. State employees should bring their printed and signed signature pages from their eQIP application and their OF 612 or resume to this appointment to get the initial review by the WAARNG-PSM.

4. Employees who require DoD network access must establish a DoD account:

- a) Using the newly acquired AKO user logon, employees who logon to a DoD computer/network must register and complete the DoD Annual Information Assurance course and test at: <https://ia.gordon.army.mil/login.asp>. Send test results to MILDLCAC@mil.wa.gov.
- b) Complete MIL FORM 603 and send to MILDLCAC@mil.wa.gov. (AKO address from step 1 is needed for MF 603).
- c) Complete the Acceptable Use Policy (AUP) (4 pages), scan and send all 4 pages as one document to MILDLCAC@mil.wa.gov. Provisional "CAC Exempt" network access may be granted by the DoD network managers once steps 1-4 are complete and while the outcome of the NACI is being processed.
- d) When the NACI investigation is complete the Personnel Security Manager reports the results in writing to the WMD State HRO Director. This process can take as long as six months.
- e) The WMD State HRO Director will inform the appropriate IT staff as to the date of the successful NACI.

B. Air Support Employees

1. Contact the 194 MSG/CF and request a temporary access account. Once this account is created the employee will be supervised by the Unit Computer System Technician (CST) while on the network.
2. Complete the following form and have your fingerprints taken. Web access links will be provided to applicants and must be completed on line.
 - a) Standard Form 85 – Questionnaire for Non Sensitive Positions
This form, SF 85, may be obtained at the below website and completed electronically. Completing the form on line prompts you when required information is missing and streamlines the final processing of your CAC Application packet. Print each form out as you complete it. Save it for your records. Notify the State HRO Director that you have completed the process.
<http://www.opm.gov/forms/html/sf.asp>
Applications must be completed on-line and submitted in a typed format.
Hand written documents will not be accepted.
 - b) FD 258 - Fingerprint Card – Employees processing the NAC documentation should contact the Installation Security Program Manager (ISPM) located in Bldg 114, Camp Murray by calling (253)512-3491 to schedule a fingerprinting appointment. State employees should bring their printed NAC packet to this appointment to get the initial review by the ISPM.
3. Employees who require DoD network access must establish a DoD account:
 - a) Using the temporary access account, employees who logon to a DoD network computer/network must complete the DoD Information Assurance Awareness CBT course and test at: https://golearn.csd.disa.mil/kc/main/kc_frame.asp. Send results to 194RSW.Comm@ang.af.mil, 194 MSG/CF for (Air West)
 - b) Complete AF Form 4394 Air Force user agreement statement and send to 194RSW.Comm@ang.af.mil, 194 MSG/CF (Air West)
 - c) When the NAC investigation is complete the Personnel Security Manager reports the results in writing to the WMD State HRO Director. This process can take as long as six months.
 - d) The WMD State HRO Director will inform the appropriate IT staff as to the date of the successful NAC.