DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, US ARMY GARRISON COMMAND, FORT KNOX
111 E CHAFFEE AVE
FORT KNOX, KENTUCKY 40121-5719

IMKN-HR

JUL 26 2019

MEMORANDUM FOR

Commanders, All Units Reporting Directly to this Headquarters
Commanders, Fort Knox Partners in Excellence
Directors and Chiefs, Staff Offices, Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo 11 - Common Access Card (CAC) Credentialing for Eligible Department of Defense (DoD) Contractors and Other Population Categories

1. References.

a. DoD Instruction 5200.46, DoD Investigation and Adjudication Guidance for Issuing the Common Access Card (CAC), 9 September 2014.

b. DoD Manual 1000.13, Volume 1, (DoD Identification (ID) Cards: ID Card Life Cycle), 23 January 2014.

c. Army Directive 2011-08, Army Implementation of Homeland Security Presidential Directive (HSPD)-12, 26 May 2011.

d. Army Directive 2014-05, Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors, 7 March 2014.

e. Defense Manpower Data Center (DMDC) Trusted Associate Sponsorship System Overview Guide, June 2014.

f. Defense Manpower Data Center (DMDC) Trusted Associate Sponsorship System (TASS) Trusted Agent (TA)/Trusted Agent Security Manager (TASM) User Guide, October 2012.

2. Purpose. To establish Fort Knox policy and responsibilities concerning the CAC Credentialing Program for eligible DoD contractors and other specific population categories.

3. Sponsorship and Eligibility. Specific population categories listed in enclosure 1, Trusted Associate Sponsorship System (TASS) Category Descriptions, require a government sponsor. The sponsor is the person affiliated with the DoD or other population category who takes responsibility for verifying and authorizing the applicant's

requirement for a government issued ID card. Applicants for a CAC shall be sponsored by a DoD government official or employee.

a. Sponsoring organizations shall establish procedures to ensure that the issuance and retrieval of CACs are part of the normal personnel in- and out-processing requirements within the organization, and that internal controls are in place to monitor the application and re-verification process. The government employees with primary responsibility to ensure eligibility, completion of the application, and CAC turn-in are the applicant's Contracting Officer's Representative (COR) and TA. The COR and TA may be the same individual.

b. A CAC-eligible applicant is defined as any U.S. or Foreign National person who is authorized and requires access to multiple (two or more) DoD-controlled installations or facilities on behalf of the Department of the Army (DA) on a recurring basis for a period of six (6) months or more; or requiring both access to a DoD controlled installation or facility and onsite or remote access to DoD or DA controlled information networks. The practical application of the term "facility", with respect to HSPD-12 CAC-eligible determination is as follows:

(1) Separate buildings located on Fort Knox that do not employ special security measures are not considered facilities separate from the installation.

(2) Buildings or activities where special security measures are employed may be considered a separate "facility" from Fort Knox, in accordance with the determination of the command leadership of the particular building activity.

(3) Buildings or offices not located on Fort Knox are considered separate facilities. Depending on their level of security measures, an individual may require a CAC in order to access even one facility of this category.

c. The CAC Credentialing Wiring Diagram (enclosure 2) provides an overview of the CAC Credentialing Program beginning with the initial determination of eligibility and ending with the final revocation of the CAC.

4. Responsibilities.

a. Commander/director will:

(1) Establish the Industrial Security Program for contractors in their command, activities, and areas of responsibilities.

(2) Ensure Supporting Security Managers (SSMs), TASMs, TAs, and CORs abide by this policy and meet training requirements.

(3) Ensure prompt reporting of credible derogatory information on all personnel, to include embedded/integrated contractors and other personnel category individuals.

(4) Ensure in- and out-processing procedures support the guidance in this policy.

b. Supporting Security Manager will:

(1) Be a Federal employee with a minimum eligibility of a Secret clearance and active CAC working in the Garrison or other Command Security Division/Section.

(2) Review Joint Personnel Adjudication System (JPAS) records for all contractors and other personnel category personnel receiving CACs.

(3) Provide written documentation to the TA whether contractors and other personnel category individuals have an interim or final credential and can receive a CAC.

(4) Complete and validate DD Form 2875, System Authorization Access Request (SAAR), Part III, for Fort Knox Nonsecure Internet Protocol Router Network (NIPRNet) requests for contractors and other personnel category requests.

(5) Provide in- and out-processing in the appropriate category in JPAS for contractors and other personnel category individuals.

(6) Initiate National Agency Check with Inquires (NACI) when no other favorable adjudicated personnel security investigation is annotated in JPAS for contractor, other personnel category individuals, and affiliated volunteers.

(7) Provide Federal Bureau of Investigations (FBI) fingerprint processing for the Special Agreement Check (SAC) for contractors and other personnel category individuals.

(8) Receive and process CAC Credentialing Letters of Denial or Revocations.

c. Trusted Associate Security Manager (TASM) will:

(1) Be a Federal employee and have a minimum of a favorable NACI and a current CAC.

(2) Grant access to new TAs and provide training and materials.

(3) Ensure TAs meet certification requirements.

(4) Conduct monthly audits on TAs to ensure compliance with this policy.

(5) Perform duties as TA if required.

d. Trusted Agent (TA) will:

(1) Be a Federal employee with a minimum of a favorable NACI and a current CAC.

(2) Determine CAC eligibility in conjunction with the sponsoring agency initially and every 180 days to ensure only authorized individuals are issued CACs

(3) Ensure the applicant is vetted through the SSM with a favorable FBI fingerprint SAC and NACI on file. This verification will be provided to the TA from the SSM in writing.

(4) Process and approve applications for CACs following procedures IAW the most current Trusted Associate Sponsorship System (TASS) Trusted Agent (TA)/Trusted Agent Security Manager (TASM) User Guide.

(5) Take immediate action to revoke the CAC, if eligibility no longer exists.

(6) Return expired and turned in CACs to the installation ID Card Facility.

(7) Maintain less than 100 active CACs.

(8) Report an adverse information, suspicious contacts, or other reportable incidents by submitting information and any documents in writing to the COR and the SSM.

(9) Follow up on interim credentialing decisions every 30 days.

(10) Brief CAC applicants on the following:

(a) The CAC applicant is responsible to account for and protect the CAC.

(b) The CAC shall be returned to the sponsoring organization upon expiration of the CAC, contract expiration, termination of employment, or when no longer needed for DoD network access or access to a DoD facility.

(c) The CAC applicant is only authorized to use a CAC for the specific contract or described employment unless written authorization is received from the COR or sponsoring agency. For instance, the contractor cannot use the CAC to visit another military installation unless authorized in writing by the COR.

e. Contracting Officer Representative (COR) will:

(1) Be a Federal employee and have a minimum of a favorable NACI for unclassified contractors and/or final eligibility and access at the highest level stated in the classified contract.

(2) Notify the TA within the organization of the new contractor needing a CAC and assist with providing necessary documentation for security verification.

(3) Retrieve the CAC from the contractor upon termination of contract or termination of employment of individual.

(4) Work with supporting contracting commands to ensure CAC security clauses and retrieval responsibilities are incorporated in the contract performance work statement.

5. CAC Credentialing.

a. Interim credentialing is authorized when a favorable FBI fingerprint SAC has been received by the SSM, a NACI or greater investigation has been scheduled by the

Office of Personnel Management (OPM), and SAC results, security questionnaire, and OF-306, Declaration of Federal Employment have been reviewed locally by the SSM IAW HSPD-12 adjudicative guidelines with no disqualifying issues. The JPAS record will show a completed (open and close date) for a SAC and a current date in the "PSQ Sent Date".

b. Final credentialing is authorized when JPAS records clearly show a NACI has been completed by OPM and adjudicated favorably by the DOD Central Adjudication Facility (DoDCAF) or other authorized official.

c. OPM and DA support reciprocity on previously conducted investigations. Provided investigation results are available, individuals who have a completed favorable adjudicated NACI or higher investigation without a twenty-four (24) month break in service will not require reinvestigation upon employment. Contractors that require a security clearance must have a National Agency Check with Law and Credit (NACLC) or higher investigation.

d. As the expiration date for a CAC approaches, the applicant must contact the TA if a continued card requirement exists, and apply for a new card. The TA must verify the applicant's valid requirement for a new card according to known policies and procedures, and the applicant's continued employment.

e. When a determination is made to deny or revoke a CAC, the individual will be afforded due process in accordance with procedures outlined in Army Directive 2014-05 referenced above.

6. CAC Retrieval.

a. Sponsors will retrieve CACs issued to contractors and other population categories upon completion of the contract duration, termination of employment by that individual, denial or revocation of final credentialing, or when personnel no longer meet the eligibility requirements outlined in paragraph 3b above.

b. Sponsors will give CACs to the TASM or TA, who will return cards to the Installation ID Card Facility using a DA Form 200, Transmittal Record. TAs may identify themselves as performing this mission in order to have front of the line privileges.

c. If the CAC cannot be retrieved, the sponsor or contractor project manager, or equivalent, will immediately provide a memorandum to the installation ID Card Facility

and to the TA explaining why the CAC could not be retrieved. Upon receipt of this memorandum, the TA will immediately revoke the CAC in TASS and send the memorandum to the Directorate of Emergency Services Military Police (MP) Station. The MP Station will enter this information into their database.

7. If the CAC is lost, stolen, or destroyed, personnel will follow the guidance in Fort Knox Policy Memorandum 10, Replacement of Lost or Stolen Government Issued Identification (ID) Card/Common Access Card (CAC). The TA will re-verify vetting with the SSM and process a new CAC application in TASS once documentation is received.

8. This Command Policy Memorandum will remain in effect until superseded or rescinded.

9. The proponent for this policy is the Director, Human Resources, ATTN: IMKN-HR at (502) 624-4162.

2 Encls
as

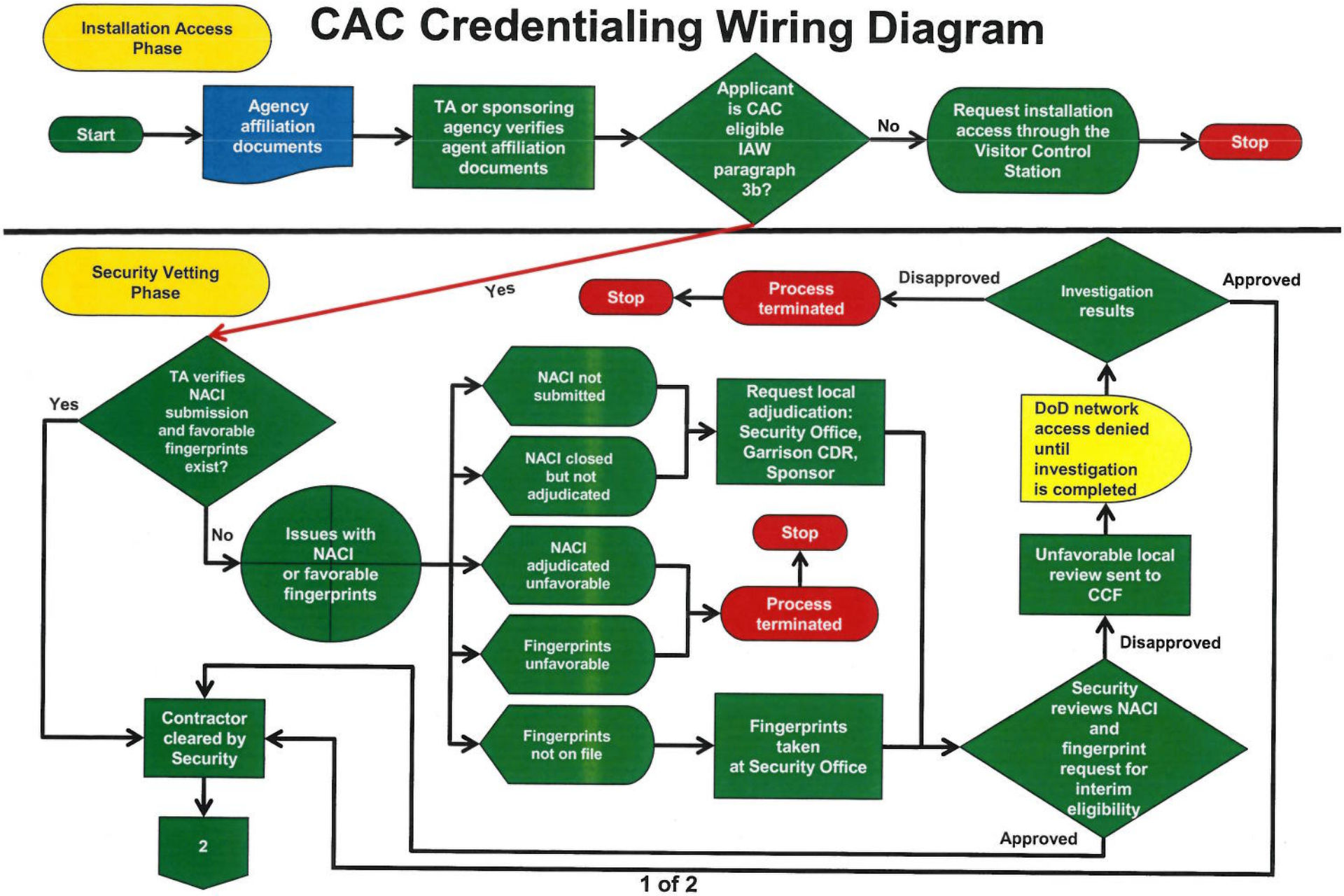
CJ KING
COL, LG
Commanding

Enclosure 1 (Trusted Associate Sponsorship System (TASS) Personnel Category Descriptions) to Fort Knox Policy Memo 11 - Common Access Card (CAC) Credentialing for Eligible Department of Defense (DoD) Contractors and Other Population Categories

Personnel Category	Description
Affiliated Volunteers	Affiliated Volunteer who need access to DoD networks.
DoD and Uniformed Service Contractor	Employees of a firm, or individual under contract or subcontract to the DoD, providing services or support to the Department. This category includes NOAA, Public Health Service Contractors, and Federally Funded Research and Development employees.
Foreign Affiliate	Non-U.S. citizen (military, civilian or contractor) sponsored by their government as part of an official visit or assignment to work with the DoD, in a DoD facility or requiring network access.
Non-DoD Civil Service Employee	Civil Service employee of a Federal Agency other than DoD or Uniformed Service.
Non-DoD Presidential Appointee	The DHRA is the only sponsoring organization option available for this category.
Non-Federal Agency Civilian Associate	This category allows the tracking of certain affiliated agencies that directly support the Uniformed Services, as well as other categories of personnel who have a direct affiliation with the Uniformed Services, but are not otherwise identified in the other Personnel Categories.
Non-US Non-Appropriated Fund (NAF) Employee	Non-US citizens using either a Foreign Identification Number or an Individual Taxpayer ID Number (ITIN) as the Person Identifiers.
OCONUS Hire	Non-US citizens hired under an agreement with the host nation and paid directly by the US forces (direct hire) or paid by an entity other than the U.S. forces for the benefits of the US forces (indirect hire).
Other Federal Agency Contractor	Supports the Department of State (DoS) waiver authorizing CAC issuance to Federal Government personnel and their prime contractors deploying to or working in the CENTCOM AOR under the authority of the Chief of Mission.

Enclosure 2 (CAC Credentialing Wiring Diagram) to Fort Knox Policy Memo 11 - Common Access Card (CAC) Credentialing for Eligible Department of Defense (DoD) Contractors and Other Population Categories

CAC Credentialing Wiring Diagram



Enclosure 2 (CAC Credentialing Wiring Diagram) to Fort Knox Policy Memo 11 - Common Access Card (CAC) Credentialing for Eligible Department of Defense (DoD) Contractors and Other Population Categories