DEPARTMENT OF DEFENSE
GUIDEBOOK FOR CAC-ELIGIBLE CONTRACTORS FOR UNCLASSIFIED NETWORK ACCESS

21 NOVEMBER 2014

Contents

Scope

The scope of this guidebook is to provide a step-by-step guide in a “how-to” format for Common Access Card (CAC)-Eligible Contractors who require Network Access in support of a Department of Defense (DoD) contract. While this guidebook only addresses the CAC processes for CAC-Eligible Contractors who require Network Access; Logical and Physical Access may be addressed in future versions.

“CAC-Eligible Contractor” is defined as a contractor employee performing under a current contract with a DoD Service/Component/Agency AND sponsored by a DoD Service/Component/Agency.

“Network Access” is defined as all DoD unclassified and classified information systems including networks (e.g., non-classified Internet Protocol Router Network, Secret Internet Protocol Router Network (SIPRNET)), Defense Research and Engineering Network, Secret Defense Research and Engineering Network web servers, and e-mail systems.

“Logical Access” is defined as electronic access controls authenticated through outside certificates accepted by the DoD to limit access to data files and systems only by vetted individuals.

“Physical Access” is defined as all DoD and non-DoD personnel entering or exiting DoD facilities or installations that authenticated a physical access control system (PACS).

This guidebook is based on current policy and regulations and will be updated accordingly. The procedures herein apply to services performed anywhere in the world by persons and/or entities under contract with the DoD. If there is a conflict between the guidelines herein and Department of Defense Instruction (DoDI) 8520.03, “Identity Authentication for Information Systems”, DoDI 1000.13, “Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals.” or Department of Defense Manual (DoDM) 1000.13 Volume 1, “DoD Identification (ID) Cards: ID Card Life-Cycle,” the provisions in the DoDI and DoDM shall take precedence.

Chapter 1: Introduction

1.1 Purpose and Background

The purpose of this guidebook is to outline the process of obtaining Network Access to DoD Information Technology (IT) systems for DoD CAC-Eligible Contractors. It is also designed to assist Contracting Officer Representatives (CORs) in the internal process of verifying and sponsoring CAC-Eligible Contractor CACs.

The DoD issues identification cards known as CACs to CAC-Eligible Contractors as well as to active-duty uniformed service personnel, certain reserve personnel, civilian employees, and other eligible populations in accordance with DoDI 1000.13. DoD CAC-Eligible Contractors use CACs to gain Logical or Network Access to DoD IT systems and to digitally sign and encrypt e-mails to facilitate daily business activity on behalf of the DoD.

1.2 Policy and Regulations

Several DoD and government-wide policies have been implemented that govern CAC-Eligible Contractor access and CAC issuance.

The following policies govern Network Access throughout the DoD.

Policy Name	Summary	Date	FAR/DFARS
FIPS 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors"	Specifies the architecture and technical requirements for a common identification standard for federal employees and CAC-Eligible Contractors	March 2006	FAR 52.204-9 (a)-(d)
HSPD-12, "Homeland Security Presidential Directive 2012"	Establishes mandatory, government-wide standards for secure and reliable forms of identification used for logical access to federal facilities	August 27, 2004	FAR 52.204-9 (a)
DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program"	Establishes policy and assigns responsibility under the DoD PIP Program	July 19, 2004	Not in FAR/DFARS
DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals"	Implements DoD policy, responsibilities, and procedures for the issuance of ID cards to members of the Uniformed Services of the United States; and prescribes ID and privilege cards for issuance to their dependents and other eligible Individuals.	January 24, 2014	Not in FAR/DFARS

DoD Manual 1000.13, Volume 1, "DoD Identification (ID) Cards: ID Card Life-Cycle"	Establishes responsibilities and procedures during DoD ID life-cycle.	January 24, 2014	Not in FAR/DFARS
DoD 5220.22-M "National Industry Security Program Operating Manual"	Establishes the standard procedures and requirements for all government CAC-Eligible Contractors, with regards to classified information.	February 28, 2006	DFARS 204.7302 (c)
DoD 8570.01-M "Information Assurance Workforce Improvement Program"	Provides guidance and procedures for the training, certification, and management of the DoD workforce (including CAC-Eligible Contractors) conducting Information Assurance (IA) functions in assigned duty positions.	December 19, 2005	DFARS 239.7102-1
DoD Instruction 8520.03 "Identity Authentication for Information Systems"	Establishes policy on how to implement identity authentication and how to use the CAC.	May 13, 2011	Not in FAR/DFARS

Chapter 2: Getting Started: Network Access

2.1 Common Access Card (CAC)

A CAC is the standard identification smart card containing several different identity and credentialing technologies. The photograph shows an example of a Contractor CAC. The CAC expiration is listed both in the top right corner (month and the year) and above the green stripe highlighting the Contractor's name (year, month, and day). The CAC will list the card holder's affiliation to the Government as Contractor and the card holder's Agency/Department (DoD). In the middle of the CAC in the green stripe, the card holder's first and last name, as recorded in the Defense Enrollment Eligibility Reporting System (DEERS), is displayed. A barcode is located in the bottom left corner next to the Integrated Circuit Chip (ICC) which is placed near the bottom-middle of the card. The back of the card has a ghost image of the CAC holder and the CAC holder's DoD identification (ID) number. Every individual entered into DEERS has one record with one DoD ID number. The 9-digit number below the bar code and following the letters "DODCAC" identifies the Real-Time Automated Personnel Identification System (RAPIDS) Site which issued the CAC.

2.2 How does a CAC-Eligible Contractor get a CAC?

Step 1: Determine Eligibility

CAC-Eligible Contractor Eligibility Requirements (Prime and Subcontractors)

To determine if the Contractor is eligible for a CAC, the Contractor must meet all of the following items in the checklist below:

CAC-Eligible Requirements under DoDM 1000.13 Volume 1	
1.	Is the Contractor performing under a current contract with a DoD Service/Component/Agency?
2.	Is the Contractor sponsored by a DoD Service/Component/Agency?
	If YES to 1 and 2, the Contractor is CAC-Eligible.

If the Contractor is deemed "CAC-Eligible", the following must occur for the CAC-Eligible Contractor to receive his/her CAC:

1. Completion of Background Vetting (includes completion of one of the forms listed under the "Forms" section under Step 2 (SF-85, SF-85P, or SF-86);

2. Submission of CAC-Eligible Contractor information into TASS and DEERS; and

3. Visit a RAPIDS Location.

Step 2: Complete Background Vetting

Background Vetting

Background vetting is required for all CAC applicants. A CAC-Eligible applicant shall not be issued a CAC without first satisfying the background vetting requirements, per DoDI 1000.13, Volume 1. Applicants who have been denied a CAC or have had a CAC terminated based on an unfavorable adjudication of a background investigation may submit an appeal. After completion of the application by the CAC-Eligible Contractor, the supporting security office submits the appropriate form to initiate a NACI, NACLC, or equivalent investigation[1], and an FBI fingerprint check for potential card holders. Investigations on CAC-Eligible Contractor personnel requested on the SF-85 and SF-85P forms require the CAC-Eligible Contractor to answer specific questions found on

[1] For a list of equivalent investigations, please see Enclosure 3, Page 11 of the DoDI 5200.46 "DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card" located here: http://www.dtic.mil/whs/directives/corres/pdf/520046p.pdf

the OF306: 1, 8, 9, 10, 11, 12, 13, 16, and 17a. The OF306 form may be used, or the specific questions and answers may be provided on an attachment to the SF-85 or SF-85P. OF306 is Declaration for Federal Employment. SF85, SF85P and OF306 are available at the Office of Personnel Management (OPM) (OPM.gov/forms).

Upon employment, CAC-Eligible Contractor personnel are encouraged to complete the relevant OPM forms to expedite the form review and background investigation process. CAC-Eligible Contractors should contact the designated employee at the CAC-Eligible Contractor's employer who handles the background investigations (i.e., security manager, facility security officer) for information about completing SF-85/SF-85P/SF-86 forms. Such person may have access to the Electronic Questionnaires for Investigations Processing (e-QIP) system and can request background investigations to be initiated for their CAC-Eligible Contractor personnel.

NOTE: Contact the CAC-Eligible Contractor's Trusted Associate Sponsorship System (TASS) Trusted Agent (TA) to determine if the Sponsoring Agency allows CAC-Eligible Contractor security managers to access e-QIP on behalf of the individual CAC-Eligible Contractor. If not, the CAC-Eligible Contractor can access e-QIP to complete the OPM forms.

NOTE: Since the background vetting process can take up to 18 months, a CAC-Eligible Contractor may be issued a CAC after an FBI fingerprint check returns favorable results provided that the NACI, NACLC or equivalent investigation has been initiated. If the NACI, NACLC or equivalent investigation process is completed and is not favorably adjudicated, the CAC will be revoked.

Cleared CAC-Eligible Contractors

CAC-Eligible Contractors who have already satisfied the background vetting requirements with a NACI, NACLC, or equivalent investigation, should inform their Facility Security Officer (FSO). The FSO will notify the TA that the CAC-Eligible Contractor's completed investigation has been confirmed in the Joint Personnel Adjudication System (JPAS) without further action required by the CAC-Eligible Contractor.

Non-Cleared CAC-Eligible Contractors

For CAC-Eligible Contractors who need to initiate the security clearance process before obtaining a CAC, the Contractor must complete and submit **one** of the following forms for CAC issuance through e-QIP. Forms required for initiating the Security Clearance process can be found here:

Forms

Form	Position	Investigation	Criteria
Questionnaire for Non-Sensitive Positions (SF-85)	Low-risk, applies to most CAC-Eligible Contractors	NACI[2] (Past 5 years)	Position is Low Risk, Non-sensitive
Questionnaire for Public Trust Positions (SF-85P)	Required for Public Trust positions	NACI/NACLC[3] (Past 7 years)	Full Time – Greater than six (6) months or longer and/or routine access Temporary – six (6) months or less and/or routine access – NACI suitability determination.
Questionnaire for National Security Positions (SF-86)	Low Risk Non-critical sensitive, including Confidential, Secret, & L access eligibility for CAC-Eligible Contractors	NACLC	For government CAC-Eligible Contractors to apply for a Security Clearance (CONFIDENTIAL, SECRET, TOP SECRET)

NOTE: The SF-85 & SF-85P are forms used to initiate the CAC issuance process while the SF-86 is used to initiate the security clearance process and investigation.

Classified Forms

If CAC-Eligible Contractors require access to classified information (CONFIDENTIAL, SECRET, TOP SECRET) during the performance of services, CAC-Eligible Contractors shall complete the Questionnaire for National Security Positions (SF-86). In addition to SF-86, CAC-Eligible Contractors will be required to satisfy the NACLC requirements.

Step 3: Create a TASS Application/DEERS

Trusted Associate Sponsorship System (TASS)

Once favorable background and vetting results are provided, the CAC-Eligible Contractor applicant must provide the following information to the TA for entry into TASS:

[2] NACI: This investigation is composed of a NAC plus written inquiries to current and past employers, schools, references, and local law enforcement agencies covering the past five years and, if applicable, to appropriate agencies for any identified arrests. All DoD NACIs include a credit search.

[3] Completion of the SF-85P and SF-86 forms initiates a NACLC (some SF-85P forms may only initiate a NACI). A NACLC is performed for CAC-Eligible Contractors who require security clearance at the confidential, secret, and L access levels. The investigation performs the following: (1) basic national agency checks which includes a security/suitability investigations index, a Defense Clearance and Investigations Index, a fingerprint classification, and a search of the FBI's investigative index) and a credit search covering all residence, employment, and education locations during the last 7 years.

- Full name (last, first, middle);
- Date of Birth;
- Person Identifier (i.e., Social Security Number or SSN);
- Primary Email;
- Contract Number; and
- Contract End Date.

The TA will create an application and provide the CAC-Eligible Contractor with login instructions to complete the TASS application. The CAC-Eligible Contractor applicant must log into TASS within 7 days of the application's creation to initialize it or it will be disabled and the TA will have to start the workflow over. Within 30 days of the CAC-Eligible Contractor's initial login, the CAC-Eligible Contractor must complete and submit the application for a CAC or the application will be disabled. Once the application is submitted, the TA will either approve the application, disable it or return it for rework. DoD and uniformed service CAC-Eligible Contractors who are non-U.S. persons (i.e. foreign nationals) will be entered into TASS the same as U.S. persons[4].

Defense Enrollment Eligibility Reporting System (**DEERS**)
Approval of a TASS application automatically submits the CAC-Eligible Contractor identity and eligibility information to DEERS. DEERS maintains the identity and eligibility information for all DoD CAC-Eligible Contractors requiring network access and assigns the CAC-Eligible Contractor a DoD ID number.

NOTE: A person with more than one personnel category may be issued a CAC for each CAC eligible personnel category, but the DoD ID number remains the same for all CACs issued to that individual. For example, an individual who is both a CAC-Eligible Contractor and a member of the Selected Reserve has two CAC-eligible personnel categories (and may be issued two CACs) but only one DoD ID number.

Identity and eligibility information about DoD and uniformed service CAC-Eligible Contractors who are non-U.S. persons (i.e. foreign nationals) are entered in to DEERS from TASS the same way as U.S. persons.

Step 4: Find a RAPIDS location

RAPIDS (Real-Time Automated Personnel Identification System)

Once the TASS application has been approved, the CAC-Eligible Contractor will be directed to visit a RAPIDS Site for identity verification and CAC issuance. Please use the RAPIDS Site Locator to find the closest RAPIDS Site. RAPIDS authenticates individuals to ensure that ID cards are provided only to those sponsored and with a current affiliation with the DoD. RAPIDS also captures uniquely identifying characteristics that bind an individual to the information maintained on that individual in DEERS and to the ID card issued by RAPIDS. These characteristics may include, but

[4] Any United States citizen or alien admitted for permanent residence in the United States.

are not limited to, digital photographs and fingerprints. A RAPIDS Verifying Official (VO) will review the CAC-Eligible Contractor's DEERS record and verify the CAC-Eligible Contractor's identity documents.

What should a CAC-Eligible Contractor bring to the RAPIDS location?

- **Two forms of ID in original form.** Both IDs must be among those listed on the I-9 Form, Lists of Acceptable Documents (page 9 of the form). One of the IDs must bear a photograph (for example, a passport or a driver's license).

- **A six (6) to eight (8) digit number to use as a PIN.** The PIN should NOT be a number derived from something easily known about the CAC-Eligible Contractor, such as part of a SSN, birthday, anniversary date, telephone number, or address. Do NOT write down the PIN.

- **The CAC-Eligible Contractor's government unclassified email address, if the CAC-Eligible Contractor uses a government computer.** Be sure to print the CAC-Eligible Contractor's full, unclassified email address (not the display name, and not a personal email address). The CAC-Eligible Contractor's computer system administrators can help with entering the correct address. If a work email address is not available, the card will be issued without an email certificate and the email address can be added later using the RAPIDS Self Service Portal.

If a CAC-Eligible Contractor encounters a problem obtaining a new card at the RAPIDS Site, and the problem is related to vetting, the CAC-Eligible Contractor should follow up with his/her sponsor or COR. If the problem is related to the CAC-Eligible Contractor's record in DEERS, the CAC-Eligible Contractor should follow up with the TA. If the CAC-Eligible Contractor does not know who his/her TA is, he/she should contact the CAC-Eligible Contractor's COR.

Prior to taking an overseas assignment, CAC-Eligible Contractors are encouraged to review their CAC expiration date. All CAC-Eligible Contractors deploying outside the continental United States must have a Letter of Authorization (LOA) that has been issued by the Contracting Officer (CO) through the Synchronized Predeployment and Operational Tracker (SPOT) system in order to receive or renew the appropriate CAC. These credentials may be issued within the continental United States, prior to deployment. All CAC-Eligible Contractors preparing to work outside the continental United States (OCONUS), but not in the area of responsibility must be processed by COs in accordance with all Status of Forces Agreements/Technical Expert Status Agreements through the DoD CAC-Eligible Contractor Personnel Office (DOCPER). CACs with overseas conditions may only be issued once the CAC-Eligible Contractor is in the host country they are assigned to work in.

2.3 CAC and Network Access

For Network Access, CACs can be used to access computers and networks equipped with a smartcard reader. The ICC on the front of the card contains information about the card holder, including a Personal Identification Number (PIN), created by the card holder at card issuance, and Public Key Infrastructure (PKI) digital certificates. When the CAC-Eligible Contractor inserts the CAC into the smartcard reader, the device asks for a PIN. Once the PIN is entered, it is communicated to the middleware software to confirm the CAC holder's identity and the entered PIN is matched with the PIN stored on the CAC. After three incorrect PIN attempts, the chip on the CAC will lock.

Personal Identification Verification (PIV) authentication certificates are issued within the CAC which are used to access a computer, digitally sign a document, or encrypt an email, signature and encryption certificates are issued. The CAC works in virtually all modern computer operating systems. A card reader, drivers, and middleware are all required to read and process the information stored on a CAC. The list of approved middleware products can be found on the FIPS 201 Approved Products List (APL), web site, under the "PIV Middleware" category.

2.4 CAC Maintenance, Renewing and Returning CACs, Lost or Stolen CACs, and Transferring CACs

Maintenance: To maintain a CAC, visit milConnect, a web application provided by the Defense Manpower Data Center (DMDC). CAC-Eligible Contractors can perform the following services at milConnect under the "ID Card" tab and by selecting "Update ID Cards – (CAC Login Only)":

- Add/Change email addresses to receive initial or new Signature and Encryption Certificates
- Add Personnel Category Code to the User Principal Name of the Signature Certificate
- Activate the PIV Authentication Certificate
- Download applications
- View/Update contact information

Renewal: CACs can be renewed up to 90 days in advance of the expiration date. If the contract under which the CAC-Eligible Contractor is working is renewed or extended, the CAC should be renewed to coincide with the end date of the contract, including option years or three years from the date the TASS application is approved, whichever is earlier. To renew a CAC, the TA will process and approve a new TASS application through the end date of the contract. Then, the CAC-Eligible Contractor should visit the nearest RAPIDS Site to receive a new CAC.

Returning CACs: Since CACs are government furnished property, all Contractors **must** return their CACs to their TA, their DoD Sponsor, or a RAPIDS Site at the completion of, termination of, end of affiliation with a contract, or upon CAC expiration. The CO may

delay final payment under the contract if the card holder (Contractor) fails to comply with these requirements.

Lost or Stolen CACs: If a CAC is stolen, lost, unaccounted for, or otherwise suspected of potential or actual unauthorized use, the Contractor must report the loss to his/her TASS TA and DoD security personnel and the TA will immediately revoke the CAC in TASS. The Contractor is required to present documentation from his/her local security office, CAC sponsor, or from the police department confirming that the CAC has been reported lost or stolen. This documentation must be scanned and stored in DEERS. A new CAC will be issued with the original expiration date to replace the missing CAC.

Transferring CACs: If a Contractor is moving from a DoD contract, to another DoD contract, the Trusted Agent Security Manager (TASM) can transfer the TASS record from the original TA to a new TA. The new TA can use the same TASS record to update the Contract Number and Period of Performance.

If a Contractor is moving from a DoD Contract to another contract anywhere within the Federal Government, the DoD TA must revoke the Contractor CAC.

2.5 Guidance for Contracting Officers and Contracting Officers Representatives

2.5.1 Components of CAC-Eligible Contractor Credentialing Process

When a contract is awarded, the CO nominates a COR to act as a liaison between the CAC-Eligible Contractor and the CO. The CO may also act as the COR and perform the same duties described herein. The COR/CO is responsible for ensuring that the CAC-Eligible Contractor is meeting the contract requirements and also monitors the CAC-Eligible Contractor performance (*See the DoD COR Handbook for more information*). If no COR/CO is assigned, contact the security office of the supported agency.

In some cases, the COR/CO is also the TA who is responsible for sponsoring CAC-Eligible Contractor CACs. It is the TA's/COR's/CO's responsibility to ensure that the CAC-Eligible Contractor is performing work under a DoD contract, has a valid need for the CAC, and has favorable background/vetting results. The TA/COR/CO should never authorize a CAC without documented vetting results from their security office. It is the TA/COR/CO's responsibility to issue, re-verify, re-issue, and revoke CACs for Contractors.

APPENDIX A: GLOSSARY

Acronym	Definition	Hyperlink
CAC	Common Access Card	http://www.cac.mil/
CAC-Eligible Contractor	Contractor who is performing under a current DoD contract and is sponsored by the DoD	
CO	Contracting Officer	
COR	Contracting Officer Representative	
COTR	Contracting Officer Technical Representative	
DEERS	Defense Enrollment Eligibility Reporting System	http://www.tricare.mil/DEERS
DFARS	Defense Federal Acquisition Regulations Supplement	DFARS
DoD	Department of Defense	DoD
DoDI	Department of Defense Instruction	
DoDM	Department of Defense Manual	
e-QIP	Electronic Questionnaires for Investigations Processing System	http://www.opm.gov/investigations/e-qip-application/
FAR	Federal Acquisition Regulations	http://www.acquisition.gov/far/
FBI	Federal Bureau of Investigation	www.fbi.gov
FSO	Facilities Security Officer	

HSPD-12	Homeland Security Presidential Directive 12: Policy for a Common Identification for Federal Employees and Contractors: This directive mandates a federal standard for secure and reliable forms of identification.	https://www.dhs.gov/homeland-security-presidential-directive-12
JPAS	Joint Personal Adjudication System	http://www.dss.mil/diss/jpas/jpas.html
Logical Access	Electronic access controls authenticated through outside certificates that are accepted by the DoD and limits access to data files and systems to only vetted individuals	
milConnect	milConnect is a web application provided by the DMDC that offers sponsors, spouses, and their children (18 years and older) access to their personal information, health care eligibility, personnel records, and other information from a centralized location.	milConnect
NACI	National Agency Check with Inquiries: This investigation is composed of a NAC plus written inquiries to current and past employers, schools, references, and local law enforcement agencies covering the past five years and if applicable, to appropriate agencies for any identified arrests. All DoD NACIs include a credit check.	
NACLC	National Agency Check with Law and Credit: Used as the initial investigation for contractors at the Confidential, Secret, and L access levels.	
Network Access	Access to DoD unclassified and classified information systems including networks (e.g., non-classified Internet Protocol Router Network, Secret Internet Protocol Router Network (SIPRNET)), Defense Research and Engineering Network, Secret Defense Research and Engineering Network web servers, and e-mail systems	
PIN	Personal Identification Number	FIPS 201.com
PIV	Personal Identity Verification	

Physical Access	Access for DoD and non-DoD personnel entering or exiting DoD facilities or installations that is authenticated by a physical access control system (PACS).	
PKI	Public Key Infrastructure	
RAPIDS	Real-time Automated Personnel Identification System	RAPIDS
RAPIDS Site Locator	Website to locate RAPIDS Sites	RAPIDS Site Locator
Requiring Activity	A DoD component/activity/service that identifies and receives contracted support during military operations. See also supported unit.	
SSBI	Single Scope Background Investigation	
TA	Trusted Agent	
TASM	Trusted Agent Security Manager	
TASS	Trusted Associate Sponsorship System (formerly known as Contractor Verification System(CVS))	TASS
VO	Verifying Official	

APPENDIX B: Agency Resources/References

DoD CAC Resource Page
http://www.cac.mil/common-access-card/

milConnect
https://www.dmdc.osd.mil/milconnect

TASS
https://www.dmdc.osd.mil/tass/

TASS FAQ
https://www.dmdc.osd.mil/tass/faqPopWindow

DMDC CAC Resource Page
http://www.cac.mil/resources/

DoD Uniformed Services ID Card
http://www.cac.mil/uniformed-services-id-card/

Federal Information Processing Standards (FIPS) Publication 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors"
http://www.cac.mil/docs/FIPS-201-1.pdf

DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals"
http://www.cac.mil/docs/DODI-1000.13.pdf

Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors"
http://www.dhs.gov/homeland-security-presidential-directive-12#1

DoD Instruction 1341.2, "DEERS Procedures"
http://www.cac.mil/docs/DODI-1341.2.pdf

Office of Personnel Management: Federal Investigation Services
http://www.opm.gov/investigations/background-investigations/

e-QIP Application
http://www.opm.gov/investigations/e-qip-application/

National Industry Security Program (via DSS)
http://www.dss.mil/isp/fac_clear/download_nispom.html

DoD Directive 8570.01-M, Information Assurance Workforce Improvement Program Manual
http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

APPENDIX C: Forms

Questionnaire for Non-Sensitive Positions: SF-85

Questionnaire for Public Trust Positions: SF-85P

Questionnaire for National Security Positions: SF-86

Valid Forms of Identification List: I-9

***DoD Public Key Infrastructure Certificate of Acceptance and Acknowledgement of Responsibilities (Registration Official): Form 2841

Instructions for DD Form 2841

***DoD Public Key Infrastructure Certificate of Acceptance and Acknowledgement of Responsibilities (Subscriber): Form 2842

Application for Identification Card/DEERS Enrollment: DD Form 1172-2

Instructions for DD Form 1172-2

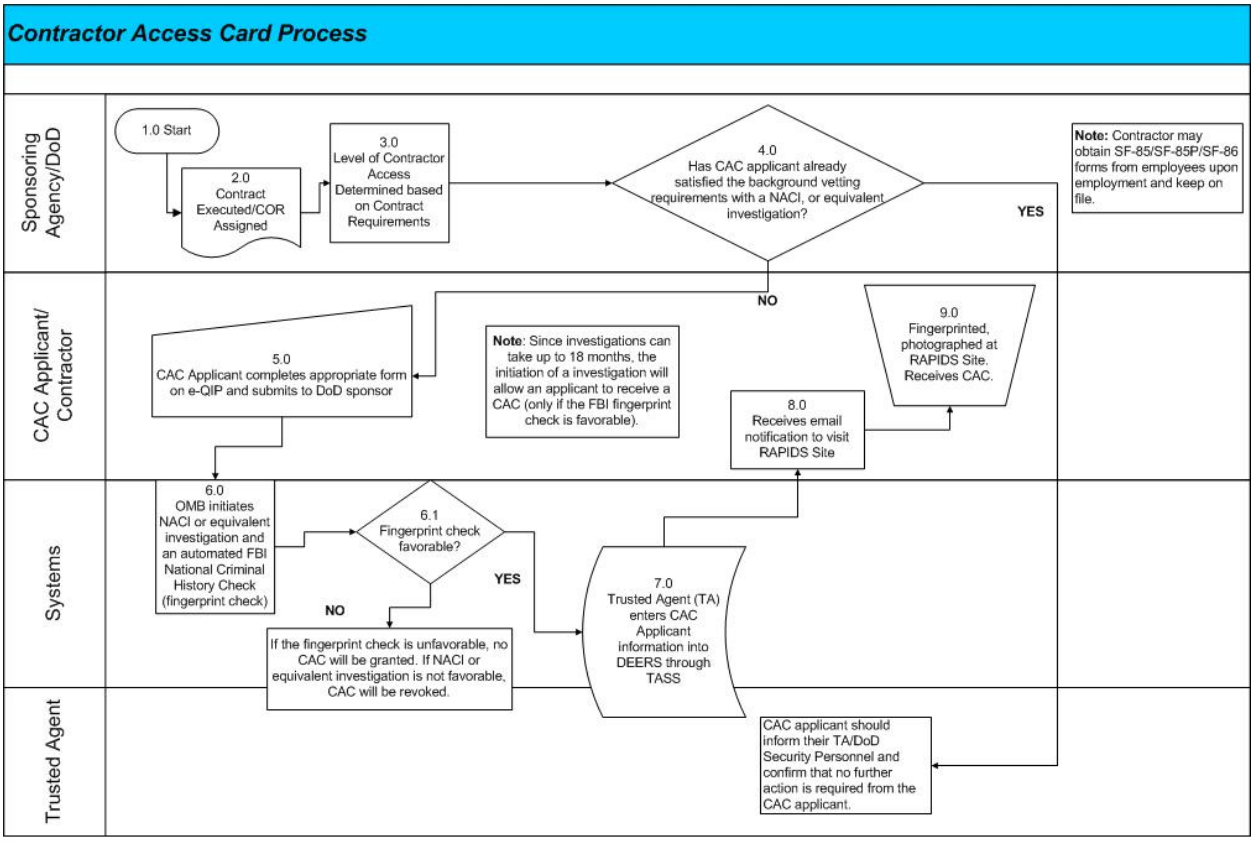
These forms are completed at the time of CAC issuance.

APPENDIX D: CAC Application Checklist

The following is a checklist for CAC-Eligible Contractors to follow during the CAC application process.

✓	**Items**	**Reference to Guidebook Section**
	Effective and signed contract between Contractor's employer and a DoD Service/Component/Agency for Contractor's services/products	
	Inform TA of existing investigation or security clearance, OR complete one of the following forms: SF85, SF-85P, or SF-86 using e-QIP	Section 2.3.1
	Initiated NACI, NACLC or equivalent investigation	Section 2.2 and Section 2.31
	Returned favorable results of FBI fingerprint check	Section 2.2 and Section 2.31
	Complete and return TASS application (TA creates application; Contractor completes and returns application)	Section 2.3.2
	Approved TASS application (TA approves TASS application)	Section 2.3.2
	Visit to a RAPIDS Site for CAC issuance with required identity and eligibility documentation	Section 2.3.2 and 2.34

APPENDIX E: CAC Application Process (VISIO)



Key:
CAC-Common Access Card
SF-Standard Form
NACI-National Agency Check with Inquiries
FBI-Federal Bureau of Investigation
DEERS-Defense Enrollment Eligibility Reporting System
TASS-Trusted Agent Sponsorship System
RAPIDS-Real-Time Automated Personnel Identification System