U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

US Coast Guard Stop 7202
2703 Martin Luther King JR Ave SE
Washington, DC 20593-7202
Staff Symbol: CG-DCMS-34
Phone: (202) 372-3703

COMDTINST 5500.18
09 SEP 2019

COMMANDANT INSTRUCTION 5500.18

Subj: COAST GUARD TRUSTED ASSOCIATE SPONSORSHIP SYSTEM (TASS)

Ref: (a) DoD Personnel Identity Protection (PIP) Program, DoD Instruction 1000.25, March 02, 2016
(b) DoD Identification (ID) Cards: ID Card Life-Cycle, DoD Manual 1000.13, Volume 1, January 23, 2014
(c) Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, HSPD-12, August 27, 2004
(d) Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals, DoD Instruction 1000.13, Incorporating Change 1, December 14, 2017
(e) Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standards Publication, FIPS PUB 201 (series)
(f) TASS Personnel Category Descriptions, TASS v5.7v3
(g) Defense Manpower Data Center (DMDC) Trusted Associate Sponsorship System (TASS) Overview Guide Version 5.7, September 2018
(h) DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC), DoD Instruction 5200.46, September 09, 2014, Incorporating Change 1, May 4, 2018
(i) Auxiliary Manual, COMDTINST M16790.1 (series)
(j) U.S. Coast Guard Cybersecurity Manual, COMDTINST M5500.13 (series) (FOUO)
(k) Visits and Assignments of Foreign Nationals, DoD Directive 5230.20, June 22, 2005
(l) Coast Guard Nonappropriated Fund (NAF) Personnel Manual, COMDTINST M12271.1 (series)
(m) DoD Civilian Personnel Management System: Employment of Foreign Nationals, DoD Instruction 1400.25, Volume 1231, June 05, 2011
(n) United States Forces, Japan USFJ Instruction HQ USF JI 36-502, Utilization of Local National Personnel, August 9, 2017

DISTRIBUTION – SDL No. 170

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X		X		X	X				
B	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
C	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
D	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
E	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		
F																	X	X	X							
G		X	X	X	X																					
H	X	X	X	X	X	X	X																			

NON-STANDARD DISTRIBUTION:

1. PURPOSE. This Instruction establishes Coast Guard policies and procedures for managing and executing the Defense Manpower Data Center (DMDC) Trusted Associate Sponsorship System (TASS).

2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements must comply with the provisions of this Instruction. Internet release is authorized.

3. DIRECTIVES AFFECTED. None.

4. DISCUSSION.

   a. DMDC is mandated to procure and distribute Federal Government access credentials by utilizing the Defense Enrollment Eligibility Reporting System (DEERS), Real-Time Automated Personnel Identification System (RAPIDS), and the TASS infrastructure. The Coast Guard utilizes TASS to issue the Common Access Card (CAC), the Volunteer Logical Access Credential (VoLAC) and Auxiliary Logical Access Card (ALAC) under DoD policy guidance as directed in References (a) through (h). Throughout this Instruction, the terms 'Federal Government access credential(s)' or 'access credential(s)' are used when referring to all three cards. These Federal Government credentials shall serve as the Federal Personal Identity Verification (PIV) cards for implementation of HSPD-12.

   b. As a web-based system, TASS allows Coast Guard-eligible sponsored populations (e.g. Affiliated Volunteers (those requiring Coast Guard Network access), DoD and Uniformed Service Contractors, Foreign Affiliates, non-DoD Civil Service Employees, non-Federal Agency Civilian Associates, non-U.S. Citizen Non-Appropriated Fund (NAF) Employees, Outside Continental United States (OCONUS) Hires and Other Federal Agency Contractors) to apply for Federal Government credentials(s) through a Government Sponsor and Trusted Agent (TA). The TASS application was designed to automate the paper application process of using the DD Form 1172-2 for Federal Government credential card issuance and DEERS enrollment. The DD Form 1172-2 will no longer be required for sponsored personnel enrollment, with the limited exception of foreign military and foreign national personnel.

      NOTE: Congress has authorized DoD to require mandatory disclosure of Social Security Numbers (SSN) of all DEERS enrollees. Applicants cannot receive Federal Government access credentials without providing their SSN.

   c. The CAC is a secure and reliable form of identification that enhances security, increases operational efficiency, reduces identity fraud, and protects personal privacy. The CAC facilitates standardized, uniform regulated access to Coast Guard facilities, installations, and regulated logical access to computer systems. The VoLAC and ALAC provide secure and reliable regulated logical access to computer systems.

   d. All Federal Government credentials are the property of the U.S. Federal Government and must be returned to the Trusted Agent (TA) upon separation, resignation, firing, termination of contract or affiliation with the Coast Guard, or upon any other event in which the individual no longer requires the use of the Federal Government credential.

e. To prevent any unauthorized use, Federal Government credentials that are expired, invalidated, stolen, lost, or otherwise suspected of potential or actual unauthorized use must be revoked by a TA in TASS. A revocation in TASS simultaneously updates DEERS and terminates the personnel record; DEERS subsequently terminates the card and updates the Certificate Authority (CA), revoking Public Key Infrastructure (PKI) certificates on the card.

NOTE: Unauthorized possession or use of a Federal Government credential can be criminally prosecuted under 18 U.S.C. §§ 499, 701.

5. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide operational guidance for Coast Guard personnel and is not intended to nor does it impose legally-binding requirements on any party outside the Coast Guard.

6. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

a. The development of this Instruction and the general policies contained within it have been thoroughly reviewed by the originating office in conjunction with the Office of Environmental Management, Commandant (CG-47). This Instruction is categorically excluded under current Department of Homeland Security (DHS) categorical exclusion (CATEX) A3 from further environmental analysis in accordance with "Implementation of the National Environmental Policy Act (NEPA)", Department of Homeland Security (DHS) Instruction Manual 023-01-001-01 (series).

b. This Instruction will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policy in this Instruction must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), Department of Homeland Security (DHS) and Coast Guard NEPA policy, and compliance with all other applicable environmental mandates.

7. DISTRIBUTION. No paper distribution will be made of this Instruction. An electronic version will be located on the following Commandant (CG-612) CGPortal sites: https://cg.portal.uscg.mil/library/directives/SitePages/Home.aspx and Internet: http://www.dcms.uscg.mil/directives/ and CG TASS Portal: https://cg.portal.uscg.mil/units/dcms34/tass/Pages/default.aspx.

8. RECORDS MANAGEMENT CONSIDERATIONS. This Instruction has been evaluated for potential records management impacts. The development of this Instruction has been thoroughly reviewed during the directives clearance process, and it has been determined there are no further records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. § 3101, et seq., National Archives and Records Administration (NARA) requirements, and the Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). All records pertaining to personal identification credentials and cards are governed by General Records Schedule 5.6 item 120 and the Privacy Act of 1974. The applicable System of Records Notice Defense Manpower Data Center, 02 DoD, Defense Enrollment Eligibility Reporting System is (are) available at: https://dpcld.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/Article/?627618=dmd

c-02.dod. This policy does not have any significant or substantial change to existing records management requirements.

9. ROLES. The full Federal Government credential life-cycle process is comprised of several specific official roles that support the sponsorship, enrollment, issuance, and administrative procedures. This process may require more than one person to serve in an official role within TASS. The responsibilities for each role are summarized below:

   a. Government/Coast Guard Sponsors. Throughout this Instruction, the term 'Sponsor' is used when referring to the Government/Coast Guard Sponsor. Sponsors approve all TASS applicants to receive/retain government access credentials. The military or civilian Sponsor employee is the person affiliated with the Coast Guard who takes responsibility for verifying an applicant's need for a Federal Government credential. Sponsoring an applicant is a multi-step process that includes establishing the individual's eligibility, and verifying that the individual has the appropriate background investigation for issuance of a Federal Government credential. Sponsors will train and monitor cardholders to ensure sponsored members:

      (1) Adhere to the DD Form 2842, DoD PKI Certificate of Acceptance to protect their Federal Government credential.

      (2) Not display the Federal Government credential in public.

      (3) Secure their Federal Government credential in a manner that precludes unauthorized use.

      (4) Not abuse, deface or place holes in the Federal Government credential.

      (5) Make a report to their Sponsor, within one business day, if their Federal Government credential is lost, stolen, or otherwise compromised.

      (6) Turn in their Federal Government credential according to the termination procedures in Section 13 of this Instruction upon termination of affiliation with the Coast Guard.

      NOTE: Contractors cannot be Sponsors.

   b. Background Investigation (BI) Verifier. The BI Verifier is the individual responsible for validating that a Tier 1 investigation (equivalent or higher), has been favorably adjudicated or that a Tier 1 investigation (equivalent or higher) package has been successfully scheduled with the investigative service provider (ISP) and a Federal Bureau of Investigation (FBI) fingerprint check has been conducted with favorable results. The unit Command Security Officer (CSO) or Trusted Agent Security Manager (TASM) will fill the role of the BI Verifier. If applicable, the CSO/TASM will use the Office of Personnel Management (OPM) Central Verification System (CVS), or its successor system, to determine if the appropriate background investigation has been favorably adjudicated or successfully scheduled at the ISP with favorable FBI fingerprint results. The OPM CVS, or its successor system, is the system of record for all federal background investigations. If the CSO/TASM does not have access to OPM CVS, they may contact the Security Center (SECCEN) at FIN-SMB-SECHelpDesk@uscg.mil to verify whether the appropriate investigation has been favorably adjudicated or successfully scheduled at the ISP with favorable FBI fingerprint results.

c. Contracting Officer's Representative (COR). A COR is a Coast Guard military or civilian employee designated by the Contracting Officer (KO) in writing to perform specific technical and administrative functions. The COR verifies the unit's need for a contractor employee to apply for a CAC. The COR also confirms eligibility and level of access of contractor employee. The COR is usually the Sponsor and Trusted Agent. All contractor employee applicants for a CAC must be overseen by a military or civilian Coast Guard COR.

d. Trusted Agent (TA). The TA is a military or civilian Coast Guard employee custodian for TASS applicants. The TA is referred to in Reference (g) as the TASS sponsor. The TA must verify the unit's need and applicant's affiliation for requesting a Federal Government credential. The TA must account for all Federal Government credential applicants they are assigned responsibility for in TASS. TA(s) have the following administrative custodial responsibilities:

(1) Initiate the application for a Federal Government credential within TASS.

(2) Validate the contractor's eligibility and requirement for a Federal Government credential. This is based on the determination of the type, level and frequency of access required for Coast Guard facilities or networks that will effectively support the mission.

(3) Confirm physical access to multiple Coast Guard facilities or multiple federally controlled facilities on behalf of the Coast Guard on a recurring basis (a minimum of 2 times per week and/or 8 times per month) for a period of 6 months or more.

NOTE: Service Point of Contact (SPOC) approval is required for any issuance of less than 6 months.

(4) Reverify Federal Government credential applicant's continued Coast Guard affiliation within TASS.

(5) Revoke Federal Government credential accounts within TASS in accordance with Section 13 of this Instruction.

(6) Request transfers of Federal Government credential accounts within TASS if they are unable to continue TA responsibilities or applicant must be reassigned to another TA.

(7) Notify the Trusted Agent Security Manager (TASM), (SPOC) or DMDC Support Center (DSC) of any suspected or known TASS system compromise.

(8) Be current with the TASS Certification Training requirements available on the Coast Guard TASS Portal at: https://cg.portal.uscg.mil/units/dcms34/tass/Pages/Reference-Documents.aspx.

(9) Manage no more than 100 active applicants without justification and prior SPOC authorization.

(10) Responsible for confirming that the background investigation requirement(s) have been met for issuance of a Federal Government credential.

e. Trusted Agent Security Manager (TASM). All TASMs must be a military or civilian Coast Guard employee and is a TASS administrator for TA applicants. The TASM manages TASS and TA(s) assigned to their TASS site, including assigning and revoking TA privileges as required. The TASM is referred to in Reference (g) as the site manager. TASM(s) have the following responsibilities:

(1) Notify the SPOC or DSC of any suspected or known TASS system compromise.

(2) Be current with the TASS Certification Training requirements available on the Coast Guard TASS Portal at: https://cg.portal.uscg.mil/units/dcms34/tass/Pages/Reference-Documents.aspx.

(3) Act as a TA.

(4) Train an alternate site TASM and all TA(s) operating TASS.

(5) Meet TASM position requirements as specified in Reference (g).

(6) Coordinate all TASS matters with the SPOC.

(7) Answer TASS questions and troubleshoot issues for their site.

(8) Ensure TA(s) do not manage more than 100 active applicants without SPOC approval.

(9) Manage no more than 200 TA(s) without justification and SPOC approval.

f. Service Point of Contact (SPOC). Commandant (CG-DCMS-34) will appoint a Coast Guard SPOC to administer the TASS program under the guidance from DMDC. The SPOC creates policies, operating procedures, and other supporting documentation in support of Coast Guard-specific implementation. The SPOC(s) handle the day-to-day TASS management and operation. A SPOC may be a Coast Guard uniformed service member, Coast Guard Civilian, or Contractor working for the Coast Guard. SPOC(s) have the following additional responsibilities:

(1) Ensure that TASM(s) and TA(s) complete all initial required TASS training, including both the TASS Certification Web-based Training (WBT) and the TASS training available on the Coast Guard TASS Portal at: https://cg.portal.uscg.mil/units/dcms34/tass/Pages/Reference-Documents.aspx.

(2) Issue appointment letters to TASM(s) and TA(s) through their respective supervisors.

(3) Transfer Federal Government credential applicants from an existing TASM/TA to another TASM/TA within the TASS application.

(4) Be current with the TASS Certification Training requirements, available on the Coast Guard TASS Portal at: https://cg.portal.uscg.mil/units/dcms34/tass/Pages/Reference-Documents.aspx.

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

(6) Issue approval letters for TA(s) to manage more than 100 active applicants and review annually.

10. GOVERNMENT ACCESS CREDENTIAL ISSUANCE. A complete list of eligible sponsored personnel that can be placed in TASS to receive a Federal Government credential is detailed in Reference (f). Each personnel category has specific processes for Federal Government credential issuance. The Coast Guard-specific processes and general personnel category descriptions include:

a. DoD and Uniformed Service Contractors. This personnel category includes all Coast Guard contractors. Contractors receive a CAC as their form of a government access credential. Steps for contractor CAC issuance processes are:

(1) Sponsor Ensures Need. A CAC will only be issued to an eligible contractor applicant based on a clear need by a Coast Guard unit. The unit assigns a Sponsor who must take responsibility for verifying and authorizing the unit organization and applicant's need for a CAC. All contractor applicants for a CAC must be sponsored by a Coast Guard COR. The Sponsor must review the unit's need for the contractor applicant to perform tasks that require:

(a) Physical access to multiple Coast Guard facilities or multiple federally controlled facilities on behalf of the Coast Guard on a recurring basis (a minimum of 2 times per week and/or 8 times per month) for a period of 6 months or more.

NOTE: SPOC approval is required for any issuance of less than 6 months.

(b) Remote access, via logon, to Coast Guard network using Coast Guard-approved remote access procedures.

(c) Both physical access to Coast Guard facility and logical access, via logon, to Coast Guard networks on-site or remotely. Access to the Coast Guard network must require the use of a computer with Government-controlled configuration or use of Coast Guard-approved remote access procedure in accordance with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide.

(2) Investigative Requirements. Initial issuance of a contractor CAC requires a favorably adjudicated Tier 1 investigation (equivalent or higher) or a Tier 1 background investigation (equivalent or higher) package that has been successfully scheduled with the ISP and a FBI fingerprint check with favorable results. The TA and Sponsor or other appropriate Federal Government representative must coordinate with the unit BI Verifier (CSO/TASM) or SECCEN to confirm the appropriate investigation has been favorably adjudicated or scheduled at the ISP with favorable FBI fingerprint results. The applicant will not be approved for CAC issuance until the background investigation requirement has been validated by the BI Verifier (CSO/TASM) or SECCEN. The TA is responsible for confirming that the appropriate background investigation requirement(s) have been met for CAC issuance.

(3) Request CAC via TASS.

(a) The Sponsor requests a TA create a TASS CAC application for a contractor on behalf of the unit.

(b) When a TA receives a contractor CAC request they must verify the following:

1) Need for a CAC as indicated in Section 10.a.(1) of this Instruction.

2) Contractor applicant has the necessary background investigation as indicated in Section 10.a.(2) of this Instruction and Reference (h).

(c) Specific TASS instructions for creating a contractor CAC application can be found on the Coast Guard TASS Portal at: https://cg.portal.uscg.mil/units/dcms34/tass/Pages/Reference-Documents.aspx.

(d) The following selections must be performed when creating an application:

1) Personnel Category Block: 'DoD and Uniformed Service Contractor'.

2) Contractor Type: 'Contractor Type Not Applicable'.

3) Agency: 'U.S. Coast Guard'.

4) Eligibility Expiration Date: end date of contract not to exceed 3 years.

5) Contract Number: Task Order Number from the contract. Follow guidance from the Coast Guard TASS Portal at: https://cg.portal.uscg.mil/units/dcms34/tass/Pages/TASS-FAQs.aspx.

6) Contract End Date: current period of performance to include all option years.

7) Check the box to certify that you have verified the applicant's background.

(e) Once a new TASS application is created, the TA provides the applicant with the TASS URL and a username. The TA must send a temporary password separately. The applicant can then log into TASS to complete and submit the application. Once the TA submits the application, the applicant has 7 days to complete an initial login to TASS and begin the application process, or TASS will automatically disable the application.

(f) Once 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 TA cannot process the application until the applicant submits a complete form. Once the applicant submits a completed application, the system automatically sends an email notification to the TA. The TA must approve the application within 30 days; otherwise, TASS will automatically disable the application. The applicant cannot make changes to a submitted application unless the TA returns the application to the applicant for correction.

(g) The TA must review the applicant's submission in TASS and approve or reject it. Approved applications generate an automated email to the applicant's email address saved in TASS. The email will contain instructions detailing how the applicant makes an appointment at a RAPIDS site to be issued a CAC. The contractor applicant is required to obtain a CAC from the RAPIDS issuing facility within 90 days; otherwise, TASS automatically disables the application.

b. Affiliated Volunteers - Auxiliary. Reference (i) identifies Auxiliary members requiring Coast Guard Network access based upon the nature of the support that they provide to Coast Guard units. Steps for ALAC issuance process:

NOTE: The only Auxiliary card TASS processes is the ALAC. See Reference (i) for other forms of Auxiliary identification.

(1) Sponsor Ensures Need. An ALAC will only be issued to an eligible Auxiliary applicant based on a clear need by a Coast Guard unit. This need is based directly upon the nature of the support that they provide to Coast Guard units; some Auxiliarists may require access to Coast Guard networks. Since ALACs allow regulated logical access to sensitive information systems, they must be issued on a strictly controlled and limited basis to Auxiliarists who have a well-defined, well-justified, and sustained need for logical access as verified by their sponsoring Coast Guard unit or office. All Auxiliary applicants for an ALAC must be sponsored by a military or civilian Coast Guard employee ALAC TA who serves on Director of Auxiliary staff. The TA must review the unit's need for the Auxiliary applicant to perform tasks that require logical access to information systems on site or remotely.

(2) Verify Eligible Sponsored Populations. The TA must confirm the Auxiliary applicants' eligibility for an ALAC. Eligibility is based on the Sponsor's determination of the type and frequency of logical access required for Coast Guard networks that will effectively support the mission.

NOTE: An ALAC is not a CAC. It must not display a photograph, does not convey benefits, entitlements, or privileges, and will not be used for physical access.

(3) Investigative Requirements. Initial issuance of an ALAC requires a favorably adjudicated Tier 1 investigation (equivalent or higher) or a Tier 1 background investigation (equivalent or higher) package that has been successfully scheduled with the ISP and a FBI fingerprint check with favorable results. The TA and Sponsor or other appropriate Federal Government representative must coordinate with the unit BI Verifier (CSO/TASM) or SECCEN to confirm the appropriate investigation has been favorably adjudicated or scheduled at the ISP with favorable FBI fingerprint results. The applicant will not be approved for ALAC issuance until the background investigation requirement has been validated by the BI Verifier (CSO/TASM) or SECCEN. The TA is responsible for confirming that the appropriate background investigation requirement(s) have been met for ALAC issuance.

(4) Request ALAC via TASS.

(a) The Sponsor contacts the TA to create a TASS application for an ALAC on behalf of the Sponsoring unit.

(b) When a TA receives an ALAC request from a Sponsor they must verify the following:

1) Need for an ALAC as indicated in Section 10.b.(1) of this Instruction.

2) Auxiliary applicant has met the investigative requirement as indicated in Section 10.b.(3) of this Instruction with favorable FBI fingerprint check to be issued an ALAC.

(c) Upon confirmation of actions listed in 10.b.(4).(b) above, the Auxiliary TA creates the TASS application.

(d) Specific TASS details that are required for a Coast Guard Auxiliary member include:

1) Personnel Category Block: 'Affiliated Volunteers'.

2) Volunteer Type: 'U.S. Coast Guard Auxiliary'.

3) Eligibility Expiration Date: end date of duty requiring access, not to exceed 3 years.

(e) Once a new TASS application is created, the TA provides the applicant with the TASS URL and a username. The TA must send a temporary password separately. The applicant can then log into TASS to complete and submit the application. Once the TA submits the application, the applicant has 7 days to complete an initial login to TASS and begin the application process, or TASS will automatically disable the application.

(f) Once 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 TA cannot process the application until the applicant submits a complete form. Once the applicant submits a completed application, the system automatically sends an email notification to the TA. The TA has 30 days to approve the application; otherwise, TASS will automatically disable the application. The applicant cannot make changes to a submitted application unless the TA returns the application to the applicant for correction.

(g) The TA must review the applicant's submission in TASS and approve or reject it. Approved applications generate an automated email to the applicant's email address saved in TASS. The email contains instructions detailing how the applicant makes an appointment at a RAPIDS site to be issued an ALAC. The Auxiliary applicant is required to obtain an ALAC from the RAPIDS issuing facility within 90 days; otherwise, TASS automatically disables the application.

c. Affiliated Volunteers – other than Auxiliary. Affiliated Volunteers (e.g. Student Intern Program and Specific Family Support Members (Ombudsmen-at-Large)) requiring Coast Guard Network access receive a VoLAC as their form of Federal Government access credential. Steps for VoLAC issuance process:

(1) Sponsor Ensures Need. A VoLAC will only be issued to an eligible volunteer applicant based on a clear need by a Coast Guard unit. This need is based directly upon the nature of

the support that they provide to Coast Guard units when these volunteers require access to Coast Guard networks. The unit assigns a TA who takes responsibility for verifying and authorizing the unit organization and applicant's need for a VoLAC. Upon determination of the need for a VoLAC, the TA must review the unit's need for the volunteer applicant to perform tasks that require logical access to Coast Guard information systems on site or remotely.

NOTE: A VoLAC is not a CAC. It must not display a photograph, does not convey benefits, entitlements, or privileges, and will not be used for physical access.

NOTE: IAW Reference (j), local ombudsmen are not authorized CGOne accounts.

(2) Investigative Requirements. Initial issuance of a VoLAC requires a favorably adjudicated Tier 1 investigation (equivalent or higher) or a Tier 1 background investigation (equivalent or higher) package that has been successfully scheduled with the ISP and a FBI fingerprint check with favorable results. The TA and VoLAC PM (for interns) or other appropriate Federal Government representative must coordinate with the unit BI Verifier (CSO/TASM) or SECCEN to confirm the appropriate investigation has been favorably adjudicated or scheduled at the ISP with favorable FBI fingerprint results. The applicant will not be approved for VoLAC issuance until the background investigation requirement has been validated by the BI Verifier (CSO/TASM) or SECCEN. The TA is responsible for confirming that the appropriate background investigation requirement(s) have been met for VoLAC issuance.

(3) Request VoLAC via TASS.

(a) The Sponsor identifies a TA to create a TASS application for a VoLAC on behalf of the sponsoring unit. The Ombudsman Program Manager is by definition the Sponsor for the Ombudsmen-at-Large. Contact Coast Guard SPOC and TASS Support Team at HQS-SMB-TASSProgram@uscg.mil for assistance.

(b) When a TA receives a VoLAC request from a Sponsor they must verify the:

1) Need for a VoLAC as indicated in Section 10.c.(1) of this Instruction.

2) Volunteer applicant has met the necessary background investigation requirements as indicated in Section 10.c.(2) of this Instruction.

(c) Upon confirmation of actions listed in 10.c.(3).(b) above, the TA creates the TASS application.

(d) Specific TASS details that are required for a VoLAC include:

1) Personnel Category Block: 'Affiliated Volunteers'.

2) Volunteer Type: 'Student Intern', 'Family Support' etc. as applicable.

3) Eligibility Expiration Date: enter expected end date of internship or spouse rotation date as appropriate, not to exceed 3 years from application date.

(e) Once a new TASS application is created, the TA provides the applicant with the TASS URL and a username. The TA must send a temporary password separately. The applicant can then log into TASS to complete and submit the application. Once the TA submits the application, the applicant has 7 days to complete an initial login to TASS and begin the application process, or TASS will automatically disable the application.

(f) Once 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 TA cannot process the application until the applicant submits a complete form. Once the applicant submits a completed application, the system automatically sends an email notification to the TA. The TA has 30 days to approve the application; otherwise, TASS will automatically disable the application. The applicant cannot make changes to a submitted application unless the TA returns the application to the applicant for correction.

(g) The TA must review the applicant's submission in TASS and approve or reject it. Approved applications generate an automated email to the applicant's email address saved in TASS. The email contains instructions detailing how the applicant makes an appointment at a RAPIDS site to be issued a VoLAC. The volunteer applicant is required to obtain a VoLAC from the RAPIDS issuing facility within 90 days; otherwise, TASS automatically disables the application.

d. Sponsored Foreign Affiliates. Foreign Affiliates (E.g. foreign military, foreign civilian and foreign contractors) receive a CAC as their form of Federal Government access credential. Per Reference (b), this category of personnel are CAC-eligible only if sponsored by their government as part of an official U.S. visit or assigned to work on a Coast Guard facility and/or require access to Coast Guard networks both on site or remotely (remote access must be on an exception only basis for this category) to support Coast Guard missions. Sections 9.g and 9.h of this Instruction covers procedures for a CAC(s) involving employment of non-U.S. Citizen NAF employees and OCONUS foreign nationals. Foreign Affiliates issuance process:

(1) Sponsor Ensures Need/Eligibility. Per Reference (k), requests for official visits within the United States must be submitted through the sponsoring government's Embassy in Washington, D.C. by the sponsoring international organization using the Foreign Visits System (FVS) and International Visits Program (IVP) procedures. Per Reference (k), sponsored visits by foreign national, except visits at activities or events that are open to the general public, must be documented using the Foreign Visits System Confirmation Module (FVS-CM) where practicable. The U.S. State Department or Embassy may use an Invitational Travel Order (ITO) for International Military Students (IMS). Sponsorship of foreign military exchange personnel are coordinated in accordance with International Memorandums of Understandings (MOUs). A CAC will only be issued to an eligible individual based on a clear need by the Coast Guard unit. The unit assigns a TA who takes responsibility for verifying and authorizing the unit organization and applicant's need for a CAC. All Foreign Affiliate applicants for a CAC must be sponsored by the U.S. State

Department and a military or civilian Coast Guard employee. Upon determination of the need for a CAC (e.g. foreign military member attending Coast Guard school, etc.); the TA must review the unit's need for the applicant to perform tasks that require one of the following:

(a) Coast Guard facilities physical and logical access, via logon, to Coast Guard networks on-site. Access to the Coast Guard network must require the use of a computer with Government-controlled configuration in accordance with the DISA Security Technical Implementation Guide.

(b) Confirm physical access to multiple Coast Guard facilities or multiple federally controlled facilities on behalf of the Coast Guard on a recurring basis (a minimum of 2 times per week and/or 8 times per month) for a period of 6 months or more.

NOTE: SPOC approval is required for any issuance of less than 6 months.

NOTE: FVS-CM Link; https://spanweb.dtsa.mil/SystemResources/NIPR/documents/fvscm/fvscm_sum.pdf

NOTE: As a Foreign Affiliate, a DD Form 1172-2 may be required for DEERS sponsored personnel enrollment.

(2) Investigative Requirements. Except for uniformed services members, non-U.S. Citizen CAC applicants that do not meet the criteria to complete a Tier 1 investigation (e.g., U.S. residency requirements), must meet one of the criteria in subparagraph 2.(a) or 2.(b) below, prior to CAC issuance. Per Reference (b), specific background investigation conducted on the non-U.S. Citizen may vary based on governing international agreements. The Sponsor is responsible for providing the TA proof that appropriate investigations has occurred. The TA is responsible for confirming that the appropriate requirements have been met for CAC issuance to a non-U.S. Citizen. The non-U.S. Citizen must:

(a) Possess (as foreign military, employee, or contract support personnel) a visit status and security assurance that has been confirmed, documented, and processed in accordance with international agreements pursuant to Reference (k). Documentation includes ITOs and appropriate documents in accordance with International MOUs.

(b) Meet the investigative requirements as recognized through international agreements.

(3) Request CAC via TASS.

(a) The Sponsor identifies a TA to create a TASS application for a CAC on behalf of the Sponsoring unit/organization. The Sponsor can contact the Coast Guard SPOC and TASS Support Team at: HQS-SMB-TASSProgram@uscg.mil for further guidance.

(b) When a TA receives a CAC request they must verify:

1) Need for a CAC as indicated in Section 10.d.(1) of this Instruction.

2) Foreign Affiliates applicant has met necessary background investigation requirements as indicated in Section 10.d.(2) of this Instruction.

(c) Upon confirmation of actions listed in 10.d.(3).(b) above, the TA creates the TASS application.

(d) Specific TASS details that are required for a Foreign Affiliates include:

1) Personnel Category Block: 'Foreign Affiliates'.

2) Foreign Affiliates Type: 'Foreign Civilian', 'Foreign Contractor', or 'Foreign Military'.

3) If foreign military: Organization; 'Foreign Army', 'Foreign Navy' etc.

4) Personal Identifier: enter Foreign Identification Number (FIN) if applicant does not have a SSN.

5) Eligibility Expiration Date: end date of class or estimated time for the need of access, not to exceed 3 years.

NOTE: Due to multiple subcategories and differences within this category, Sponsors and TAs may Contact Coast Guard SPOC and TASS Support Team at HQS-SMB-TASSProgram@uscg.mil for assistance.

(e) Once a new TASS application is created, the TA provides the applicant with the TASS URL and a username. The TA must send a temporary password separately. The applicant can then log into TASS to complete and submit the application. Once the TA submits the application, the applicant has 7 days to complete an initial login to TASS and begin the application process, or TASS will automatically disable the application.

(f) Once 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 TA cannot process the application until the applicant submits a complete form. Once the applicant submits a completed application, the system automatically sends an email notification to the TA. The TA has 30 days to approve the application; otherwise, TASS will automatically disable the application. The applicant cannot make changes to a submitted application unless the TA returns the application to the applicant for correction.

(g) The TA must review the applicant's submitted CAC application and approve or reject it. Approved applications will generate an automated email to the applicant's email address saved in TASS. The email contains instructions detailing how the applicant makes an appointment at a RAPIDS site to be issued a CAC. The applicant is required to obtain a CAC from the RAPIDS Issuing Facility within 90 days; otherwise, TASS automatically disables the application.

e. Non-DoD Civil Service Employee. Non-DoD Civil Service Employees (E.g. Department of Homeland Security, Department of State, Department of Transportation, etc.) receive a CAC as their form of Federal Government access credential. Non-DoD Civil Service Employees issuance process:

(1) Sponsor Ensures Need. A CAC will only be issued to an eligible non-DoD Civil Service Employee based on a clear need by a Coast Guard unit. All applicants for a CAC must be sponsored by a military or civilian Coast Guard employee. Upon determination of the need for a CAC (e.g. DHS employee assigned to work at a Coast Guard facility); the Sponsor must review the unit's need for the applicant to perform tasks that require one of the following:

(a) Physical access to multiple Coast Guard facilities or multiple federally controlled facilities on behalf of the Coast Guard on a recurring basis (a minimum of 2 times per week and/or 8 times per month) for a period of 6 months or more.

NOTE: SPOC approval is required for any issuance of less than 6 months.

(b) Remote access, via logon, to Coast Guard network using Coast Guard-approved remote access procedures.

(c) Both physical access to Coast Guard facility and logical access, via logon, to Coast Guard networks on-site or remotely. Access to the Coast Guard network must require the use of a computer with Government-controlled configuration or use of Coast Guard-approved remote access procedure in accordance with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide.

(2) Verify Eligible Sponsored Populations. The TA must confirm CAC eligibility based on the Sponsor's determination of the type, level and frequency of access required to Coast Guard facilities or networks that will effectively support the mission.

(3) Investigative Requirements. Initial issuance of a CAC requires a favorably adjudicated Tier 1 investigation (equivalent or higher) or a Tier 1 background investigation (equivalent or higher) package that has been successfully scheduled with the ISP and a FBI fingerprint check with favorable results. The TA and Sponsor or other appropriate Federal Government representative must coordinate with the unit BI Verifier (CSO/TASM) or SECCEN to confirm the appropriate investigation has been favorably adjudicated or scheduled at the ISP with favorable FBI fingerprint results. The applicant will not be approved for CAC issuance until the background investigation requirement has been validated by the BI Verifier (CSO/TASM) or SECCEN. The TA is responsible for confirming that the appropriate background investigation requirement(s) have been met for CAC issuance.

(4) Request CAC via TASS.

(a) The Sponsor identifies a TA to create a TASS application for a CAC on behalf of the sponsoring unit.

(b) When a TA receives a CAC request they must verify the:

1) Need for a CAC as indicated in Section 10.e.(1) of this Instruction.

2) Non-DoD Civil Service Employee applicant has the necessary background investigation as indicated in Section 10.e.(3) of this Instruction.

(c) Upon confirmation of actions listed in 10.e.(4).(b) above, the TA creates the TASS application.

(d) Specific TASS details that are required for a non-DoD Civil Service Employee include:

1) Personnel Category Block: 'Non-DoD Civil Service Employee'.

2) Government Agency: select appropriate Agency per Reference (f).

3) Eligibility Expiration Date: end date of work with Coast Guard not to exceed 3 years.

(e) Once a new TASS application is created, the TA provides the applicant with the TASS URL and a username. The TA must send a temporary password separately. The applicant can then log in to TASS to complete and submit the application. Once the TA submits the application, the applicant has 7 days to complete an initial login to TASS and begin the application process, or TASS will automatically disable the application.

(f) Once 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 TA cannot process the application until the applicant submits a complete form. Once the applicant submits a completed application, the system automatically sends an email notification to the TA. The TA has 30 days to approve the application; otherwise, TASS will automatically disable the application. The applicant cannot make changes to a submitted application unless the TA returns the application to the applicant for correction

(g) The TA must review the applicant's submitted CAC application and approve or reject it. Approved applications will generate an automated email to the applicant's email address saved in TASS. The email contains instructions detailing how the applicant makes an appointment at a RAPIDS site to be issued a CAC. The applicant is required to obtain a CAC from the RAPIDS Issuing Facility within 90 days; otherwise, TASS automatically disables the application.

f. Non-Federal Agency Civilian Associates. Non-Federal Agency Civilian Associates (E.g. National Guard State Employees or other State and local Government employees) receive a CAC as their form of Federal Government access credential. Non-Federal Agency Civilian Associates issuance process:

(1) Sponsor Ensures Need. A CAC will only be issued to an eligible individual based on a clear need by a Coast Guard unit. The unit assigns a Sponsor who takes responsibility for verifying and authorizing the unit organization and applicant's need for a CAC. All applicants for a CAC must be sponsored by a military or civilian Coast Guard employee. Upon determination of the need for a CAC, the Sponsor will review the unit's need for the applicant to perform tasks that require one of the following:

(a) Physical access to multiple Coast Guard facilities or multiple federally controlled facilities on behalf of the Coast Guard on a recurring basis (a minimum of 2 times per week and/or 8 times per month) for a period of 6 months or more.

NOTE: SPOC approval is required for any issuance of less than 6 months.

(b) Remote access, via logon, to Coast Guard network using Coast Guard-approved remote access procedures.

(c) Both physical access to Coast Guard facility and logical access, via logon, to Coast Guard networks on-site or remotely. Access to the Coast Guard network must require the use of a computer with Government-controlled configuration or use of Coast Guard-approved remote access procedure in accordance with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide.

(2) Verify Eligible Sponsored Populations. Sponsors must confirm CAC eligibility based on the Sponsor's determination of the type, level and frequency of access required to Coast Guard facilities or networks that will effectively support the mission.

(3) Investigative Requirements. Initial issuance of a CAC requires a favorably adjudicated Tier 1 investigation (equivalent or higher) or a Tier 1 background investigation (equivalent or higher) package that has been successfully scheduled with the ISP and a FBI fingerprint check with favorable results. The TA and Sponsor or other appropriate Federal Government representative must coordinate with the unit BI Verifier (CSO/TASM) or SECCEN to confirm the appropriate investigation has been favorably adjudicated or scheduled at the ISP with favorable FBI fingerprint results. The applicant will not be approved for CAC issuance until the background investigation requirement has been validated by the BI Verifier (CSO/TASM) or SECCEN. The TA is responsible for confirming that the appropriate background investigation requirement(s) have been met for CAC issuance.

(4) Request CAC via TASS.

(a) The Sponsor identifies a TA to create a TASS application for a CAC on behalf of the Sponsoring unit.

(b) When a TA receives a CAC request they must verify the:

1) Need for a CAC as indicated in Section 10.f.(1) of this Instruction.

2) Non-Federal Agency Civilian Associate applicant has the necessary background investigation as indicated in Section 10.f.(3) of this Instruction and Reference (h) with favorable FBI fingerprint check to be issued a CAC.

(c) Upon confirmation of actions listed in 10.f.(4).(b) above, the TA creates the TASS application.

(d) Specific TASS details that are required for a non-Federal Agency Civilian Associate can be found on the TASS Portal and include:

1) Personnel Category Block: 'Non-Federal Agency Civilian Associate'.

2) Civilian Associate Type: 'National Guard', 'Intergovernmental Personnel Act (IPA)', etc. as appropriate, per Reference (f).

3) Eligibility Expiration Date: end date of assignment not to exceed 3 years.

(e) Once a new TASS application is created, the TA provides the applicant with the TASS URL and a username. The TA must send a temporary password separately. The applicant can then log into TASS to complete and submit the application. Once the TA submits the application, the applicant has 7 days to complete an initial login to TASS and begin the application process, or TASS will automatically disable the application.

(f) Once 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 TA cannot process the application until the applicant submits a complete form. Once the applicant submits a completed application, the system automatically sends an email notification to the TA. The TA has 30 days to approve the application; otherwise, TASS will automatically disable the application. The applicant cannot make changes to a submitted application unless the TA returns the application to the applicant for correction.

(g) The TA must review the applicant's submitted CAC application and approve or reject it. Approved applications will generate an automated email to the applicant's email address saved in TASS. The email contains instructions detailing how the applicant makes an appointment at a RAPIDS site to be issued a CAC. The applicant is required to obtain a CAC from the RAPIDS Issuing Facility within 90 days; otherwise, TASS automatically disables the application.

g. Non-U.S. Citizen Nonappropriated Fund (NAF) Employee. This category is only to be used by the Community Services Command (CSC) when hiring a non-U.S. Citizen employee for the Coast Guard Exchange (CGX), or Morale, Well-Being, and Recreation (MWR) program. TASS allows CSC to track NAF employees who are non-U.S. Citizens using either a Foreign Identification Number (FIN) or an Individual Taxpayer ID Number (ITIN) as the Person Identifiers. Non-U.S. Citizen NAF Employees receive a CAC as their form of Federal Government credential. Non-U.S. Citizen NAF Employee issuance process:

(1) NAF Guidance. Sponsorship and eligibility will be determined by the existing hiring procedures in Reference (l).

NOTE: As a non-U.S. Citizen, a DD Form 1172-2 may be required for DEERS sponsored personnel enrollment.

(2) Investigative Requirements. Initial issuance of a CAC requires a favorably adjudicated Tier 1 investigation (equivalent or higher) or a Tier 1 background investigation (equivalent or higher) package that has been successfully scheduled with the ISP and a FBI fingerprint check with favorable results after employment authorization has been appropriately verified. To meet the investigative requirements for CAC issuance, the non-U.S. Citizen must have

been in the United States or U.S. territory for at least 3 years. The TA and Sponsor or other appropriate Federal Government representative must coordinate with the unit BI Verifier (CSO/TASM) or SECCEN to confirm the appropriate investigation has been favorably adjudicated or scheduled at the ISP with favorable FBI fingerprint results. The applicant will not be approved for CAC issuance until the background investigation requirement has been validated by the BI Verifier (CSO/TASM) or SECCEN. The TA is responsible for confirming that the appropriate background investigation requirement(s) have been met for CAC issuance.

(3) Request CAC via TASS.

(a) The Sponsor identifies a TA to create a TASS application for a CAC on behalf of the CSC.

(b) When a TA receives a CAC request they must verify the non-U.S. Citizen NAF Employee applicant has the necessary background investigation as indicated in Section 10.g.(2) of this Instruction.

(c) Upon confirmation of actions listed in 10.g.(2) above, the TA creates the TASS application.

(d) Specific TASS details that are required for a non-U.S. Citizen NAF Employee include:

1) Personnel Category Block; 'Non-US Non-Appropriated Fund (NAF) Employee'.

2) Personal Identifier; enter Foreign Identification Number (FIN), Individual Taxpayer ID Number (ITIN), or SSN as appropriate.

3) Eligibility Expiration Date; end date of assignment requiring access not to exceed 3 years.

(e) Once a new TASS application is created, the TA provides the applicant with the TASS URL and a username. The TA must send a temporary password separately. The applicant can then log into TASS to complete and submit the application. Once the TA submits the application, the applicant has 7 days to complete an initial login to TASS and begin the application process, or TASS will automatically disable the application.

(f) Once 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 TA cannot process the application until the applicant submits a complete form. Once the applicant submits a completed application, the system automatically sends an email notification to the TA. The TA must approve the application within 30 days; otherwise, TASS will automatically disable the application. The applicant cannot make changes to a submitted application unless the TA returns the application to the applicant for correction

(g) The TA must review the applicant's submission in TASS and will approve or reject it. Approved applications generate an automated email to the applicant's email address saved in TASS. The email contains instructions detailing how the applicant makes an

appointment at a RAPIDS site to be issued a CAC. The applicant is required to obtain a CAC from the RAPIDS Issuing Facility within 90 days; otherwise, TASS automatically disables the application.

h. OCONUS Hire. This category is for non-U.S. Citizens hired under an agreement with the host nation and paid directly by U.S. Forces (direct hire) or paid by an entity other than the U.S. Forces for the benefit of U.S. Forces (indirect hire). Per Reference (m), security must be a major consideration in foreign national employment systems, including provisions for assessing the suitability of potential employees, the unequivocal right to terminate the services of employees considered by the United States or the host nation to be a security risk, and the right to institute higher security measures when the responsible U.S. commander deems it necessary. OCONUS Hire individuals receive a CAC as their form of Federal Government credential. OCONUS Hire issuance process:

(1) Existing Guidance. Sponsorship and eligibility are established by the existing hiring procedures in References (m) and (n), detailing instructions for employment of an OCONUS hired non-U.S. Citizens.

NOTE: As a non-U.S. Citizen, a DD Form 1172-2 may be required for DEERS sponsored personnel enrollment.

(2) Investigative Requirements. Coast Guard units will likely fall under a DoD host command with existing international agreements and established joint committees directing procedures for hiring OCONUS local non-U.S. Citizens. Coast Guard units will follow host command procedures. Per Reference (n), special considerations apply for the investigative requirements for the utilization of Local National (LN) personnel by the United States Forces, Japan.

NOTE: If there are no local procedures for investigating non-U.S. Citizens at the OCONUS location, contact Coast Guard SPOC and TASS Support Team at: HQS-SMB-TASSProgram@uscg.mil for guidance and assistance.

(3) Request CAC via TASS.

(a) The Sponsor identifies a TA to create a TASS application for a CAC on behalf of the Command.

(b) When a TA receives a CAC request they must verify the OCONUS Hire employee applicant has the necessary background investigation as indicated in Section 10.h.(2) of this Instruction.

(c) Upon confirmation of actions listed in 10.h. (3).(b) above, the TA creates the TASS application.

(d) Specific TASS details that are required for a OCONUS Hire employee can be found on the TASS Portal and include:

1) Personnel Category Block; ‘OCONUS Hire’.

2) Personal Identifier; enter Foreign Identification Number (FIN), Individual Taxpayer ID Number (ITIN), or SSN as appropriate.

3) Eligibility Expiration Date: end date of assignment not exceed 3 years.

(e) Once a new TASS application is created, the TA provides the applicant with the TASS URL and a username. The TA must send a temporary password separately. The applicant can then log in to TASS to complete and submit the application. Once the TA submits the application, the applicant has 7 days to complete an initial login to TASS and begin the application process, or TASS will automatically disable the application.

(f) Once 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 TA cannot process the application until the applicant submits a complete form. Once the applicant submits a completed application, the system automatically sends an email notification to the TA. The TA has 30 days to approve the application; otherwise, TASS will automatically disable the application. The applicant cannot make changes to a submitted application unless the TA returns the application to the applicant for correction.

(g) The TA must review the applicant's submitted CAC application and approve or reject it. Approved applications will generate an automated email to the applicant's email address saved in TASS. The email contains instructions detailing how the applicant makes an appointment at a RAPIDS site to be issued a CAC. The applicant is required to obtain a CAC from the RAPIDS Issuing Facility within 90 days; otherwise, TASS automatically disables the application.

i. Other Federal Agency Contractors. Other Federal Agency Contractors (E.g. DHS Contractors) receive a CAC as their form of Federal Government access credential. Other Federal Agency Contractor issuance process:

(1) Sponsor Ensures Need. A CAC will only be issued to an eligible Other Federal Agency Contractors based on a clear need by a Coast Guard unit. The unit assigns a Sponsor who takes responsibility for verifying and authorizing the unit organization and applicant's need for a CAC. All applicants for a CAC must be sponsored by a military or civilian Coast Guard employee. Upon determination of the need for a CAC in situations such as a DHS Contractor having continual assignments working on a Coast Guard facility; the Sponsor must review the unit's need for the applicant to perform tasks that require one of the following:

(a) Physical access to multiple Coast Guard facilities or multiple federally controlled facilities on behalf of the Coast Guard on a recurring basis (a minimum of 2 times per week and/or 8 times per month) for a period of 6 months or more.

NOTE: SPOC approval is required for any issuance of less than 6 months.

(b) Remote access, via logon, to Coast Guard network using Coast Guard-approved remote access procedures.

(c) Both physical access to Coast Guard facility and logical access, via logon, to Coast Guard networks on-site or remotely. Access to the Coast Guard network must require the use of a computer with Government-controlled configuration or use of Coast Guard-approved remote access procedure in accordance with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide.

(2) Verify Eligible Sponsored Populations. Sponsors must confirm CAC eligibility based on the Sponsor's determination of the type, level and frequency of access required to Coast Guard facilities or networks that will effectively support the mission.

(3) Investigative Requirements. Initial issuance of a CAC requires a favorably adjudicated Tier 1 investigation (equivalent or higher) or a Tier 1 background investigation (equivalent or higher) package that has been successfully scheduled with the ISP and a FBI fingerprint check with favorable results. The TA and Sponsor or other appropriate Federal Government representative must coordinate with the unit BI Verifier (CSO/TASM) or SECCEN to confirm the appropriate investigation has been favorably adjudicated or scheduled at the ISP with favorable FBI fingerprint results. The applicant will not be approved for CAC issuance until the background investigation requirement has been validated by the BI Verifier (CSO/TASM) or SECCEN. The TA is responsible for confirming that the appropriate background investigation requirement(s) have been met for CAC issuance.

(4) Request CAC via TASS.

(a) The Sponsor identifies a TA to create a TASS application for a CAC on behalf of the Sponsoring unit.

(b) When a TA receives a CAC request they must verify:

1) Need for a CAC as indicated in Section 10.i.(1) of this Instruction.

2) Other Federal Agency Contractors applicant has the necessary background investigation as indicated in Section 10.i.(3) of this Instruction.

(c) Upon confirmation of actions listed in 10.i.(4).(b) above, the TA creates the TASS application.

(d) Specific TASS details required for an Other Federal Agency Contractor include:

1) Personnel Category Block; 'Other Federal Agency Contractors'.

2) Government Agencies; select appropriate Agency, per Reference (f).

3) Eligibility Expiration Date; expected end date of work with Coast Guard, not to exceed 3years.

(e) Once a new TASS application is created, the TA provides the applicant with the TASS URL and a username. The TA must send a temporary password separately. The applicant can then log in to TASS to complete and submit the application. Once the TA

submits the application, the applicant has 7 days to complete an initial login to TASS and begin the application process, or TASS will automatically disable the application.

(f) Once 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 TA cannot process the application until the applicant submits a complete form. Once the applicant submits a completed application, the system automatically sends an email notification to the TA. The TA has 30 days to approve the application; otherwise, TASS will automatically disable the application. The applicant cannot make changes to a submitted application unless the TA returns the application to the applicant for correction.

(g) The TA must review the applicant's submitted CAC application and approve or reject it. Approved applications will generate an automated email to the applicant's email address saved in TASS. The email contains instructions detailing how the applicant makes an appointment at a RAPIDS site to be issued a CAC. The applicant is required to obtain a CAC from the RAPIDS Issuing Facility within 90 days; otherwise, TASS automatically disables the application.

11. REGULATED LOGICAL/COMPUTER ACCESS. This Instruction does not govern the management, accountability, access approvals, user level access credentials, user accounts or access to any CG Information Technology (IT) systems, Computers, or Network Systems. For logical IT guidance, see Reference (j).

12. REVERIFICATION PROCEDURES.

    a. Every 6 months (180 days), the TA must coordinate with the Sponsor/COR to verify the cardholder's continued affiliation with Coast Guard as described in this Instruction.

    b. The TA will receive confirmation from the Sponsor/COR verifying the cardholder's continued need of the Federal Government credential.

    c. The TA will re-verify the cardholder in TASS upon receipt from the Sponsor/COR confirming continued need of the Federal Government credential.

13. LOST, TERMINATION, AND REVOCATION PROCEDURES.

    a. In the event of a damaged, lost, compromised, or stolen Federal Government credential, the Sponsor will complete a memorandum highlighting the details of the event. Per Reference (b), this memorandum will be presented to the RAPIDS Site to obtain a new Federal Government credential.

    b. A Sponsor must notify the applicable TA within one business day when a cardholder's affiliation with the Coast Guard is terminated prior to the Federal Government credential expiration.

    c. The TA or TASM must contact their cognizant CSO and Security Manager immediately when a cardholder's affiliation with the Coast Guard is terminated due to derogatory circumstances and the Federal Government credential is not immediately retrieved.

d. The Sponsor, TA, COR, or TASM will turn in any compromised, recovered, retrieved, mutilated, damaged terminated, revoked, and/or outdated Federal Government credentials received to the nearest RAPIDS Site.

e. Coast Guard security guards, watch standers, and RAPIDS operators are authorized to seize compromised, mutilated, inactive, damaged, expired, or stolen Federal Government credentials. If the Federal Government credential is not considered evidence, it will be turned in to the RAPIDS Site.

f. If for any reason, a cardholder no longer requires access to Coast Guard facilities and/or information systems, the TA must perform the revocation process within TASS IAW Reference (g) and have the card collected by the Sponsor, TA, or COR within one business day. The Sponsor, TA, or COR must submit a CGFIXIT ticket to revoke access to their CGONE account and removal from all CGIT systems. If the unit utilizes any an Electronic Physical Access Control System (EPACS), the Sponsor, TA, or COR must notify the System Administrator/CSO to remove the card's access within one business day. The following are some causes for termination/revocation and retrieving Federal Government credentials:

(1) Card expiration.

(2) Cardholder no longer meets the background investigation eligibility requirements.

(3) Card or Contract expiration and/or option period not exercised.

(4) Auxiliarist duties reassigned to another individual or responsibility no longer needed.

(5) Contract/Contractor termination/transfer/removed by the Federal Government/vendor.

(6) Summer internship ends.

(7) Federal Government course ends (applies mostly to Foreign Affiliates).

(8) Arrest or disciplinary action.

g. The Sponsor and TA must coordinate with the sponsored cardholder to facilitate and ensure the return of expired/revoked Federal Government credential. The Sponsor must document the final disposition of the Federal Government credential. The Sponsor/COR must notify the TA of any collected Federal Government credentials. The Sponsor/COR must notify the TA within one business day of any uncollected Federal Government credentials. If the cardholder's Supervisor or Sponsor/COR turn the card into RAPIDS, they must send an email notification to the assigned TA within two business days. TA must receive an email from the Sponsor within two days detailing the final status of CAC to ensure its proper disposition.

h. Once a Federal Government credential is collected by the TA or Sponsor, it must be returned the nearest RAPIDS site within two business days for termination within DEERS, revoking PKI certificates/infrastructures, and final disposition. Nearest RAPIDS locations can be found at: https://www.dmdc.osd.mil/rsl/appj/site.

14. ACCOUNT TRANSFERS. A TASM can transfer applicant accounts between TA(s) at their assigned site. A SPOC can transfer applicant accounts between TA(s) for any site within their assigned service or agency. Account custodian responsibilities may need to be transferred to another TA due to:

    a. Situations wherein an applicant moves job assignments within the Agency.

    b. Instances where the TA has an unmanageable number of applicants (over 100) accounts, a prolonged sickness, or any reason they can no longer perform TA functions.

15. INTERNAL CONTROLS.

    a. Coast Guard TASS SPOC(s) will:

        (1) Perform monthly audits of at least 10% of all TASS issued cards to verify Personnel Category Descriptions are entered correctly into TASS. This monthly audit will also ensure TA(s) and TASM(s) do not exceed account management capacities per Sections 9.e.(9) and 9.f.(11) of this Instruction.

        (2) Conduct Annual TASS Site Assessments to evaluate compliance with current TASS policies and directives. An individualized site assessment report will be sent to each assigned TASM for review and comment.

        (3) Conduct TASM Quarterly Teleconference Call Meetings to relay system and training updates, important TASS announcements, and support information. TASMs to share feedback, experiences and recommendations on TASS related issues from the TAs and applicants in the field.

        (4) Conduct Quarterly Beginner, Intermediate/Advanced CG-Specific TASS Training available on the Coast Guard TASS Portal at: https://cg.portal.uscg.mil/units/dcms34/tass/Pages/Reference-Documents.aspx.

        (5) Conduct no-notice evaluations of TASS sites to ensure TASMs and TAs perform their duties IAW this Instruction.

16. FORMS/REPORTS. None.

17. REQUEST FOR CHANGES. Units and individuals may recommend changes via the chain of command to: HQS-DG-lst-DCMS-34@uscg.mil.

M. F. MCALLISTER /s/
Vice Admiral, U.S. Coast Guard
Deputy Commandant for Mission Support