EMAIL FORM

Date:

CONTRACTOR APPLICATION FOR A COMMON ACCESS CARD (CAC)

PRIVACY ACT STATEMENT

AUTHORITY: Authority: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136 Under Secretary of Defense for Personnel Readiness; DoD Directive 1341.1, Defense Enrollment/Eligibility Reporting System; SORN DMDC 02 DoD and E.O. 9397 (SSN).

PURPOSE: The purpose of the system is to provide a database for determining eligibility to DoD entitlements and privileges; to support DoD health care management programs; to provide identification of deceased members; to record the issuance of DoD badges and identification cards, i.e. Common Access Cards (CAC) or beneficiary cards; and to detect fraud and abuse of the benefit programs by claimants and providers to include appropriate collection actions arising out of any debts incurred as a consequence of such programs. To authenticate and identify DoD affiliated personnel (e.g., contractors); to assess manpower, support personnel and readiness functions; to perform statistical analyses; identify current DoD civilian and military personnel for purposes of detecting fraud and abuse of benefit programs; to register current DoD civilian and military personnel and their authorized dependents for purposes of obtaining medical examination, treatment or other benefits to which they are entitled; to ensure benefit eligibility is retained after separation from the military; information will be used by agency officials and employees, or authorized contractors, and other DoD Components for personnel and manpower studies; and to assist in recruiting prior-service personnel.

ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To Federal agencies and/or their contractors, in response to their requests, for purposes of authenticating the identity of individuals who, incident to the conduct of official business, present the Common Access Card or similar identification as proof of identity to gain physical or logical access to government and contractor facilities, locations, networks, or systems. The DoD 'Blanket Routine Uses' set forth at the beginning of the DoD compilation of systems of records notices apply to this system.

DISCLOSURE: Disclosure of requested information is voluntary, however, failure to provide such information may result in a delay of your access to DoD facilities and networks.

APPLICANT INFORMATION

LEGAL LAST NAME	LEGAL FIRST NAME	LEGAL MIDDLE NAME	SUFFIX (Sr., Jr., IV, Etc.)

EMAIL ADDRESS (Must be employer or .mil; cannot be personal - gmail, yahoo, Etc.)	SOCIAL SECURITY NUMBER (No dashes)

DATE OF BIRTH	TELEPHONE	CAC DETAILS

EMPLOYER INFORMATION

EMPLOYER COMPANY NAME

FACILITY SECURITY OFFICER (FSO) (Last name, First, MI)	FSO TELEPHONE

CONTRACT INFORMATION

CONTRACT NUMBER	CONTRACT END DATE

COMPETENCY SUPPORTED	TIER 3 OR ABOVE PHONE

REASON CAC NEEDED ☐ Multiple DoD Installations Access ☐ DoD IT Networks ☐ Overseas

LIST DoD INSTALLATIONS (Minimum of two required - SSC Atlantic, SSC Pacific, etc.)

APPROVALS

Employer FSO signature certifies that the information provided on this form is true and accurate for the above applicant.

EMPLOYER FSO (Printed name)	DATE	SIGNATURE

SSC Atlantic Tier 3 or above signature certifies that the above applicant, based on personal knowledge and available documentation, is in a status eligible for a CAC and requires a CAC in the performance of his/her duties with the Uniformed Services.

SPAWAR ID SAAR-N Approval Date IA Training Completion Date

TIER 3 OR ABOVE (Printed name)	DATE	SIGNATURE

INSTRUCTIONS AND NON-DISCLOSURE AGREEMENT

Before starting the CAC process:
ALL CONTRACTORS MUST HAVE A SPAWARSYSCENLANT 5230/8 AND AN OPNAV Form 5239/14 SUBMITTED AND APPROVED PRIOR TO FILLING OUT THIS CAC APPLICATION. (Processing these forms generates the SPAWAR ID, SAAR-N date, and the IA training date required on this application.) Contractors must check with their company Facility Security Officer (FSO) to see if they meet all requirements to obtain a Common Access Card (CAC). IN ACCORDANCE WITH SSC ATLANTIC POLICY: ISSUANCE OF A CAC REQUIRES, AT A MINIMUM, COMPLETION OF AN FBI FINGERPRINT CHECK WITH FAVORABLE RESULTS AND SUBMISSION OF A NACLC (NATIONAL AGENCY CHECK WITH LOCAL AGENCY AND CREDIT CHECK) TO THE OFFICE OF PERSONNEL MANAGEMENT(OPM), OR A DOD-DETERMINED EQUIVALENT INVESTIGATION (DTM-08-003).

Submitting this form:
Complete your information and obtain signatures from your Employer Facility Security Office (FSO) and from a SSC Atlantic Tier 3 or above. Please type or print neatly.

Submit your application to the Trusted Agent (TA) Office **ONLY ONCE** via one of the following methods:
- Faxing it to 843-218-4188; OR
- Hand carrying it to the TA Office located in Building T-1 next to the CAC Office; OR
- **Emailing it via encrypted email to**: ssclant_cacappl.fcm@navy.mil

IMPORTANT: Because of the personally identifiable information (PII) on the form, all CAC applications sent via email must be encrypted.

After submitting your application to the Trusted Agent (TA) Office: Wait for an email from the TA that will contain further instructions, along with a user ID and password that you will use to access the Trusted Associate Sponsorship System (TASS).

Once you receive this information, fill out the application online in TASS, ensure that you submit for approval and click the Confirm button so that your TASS application will go back to the TA for approval.

Do not make a CAC appointment until you complete the CAC process online in TASS AND receive your automated approval email message from TASS.

Feel free to contact the Trusted Agent Office at 843-218-5948 with additional questions.

NON-DISCLOSURE AGREEMENT
I understand that I may receive or have access to information, including information maintained in various Government information systems and secure websites (e.g. Navy Enterprise Resource Planning (N-ERP), Electronic Document Access (EDA), Wide Area Workflow (WAWF)). Accessed information may include “sensitive information” or other information not previously made available to the public that cannot be disclosed.

As used in this Agreement, "sensitive information" includes:
- All types and forms of confidential business information, including financial information relating to a contractor's pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;
- Source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 423);
- Information marked as "business confidential, proprietary, procurement sensitive, source selection sensitive," or other similar markings;
- Other information designated as sensitive by SSC LANT.

SSC LANT recognizes its obligation to protect contractors and their subcontractors from potential competitive harm that could result from the disclosure of sensitive information. SSC LANT's policy is to permit access to information only where such information is required by SSC LANT contractors and their subcontractors in the performance of the contract/task order, and is restricted to those individuals requiring access in the performance of the contract/task order (i.e., "need to know").

In accordance with the above policy, I agree to:
- Utilize accessed information only to perform the services as required by the contract/task order and not for any other purpose unless authorized, and to assume only those user roles and privileges for which I am authorized;
- Safeguard accessed information from unauthorized use and disclosure, providing the same level of protection that would be provided by SSC LANT employees, and exercising the same reasonable degree of care that would normally be used to protect a contractor's own confidential business information;
- Not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract/task order or as authorized by Federal statute, law, or regulation;
- Immediately notify the authorized company representative in the event that I inadvertently access any information marked as “proprietary,” “procurement sensitive,” or “source selection sensitive,” or that, even if not properly marked otherwise indicates I may not be authorized to access the information, and refrain from any further access until authorized in writing (via letter or email) by the Contracting Officer; and
- Report any violations of this Agreement to the authorized company representative as soon as the violation is identified.