



Defense Manpower Data Center (DMDC)

Trusted Associate Sponsorship System (TASS)

Trusted Agent User Guide (TASS TASM/TA User Guide)

Version 4.00
March 2013

Prepared by:
The Defense Manpower Data Center

Document History

Version	Date	Comments
0.1	12/18/02	Origin
1.0	01/31/03	Revision
1.1	03/04/03	Revision
1.2	05/09/03	Revision, incorporating Navy comments
1.3	08/6/03	Revision, incorporating comments by W. Shaffer
1.4	09/23/04	Revision, reflecting upgrade
1.5	05/13/05	Revision, addition of Contractor reverification notification content. Addition of modified page for TA Change Contact Information page.
1.6	12/10/05	New Section 3 added
1.7	11/17/06	Revision incorporates changes made for version 2.0
1.8	02/24/07	Revision incorporates changes made for version 2.02
1.9	07/10/07	Revision incorporates changes made for version 2.03
1.9.2	08/31/07	Revision of security content; changes made 10/25/07
2.0	12/02/08	Revision incorporating changes from 2.03 through 3.0
2.0.1	03/30/09	Revision incorporating edits
3.03	04/05/10	Revised guide for TASMs and TAs with updates inclusive of version 3.03
3.03	06/07/10	Updated section 3.6.1
3.03	07/08/10	Updated section 3.4
3.06	04/15/11	Revised with updates inclusive of version 3.06
4.00	06/26/12	Revision of new name and updates inclusive of version 3.08 and the 4.00 CVS name change to TASS
4.00	03/21/13	Revision for updates inclusive of version 4.00

Table of Contents

1	Introduction	10
1.1	Overview of Changes	10
1.2	Purpose of TASS	11
1.3	CAC Program Background	11
2	TASS Roles and Responsibilities	13
2.1	Participating Organizations	13
2.2	Defense Manpower Data Center (DMDC)	13
2.3	Service or Agency Point of Contact (SPOC)	13
2.3.1	SPOC Responsibilities	13
2.3.2	SPOC Requirements.....	14
2.4	Trusted Agent Security Manager (TASM).....	15
2.4.1	TASM Responsibilities	15
2.4.2	TASM Requirements.....	15
2.5	Trusted Agent (TA)	16
2.5.1	TA Responsibilities	16
2.5.2	TA Requirements.....	16
3	TASS Business Process Overview	18
3.1	Site Creation and TASM Registration	18
3.2	TA Registration	18
3.3	TASM/TA TASS Training.....	19
3.4	TA Submission of Application	20
3.5	Applicant Login	21
3.6	Verification.....	22
3.6.1	Letter of Authorization	22
3.6.2	Status-of-Forces Agreement.....	22
3.7	Card Issuance	23
3.8	DEERS Updates	23
3.9	Applicant Reverification	23
3.10	Eligibility Expiration	23
3.11	Applicant Revocation	24
3.12	TA Sponsorship Transfer.....	24
4	Timeline to Complete Key TASS Procedures	25
5	Definition of Terms	27

5.1	Navigational References	27
5.2	Figure Usage	27
6	TASM User Guide	28
6.1	Site Registration	28
6.1.1	Site Definition	28
6.1.2	SPOC Requests to DEERS	28
6.1.3	DEERS Turnaround	28
6.1.4	Site ID Notification	29
6.2	TASM Registration	29
6.2.1	TASM Registration Request	29
6.2.2	SPOC Request to DEERS.....	29
6.2.3	DEERS Turnaround	29
6.2.4	TASM Registration Notification	30
6.2.5	Updating TASM Information	30
6.2.6	Criteria and Procedures for TASM Removal	30
6.3	TA Registration.....	31
6.3.1	TA Identification and Qualifications	31
6.3.2	TA Registration Process.....	32
6.3.3	Updating TA Information.....	32
6.3.4	Criteria and Actions for TA Removal	32
6.4	Logging in as a TASM.....	33
6.4.1	Prerequisites.....	33
6.4.2	CAC Login.....	33
6.4.3	Login Failure.....	36
6.5	TASM Homepage	37
6.6	Changing a TASM User Profile.....	38
6.6.1	Changing TASM Contact Information	39
6.7	Creating a Trusted Agent Account	41
6.7.1	Prerequisites.....	41
6.7.2	Creating a New TA Account	42
6.8	Managing TA Accounts	45
6.8.1	Viewing Trusted Agents	45
6.8.2	Browse Applicants Screen.....	47
6.8.3	Reassigning Applicants	49
6.8.4	Reassigning CAC Holders to a New TA	50

7	TA User Guide.....	53
7.1	Logging in as a TA	53
7.1.1	Prerequisites.....	53
7.1.2	CAC Login.....	53
7.1.3	Login Failure.....	56
7.2	TA Homepage	57
7.3	Updating Your TA Profile.....	59
7.3.1	Changing TA Contact Information	59
7.4	Creating a New Application	61
7.4.1	Prerequisites.....	61
7.4.2	Creating an Application	62
7.5	Reusing an Existing Application to Create a New Application.....	69
7.5.1	Prerequisites.....	69
7.5.2	Reusing an Application.....	70
7.6	Browsing Applications	74
7.6.1	Searching for an Application.....	74
7.6.2	Viewing an Application	76
7.6.3	Comparing an Application with DEERS.....	78
7.7	Maintaining an Application.....	79
7.7.1	Approving an Application.....	79
7.7.2	Returning an Application	84
7.7.3	Rejecting an Application.....	86
7.7.4	Disabling an Application	87
7.7.5	Reusing an Application.....	88
7.7.6	Resetting an Applicant Password.....	88
7.8	Maintaining a CAC	90
7.8.1	Searching for a CAC	90
7.8.2	Reverifying a CAC	92
7.8.3	Revoking a CAC	95
7.9	High Volume Data Feed	98
7.9.1	Prerequisites.....	98
7.9.2	Submitting Multiple Applications Using High Volume Data Feed.....	98
7.9.3	Searching for a Batch Processing Transaction History.....	105
8	TASS Application Features.....	108
8.1	Quick Links.....	108

8.1.1	Forms.....	108
8.1.2	Policies.....	109
8.1.3	Training-Courseware.....	110
8.1.4	System Requirements.....	112
8.2	Additional TASS Application Functions	113
8.2.1	Print	113
8.2.2	Per Page Display	114
8.2.3	Page Number, Next, and Last.....	115
8.3	Help	115
8.4	Frequently Asked Questions (FAQs).....	116
8.5	Contact Us.....	116
8.6	DoD Policy.....	116
8.7	Log Off	119
Appendix A	DD Form 2875 System Authorization Access Request (SAAR)	121
Appendix B	DD Form 2875 Instructions	123
Appendix C	DD Form 1172-2	124
Appendix D	DD Form 1172-2 Instructions.....	125
Appendix E	TASS Email Notifications.....	136
I.	Schedule for Contractor Reverification Notifications	136
II.	Batch Upload Success Notification	137
Appendix F	Acronyms, Abbreviations, and Terms.....	138
Appendix G	Alphanumeric Character Translations.....	140
Appendix H	Documentation for DEERS Data Changes.....	142
I.	DSO Name Correction Request Form.....	142
II.	DSO DOB Correction Request Form.....	143
III.	DSO Person Identifier Correction Request Form.....	144

Table of Figures

Figure 1.	Navigational Layout	27
Figure 7.	Login—Select Role Screen	36
Figure 8.	Login Screen—Login Failure	37
Figure 9.	TASM Homepage	38
Figure 10.	TASM Profile Screen	39
Figure 11.	TASM Edit Contact Info Screen	40
Figure 12.	RSS Portal Actions	41
Figure 13.	DEERS Security Online Registered User Log In Screen	42
Figure 14.	DEERS Security Online Welcome To Site Security Manager Screen	43
Figure 15.	DEERS Security Online Enter Person ID Screen	43
Figure 16.	DEERS Security Online Add Site User Screen	44
Figure 17.	DEERS Security Online Update Site User Detail Screen	45
Figure 18.	View Trusted Agents Screen	46
Figure 19.	View Trusted Agents Screen—Search Results	47
Figure 20.	Browse Applicants Screen	48
Figure 21.	Browse Applicants Screen—Search Results	49
Figure 22.	View/Reassign Applications Screen	50
Figure 23.	View/Reassign CACs Screen	51
Figure 24.	TASM View Application Screen	52
Figure 30.	Login—Select Role Screen	56
Figure 31.	Login Screen—Login Failure	57
Figure 32.	TA Homepage	58
Figure 33.	TA Profile Screen	59
Figure 34.	TA Edit Contact Info Screen	60
Figure 35.	RSS Portal Actions	61
Figure 36.	Example of TASS/PIV Verification Warning Notice	62
Figure 37.	Create New Application Account Screen	63
Figure 38.	Create New Application Account—Confirm Screen	67
Figure 39.	Create New Application Account—Success Screen	68
Figure 40.	Create Account Failure	69
Figure 41.	Browse Applications Screen—Search Results	71
Figure 42.	Reuse Old Record to Create New Application Screen	71
Figure 43.	Reuse Old Record to Create New Application—Confirm Screen	72

Figure 44. Reuse Old Record to Create New Application—Success Screen	73
Figure 45. Browse Applications Screen	74
Figure 46. Browse Applications Screen—Search Results	75
Figure 47. View Application Screen	77
Figure 48. Compare to DEERS Screen	78
Figure 49. Button Row—Submitted Application	79
Figure 50. Browse Applications Screen—Submitted Applications	80
Figure 51. Confirm Application Approval	81
Figure 52. Application Approval Status Screen	82
Figure 53. Email to Applicant Following Approval	82
Figure 54. Browse Applications Screen—Submitted Applications	84
Figure 55. Application View/Maintenance Screen	85
Figure 56. Return Application Screen.....	86
Figure 57. Reject Application Screen	87
Figure 58. Disable Application Message	88
Figure 59. Disable Application Screen	88
Figure 60. Application View Maintenance Screen—Resetting a Password.....	89
Figure 61. Reset Password for Applicant Screen	89
Figure 62. Successful Reset of Applicant Password	90
Figure 63. Browse CACs Screen	91
Figure 64. Browse CACs Screen—Search Results	92
Figure 65. Browse Reverifications Screen	93
Figure 66. Reverification Screen—View Applicants	94
Figure 67. Reverifications Screen—After Applicant Reverification	95
Figure 68. Confirm Revoke Request Message	96
Figure 69. Reverifications Screen—Revoked CAC	96
Figure 70. Browse Applications Screen	99
Figure 71. High Volume Applications Data Uploading Screen	99
Figure 72. High Volume Data Uploading—CC Notification Section	100
Figure 73. XML Schema Screen	101
Figure 74. Choose File Screen	102
Figure 75. High Volume Applications Data Uploading Screen—Ready to Upload.....	102
Figure 76. .xml File Must Be Selected Error Message	103
Figure 77. High Volume Applications Data Uploading—Processing Upload	103
Figure 78. Monitor Batch Processing Screen	104

Figure 79. Batch Processing Screen—Transaction History	104
Figure 80. High Volume Applications Data Uploading Screen—Error	105
Figure 81. Batch Processing Screen—Transaction History	106
Figure 82. Batch Processing—Transaction History Search Criteria	106
Figure 83. Batch Processing—Transaction History Search Results	107
Figure 84. Quick Links Menu	108
Figure 85. Forms Screen.....	109
Figure 86. Policies Screen.....	110
Figure 87. Training-Courseware	111
Figure 88. System Requirements Screen	113
Figure 89. Print Icon.....	113
Figure 90. Print Screen	114
Figure 91. Per Page Display Drop-Down Menu	114
Figure 92. Page Number, Next, and Last Links	115
Figure 93. Help Screen	116
Figure 94. Agency Disclosure Notice/Privacy Statement/Warning Notice Links	117
Figure 95. Agency Disclosure Notice Screen.....	117
Figure 96. Privacy Act Statement Screen	118
Figure 97. Warning Notice and Consent to Monitor Screen	118
Figure 98. Log Off Successful Screen.....	119
Figure 99. Confirmation Message to Close Browser Window	119

1 Introduction

This section provides an overview of the changes to the Trusted Associate Sponsorship System (TASS) application inclusive of version 4.00 and discusses the purpose and background of the Common Access Card (CAC) program.

1.1 Overview of Changes

This section describes the functional changes to versions 3.09 and 4.00 of the TASS application. The following list provides the new application elements and functionality for the TASM and TA roles within TASS:

- **TASM, TA and Applicant various label changes:** Various label changes made to the TASS application and application display screens.
- **TA new and updated Personnel Categories:** TASS has expanded Personnel Categories and corresponding drop-down menus for better identification of an Applicant's affiliation and access requirements.
 - *OCONUS Local Hire* and *Foreign Affiliate* are new Personnel Categories.
 - *Presidential Appointee* has been removed from the list of Personnel Categories.
 - The *Affiliated Volunteers* Personnel Category has six new sub-categories: American Red Cross Volunteer, Education, Family Support, Legal Assistance, Religious, and Student Intern
 - The *DoD and Uniform Services Contract Employee* Personnel Category has a new sub-category for Federally Funded Research and Development Center (FFRDC) employees.
- **High Volume Data Feed (HVDF) or Batch Upload process updated:** The Batch Upload process has been updated to allow for *OCONUS Local Hire* and *Foreign Affiliate* personnel categories to be utilized. Additionally, the HVDF now has a vetting checkbox for TAs to verify the vetting of batch processed applicants.
- **DD Form 1172-2 updated:** The DD Form 1172-2 has been updated as of April 2012.
- **RAPIDS Self Service (RSS) application:** TASS will offer TAs, TASMs and SPOCs an option of changing contact and email information at a RAPIDS facility or through the new RAPIDS Self Service application.

- **CAC Login screen and Consent to Monitor notification updated:** The CAC Login screen has been updated and the Consent to Monitor notification now appears on a separate screen.

TA, TASM, and SPOC password screen removed: TAs, TASMs, and SPOCs can only log in using their CAC. All password screen references for TAs, TASMs and SPOCs have been removed.
- **TASM Manage TAs tab updated:** The TASMs *Manage TAs* tab now has two tabs (**By TASM/TA** and **By Applicant**) in the second row navigation bar. The **By TASM/TA** navigation tab opens the *View Trusted Agents* search screen and allows you to run a query for records by the TASM or TA's last name, role, or status. The added **By Applicant** navigation tab opens the *Browse Applicants* search screen which allows you to run a query for records by an Applicant's person ID, last name, first name, or contract number.
- **Contract number verification:** TASS now verifies contract numbers through Personal Identification Verification System (PIVS).
- **TASS record archival:** TASS has been modified to archive old records and will allow TAs and TASMs to conduct a search for archived records.
- **New TASS System Requirements:** TASS system requirements have been updated.

Section 6 (TASM User Guide) and **Section 7 (TA User Guide)** describe these changes or new capabilities in more detail.

1.2 Purpose of TASS

The TASS application, initially designed in 2003 as the Contractor Verification System (CVS), was designed to replace the paper application process using DD Form 1172-2, *Application for Department of Defense (DoD) CAC Defense Enrollment Eligibility Reporting System (DEERS) Enrollment*. See **Appendix C** and **Appendix D**, respectively, for copies of DD Form 1172-2 and instructions. As a web-based system, TASS allows Affiliated Volunteers (requiring DoD Network access), DoD and Uniformed Service Contractors, Foreign Affiliates, Non-DoD Civil Service Employees, Non-Federal Agency Civilian Associates, Non-US Non-Appropriated Fund (NAF) Employees, OCONUS Hires, Other Federal Agency Contractors to apply for a Common Access Card (CAC) or other government credential electronically through the Internet. Government sponsors approve the applications to receive government credentials.

1.3 CAC Program Background

The DoD began issuing advanced identification (ID) cards for Active Duty Military, Selected Reserves, DoD civilians, and “inside the wall” Contractors in October 2000. The new CAC is a personalized “Smart Card”—a plastic card the size of a credit card with an

embedded integrated circuit chip (ICC) for storing and processing data. Incorporated with public key infrastructure (PKI) security, the CAC consolidates multiple credentials and data and may be used for various applications, including network security and secure email communication.

TASS also supports other types of government credentials such as the Volunteer Logical Access credential and the Uniformed Services ID (USID) card.

The original CAC featured 32 kilobytes of Electronically Erasable Programmable Read-Only Memory (EEPROM) and supported on-card secure cryptographic functions, including key generation encryption and digital signing. With PKI, data encrypted with the public key may be decrypted only with the private key. The ICC contains protected data about the cardholder (including personal identification number [PIN]), personal demographics, benefits, digital certificates, and card management and security applets. Four unique digital certificates stored on the chip allow the cardholder to digitally sign documents, encrypt data for transmission or storage, and establish secure web sessions to access and update information via the Internet.

The new version of the CAC is equipped with 144 kilobytes of EEPROM. The increased memory provides for the creation of more complex and functional applets in support of business processes.

The Defense Manpower Data Center (DMDC) Identity Services Division and Identity Programs Branch Program Management and Development organizations sponsor the CAC program.

2 TASS Roles and Responsibilities

This section describes each of the roles within TASS and discusses the responsibilities of the individuals assigned to each role.

2.1 Participating Organizations

Since the release of TASS version 2.0, organizations seeking to use TASS no longer need to submit a Memorandum of Agreement (MOA) to implement TASS service. The TASS application has become a DoD application and no longer requires every entity to possess an individual MOA with DMDC.

2.2 Defense Manpower Data Center (DMDC)

DMDC, as the administrator of DEERS and Real-Time Automated Personnel Identification System (RAPIDS), operates and maintains the TASS infrastructure.

2.3 Service or Agency Point of Contact (SPOC)

SPOCs handle the day-to-day TASS management and operation. SPOCs perform the following tasks:

- Manage TASS for their service or agency
- Coordinate with DMDC
- Establish sites with TASS capability, oversee TASM registration, and ensure the maintenance of other required field support

2.3.1 SPOC Responsibilities

An SPOC has the following responsibilities:

- Meet SPOC position requirements as specified in **Section 2.3.2 (SPOC Requirements)**
- Administer the TASS program within his or her service or agency, including establishing and updating site ID numbers and TASM accounts
- Coordinate requests for new or additional TASS capabilities between his or her service or agency and DMDC
- Work with the DMDC Security Team (DST) to register and revoke site IDs and TASMs, and ensure the currency of site and TASM information
- Ensure that TASS TASMs and TAs complete all required TASS training, including both the TASS Certification Web-based Training (WBT) and the TASS training specified by the service or agency

- Transfer Applicants from an existing TASM/TA to another TASM/TA within the TASS application for his or her associated service or agency
- Create policies, operating procedures, and other supporting documentation in support of service- or agency-specific implementation
- Manage and oversee an internal Management Service that includes the following:
 - The service or agency TASS program
 - All responsible TASS sites
 - All responsible TASM accounts
 - Contact information for all TASM and TA personnel
- Ensure assigned TASM and TA personnel have met all requirements for their roles; see **Section 2.4.2 (TASM Requirements)** and **Section 2.5.2 (TA Requirements)**
- Provide documented policies and guidelines for assigned TASMs to provide training on how TAs are to complete and maintain the sponsorship process and their responsibilities

2.3.2 SPOC Requirements

The TASS SPOC must meet the following requirements:

- Be a U.S. citizen
- Be a DoD uniformed service member, DoD civilian, or Contractor working for the service or agency
- Be a CAC holder
- Be capable of sending and receiving digitally signed and encrypted email
- Have a working knowledge of service or agency structure, including populations and missions of service or agency posts and sites
- Be familiar with PKI, the CAC issuance process, and the service or agency TASS Business Process policy
- Have not been convicted of a felony offense
- Have had an FBI fingerprint check with favorable results
- Have had, at minimum, a National Agency Check with Inquiries (NACI) background investigation performed
- Have completed the required annual TASS Certification Training
- Have not knowingly been denied a security clearance or had a security clearance revoked
- Be trustworthy
- Be retainable for a minimum of 12 months

2.4 Trusted Agent Security Manager (TASM)

The SPOCs appoint TASMs for each site. In turn, TASMs handle user management and administration for their specific site, as well as oversee TA activity. Each site may only have two TASMs, a primary and an alternate.

2.4.1 TASM Responsibilities

TASMs have the following responsibilities:

- Meet TASM position requirements as specified in **Section 2.4.2 (TASM Requirements)**
- Act as a TA
- Troubleshoot TASS questions and issues for his or her site
- Manage TASM and TA users for his or her site
- Train an alternate site TASM and all TAs operating TASS
- Provide visibility for TASS at his or her site. The TASM may accomplish this via staff call, newsletter or weblink, or another effective means. Information should include the TASS location, hours of operation, telephone numbers, and other pertinent data
- Submit requests through his or her SPOC for new or additional TASS capability
- Coordinate all TASS matters with his or her SPOC
- Notify the SPOC and DMDC Support Center (DSC) of the following:
 - TASS outages
 - Suspected or known TASS system compromise
- Provision, appoint, or authorize TAs
- Ensure positive identification of all site TAs

Note: To access TASS and perform TASM duties, the TASM must pass the annual TASS Certification Training requirements.

2.4.2 TASM Requirements

A TASM must meet the following requirements:

- Be a U.S. citizen
- Be a DoD uniformed service member or DoD civilian working for the service or agency
- Be a CAC holder
- Be capable of sending and receiving digitally signed and encrypted email
- Have a working knowledge of the structure of the site under his or her control, including unit populations and missions

- Have had an FBI fingerprint check with favorable results
- Have had, at minimum, a NACI background investigation performed
- Have completed the required annual TASS Certification Training
- Have not been convicted of a felony offense
- Have not knowingly been denied a security clearance or had a security clearance revoked
- Be trustworthy
- Be retainable for a minimum of 12 months

Note: TASMs may not be Contractors. If a TASM who is also a Contractor attempts to log in to TASS as a TASM or TA, TASS will lock him or her out of the system and send an email notification to his or her SPOC, TASM, and TA.

2.5 Trusted Agent (TA)

TASMs identify and approve nominated TAs, and then register them in TASS through the DEERS Security Online application. DMDC recommends that TASMs not exceed 200 TAs per site.

Note: DMDC requires that TAs not manage more than 100 active Applicants per TA.

TAs handle the following:

- Establish sponsorship of the Applicant with the service or agency
- Verify the Applicant's need for logical or physical access to either a DoD network or facility, both initially and ongoing through semiannual reverifications

Note: Non-Federal Agency Civilian Associates may not require logical or physical access to a DoD network or facility.

- Initiate the process of application for registration of a government credential

2.5.1 TA Responsibilities

TAs have the following responsibilities:

- Establish sponsorship of Applicants with the service or agency
- Notify the TASM or SPOC (if the TASM is unavailable) of site capability (TASS) outages
- Notify the TASM, SPOC, or DSC of any suspected or known TASS system compromise
- Be current with the TASS Certification Training requirement, which allows access to TASS to perform the duties of the TA role

2.5.2 TA Requirements

A TA must meet the following requirements:

- Be a U.S. citizen
- Be a DoD uniformed service member or DoD civilian working for the service or agency
- Have had an FBI fingerprint check with favorable results
- Have had, at minimum, a NACI background investigation performed
- Be a CAC holder
- Be capable of sending and receiving digitally signed and encrypted email
- Have completed the required annual TASS Certification Training
- Have not been convicted of a felony offense
- Have not knowingly been denied a security clearance or had a security clearance revoked
- Be trustworthy

Note: TAs may not be Contractors. If a TA who is also a Contractor attempts to log in to TASS as a TA, TASS will lock him or her out of the system and send an email notification to his or her SPOC, TASM, and TA.

3 TASS Business Process Overview

The following sections describe the elements of the TASS Business Process.

3.1 Site Creation and TASM Registration

The SPOC first contacts the DST and authorizes the support team to establish a site ID and add the TASMs to the site in the system. The SPOC transmits the data required for site and TASM registration to the DST by sending digitally signed and encrypted email request forms (see **Appendix A** and **Appendix B**). The DST generates site ID and TASM records in DEERS and then delivers new login information to the SPOC or the established primary TASM by encrypted email. Typically, it takes the DST 48 hours to set up accounts for site IDs and TASMs.

3.2 TA Registration

The TASM registers a TA in TASS through the DEERS Security Online application (<https://webct2.dmdc.osd.mil/appj/audit>). You can also find a link to the DEERS Security Online application in the TASS application.

Note: For more information on using DEERS Security Online, you can access the DEERS Security Online Guide by completing the following steps:

1. Log in to DEERS Security Online.
2. Click **Help** in the upper right corner of the screen.
3. Click **Search**.
4. In the Search field, type User Guide.
5. Click **Go**.
6. Search results will display in the left navigation column. To print, right click on the search results and click **Select All**. Right click a second time and click **Print**.

The TA must already be enrolled in DEERS to be registered in TASS. DEERS generates a username and initial password for the new TA account associated to an existing TASS Site ID. The TASM obtains the username and site information in DEERS Security Online and provides it to the TA. TASS requires CAC log in only and does not use a password for log in purposes. However, if the TA requires the activation of his or her account for CAC log in, he or she must contact the DSC at 1-800-372-7437 and request account activation. Once the DSC activates the TA account, the TA can log in to TASS by using his or her CAC only. TA registration provides access only to the TASS application. TAs who previously registered for another DMDC application will not receive a new username. The TA uses the same username information for TASS and just needs to know the new TASS Site ID.

3.3 TASM/TA TASS Training

All new TASMs and TAs must complete and pass the TASS Certification Training via the DMDC Learning Site prior to beginning their respective roles.

All active TASMs and TAs must complete and pass TASS Certification Training on an annual basis. When the annual training date draws closer and the TAs or TAsMs log in to the TASS application, they see a notification to complete the training requirement. TAsMs and TAs receive the notification 30 days prior to the beginning of the 30-day recertification period. Once the 30-day notification has lapsed, TAs and TAsMs have 30 days to complete the certification training. If they do not meet the training requirement within 30 days, TASS locks them out of the application, preventing them from performing their duties within TASS until they satisfy the training requirement.

TASMs must complete and pass the following training courseware on the DMDC Learning Site:

- TASS001, *Introduction to Web-based Training on the DMDC Learning Site*
- TASS002, *Trusted Associate Sponsorship System (TASS) Training Overview*
- TASS003, *Trusted Associate Sponsorship System (TASS) Trusted Agent (TA) Training*
- TASS004, *Trusted Associate Sponsorship System (TASS) Trusted Agent Security Manager (TASM) Training*
- SEC000, *Introduction to Site Security Manager Web-based Training*
- SEC001, *Site Security Manager Roles and Responsibilities*
- SEC002, *Site Security Manager DMDC Security Online*

Note: Site Security Manager (SSM) is the similar role in RAPIDS to a TASM in TASS. In using DEERS Security Online or in training, TAsMs may see the SSM role referenced, but should understand that in the context of TASS, the information applies to the TASM role.

TAs must complete and pass the following training courseware on the DMDC Learning Site:

- TASS001, *Introduction to Web-based Training on the DMDC Learning Site*
- TASS002, *Trusted Associate Sponsorship System (TASS) Training Overview*
- TASS003, *Trusted Associate Sponsorship System (TASS) Trusted Agent (TA) Training*

Successful completion of the training updates the TASM or TA's profile in DEERS. If TASMs and TAs do not successfully complete the training, the TASS application does not allow them to log in.

Important: You have five attempts to pass a TASS certification course post-test. A failed fifth attempt locks you out of the course. To resume training, you must call the DSC Help Desk at 1-800-372-7437 to have your test reset. You can prevent lockout by considering the following tips:

1. Always read the course material thoroughly when navigating through the course.
2. Be sure to read the test questions and simulation instructions carefully before selecting an answer.
3. Allow the system time to process your action when taking a test that contains a simulation; refrain from clicking twice or clicking too fast while the simulation is in progress.
4. Press F5 to reload the simulation if it appears to stall while loading.

Important: Each use of F5 will count against you as a failed attempt.

5. If the Internet connection is lost while taking the course, the system will automatically mark the attempt in progress as failed. If the simulation inaccurately scores incorrect on the scored page of the simulation, ensure you properly exit out of the browser window to try again. DO NOT close the browser or you will fail.
6. Press F11 when unable to see the simulation in its entirety. Select the browser window, and press F11 to resize it. This enables you to view the simulation in a larger window.

3.4 TA Submission of Application

An Applicant requesting a government credential must first be vetted through his or her employer using the DoD-approved process and the process outlined in the following documents:

- Federal Information Processing Standards Publication 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- DoD Regulation 5200.2-R, "Personnel Security Program"
- Directive-Type Memorandum (DTM) 08-003—"Next Generation Common Access Card (CAC) Implementation Guidance"

Note: You should check with your service or agency for any additional internal policies or guidelines governing this process.

Note: All CAC holders must minimally have an initiated National Agency Check with Inquiries (NACI) and a favorable completion of a Federal Bureau of Investigation

(FBI) fingerprint check, or a DoD-determined equivalent investigation, or greater. However, Affiliated Volunteers requiring network access are only required to have an initiated National Agency Check (NAC), and a favorable completion of an automated FBI National Criminal History Check (fingerprint check). Per policy, personnel (e.g., Non-Federal Agency Civilian Associates for National Guard State Employees and United Services Organization (USO) eligible only for the DD Form 2765 (self-sponsored Civilian ID card) do not require background vetting.

Note: The FBI fingerprint check adjudication process may take up to four weeks to complete. You must confirm the favorable completion of the FBI fingerprint check before you create the application.

The TA must verify that the employer organization has vetted the Applicant according to these guidelines, and establish the affiliation of the Applicant with the service or agency. Once the TA has confirmed the vetting, the TA creates the application for submittal.

Before a TA can create a new application, he or she must meet the following prerequisites:

- Ensure the Applicant is not registered as a TASS TASM or TA
- Determine and verify the Applicant has a valid requirement for a government credential
- Verify the Applicant's sponsoring service or agency has vetted the Applicant
- Have the following Applicant information:
 - Last name
 - First name
 - Middle name (optional)
 - Person Identifier (e.g. Social Security Number [SSN])
 - Email address (use the Applicant's work email address, if available)
 - Date of birth
 - Personnel category
 - Organization
 - Eligibility expiration date
 - Contract information (number and end date), if the Applicant is a DoD Contractor or Other Federal Agency Contractor

3.5 Applicant Login

Once the TA submits a new application, the TA uses a secure means to provide the Applicant with his or her user ID and temporary password and the TASS weblink Uniform Resource Locator (URL). The Applicant can then log in to TASS to complete and submit the application. Once the TA submits the application, the Applicant has seven

days to complete an initial log in to TASS and begin the application process, or TASS will automatically disable the Applicant's application.

Once the Applicant has logged in for the first time, he or she has 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 it in a complete form. Once the Applicant submits a completed application, the system automatically sends an email notification to the TA. The Applicant cannot make changes to a submitted application unless the TA returns the application to the Applicant for correction.

3.6 Verification

After the TA receives notification that the Applicant has submitted his or her application, the TA logs in to TASS and reviews the application. Upon review, the TA can reset the password, approve the application, return it to the Applicant for changes, reject, or disable it. Before approving an application, the TA must establish an Applicant's need for logical or physical access to either a DoD network or facility (not required for some Non-Federal Agency Civilian Associates), and verify vetting and the Applicant's affiliation with the service or agency.

Once the TA approves the application, the Applicant needs to obtain a card through the RAPIDS Issuing Facility within 90 days; otherwise, the system automatically disables the application; see **Section 4 (Timeline to Complete Key TASS Procedures)**.

If the TA rejects or disables the application, the system notifies the Applicant by email and updates the appropriate status in the Applicant's record.

If the TA approves the application, the system updates DEERS with the Applicant information, and TASS reflects this status change in the Applicant's record; see **Section 3.8 (DEERS Updates)**.

3.6.1 Letter of Authorization

Some Applicants require a Geneva Convention CAC due to the nature of their work. In accordance with the Department of Defense Instruction (DoDI) 3020.41, "Contractor Personnel Authorized to Accompany the U.S. Armed Forces," if the Applicant plans to work overseas, the Applicant may need to obtain a Synchronized Predeployment & Operational Tracker (SPOT) Letter of Authorization (LOA) and present it at the RAPIDS Issuing Facility, along with the other required identification and eligibility documents, in order to obtain the CAC. The requirement has expanded from an Army-only system to a Department of Defense (DoD)-wide system and is currently being implemented in other government agencies.

3.6.2 Status-of-Forces Agreement

Applicants who work overseas (e.g., those who accompany and support military forces) may require Geneva Convention CACs and may need to provide documentation of the

appropriate Status-of-Forces Agreement (SOFA) at the RAPIDS Issuing Facility in order to receive a government credential.

SOFAs are usually an integral part of overall military base agreements that allow U.S. military forces to operate within a foreign host country. Each SOFA is negotiated separately with the individual host country and deals with particular circumstances unique to that country. SOFAs not only deal with issues necessary for day-to-day business, but also deal with civil and criminal jurisdiction. They are a means for the DoD to protect U.S. personnel who might be subject to foreign criminal investigation, prosecution, and imprisonment.

3.7 Card Issuance

Once the TA approves the application, the Applicant has 90 days to obtain a government credential from a RAPIDS Issuing Facility. At the RAPIDS Issuing Facility, an operator verifies and updates the DEERS data with the Applicant's data and status of the card.

3.8 DEERS Updates

TASS runs a nightly offline process to provide DEERS updates to TASS regarding government credentials and card statuses. When the process runs after the RAPIDS Issuing Facility has issued a card, the TASS application status changes from 'Approved' to 'Issued.'

3.9 Applicant Reverification

TASS requires TAs to either reverify or revoke active Applicant records every 6 months (180 days). In addition to confirming the Applicant's personal information and continued affiliation with the DoD for reverification, the TA must confirm that the Applicant has a continued need for a government credential. TASS notifies TAs and Applicants by email when reverification is due. A TA may also revoke an Applicant's government credential at any time; see **Section 7.8.3 (Revoking a CAC)**.

See **Appendix E** for the schedule for email notifications for Applicants requiring reverification.

3.10 Eligibility Expiration

Government credentials typically expire after 3 years. As the expiration date approaches, an Applicant must contact the TA, if a continued card requirement exists, and apply for a new card.

Before the TA initiates the application process for a new card, the TA must verify the Applicant's valid requirement for a new card according to known policies and procedures, and the Applicant's continued employment under contract to the DoD.

3.11 Applicant Revocation

The TA can have an Applicant's current card revoked at any time. The TA performs the revocation process within TASS by clicking the **Revoke** button; see **Section 7.8.3 (Revoking a CAC)** for further details. TASS updates DEERS and terminates the personnel record, and DEERS subsequently terminates the card and updates the Certificate Authority (CA). The CA revokes the Applicant's certificates. The Applicant, TA, and TASM receive notice of revocation by email. The TA coordinates the collection and return of the government credential in accordance with established policies, guidelines, and procedures. The TA must coordinate with Security personnel when Applicants do not return revoked cards.

Contractors must return the government credential to the issuing agency as soon as one of the following occurs, unless otherwise determined by the service or agency:

- When credential is no longer needed for contract performance
- Upon completion of employment
- Upon contract completion or termination

The contracting officer may delay final payment under the contract if the Applicant (Contractor) fails to comply with these requirements.

3.12 TA Sponsorship Transfer

TASMs can transfer Applicant sponsorship between TAs for only their assigned site. SPOCs can transfer Applicant sponsorship between TAs for any site within their assigned service or agency. An SPOC or TASM might need to transfer sponsorship because the TA is sick, the TA no longer works in a TA capacity, or the TA has an unmanageable number of Applicants. SPOCs and TASMs use the TASS application to perform Applicant transfers. The system notifies the TASMs, TAs, and affected Applicants of the TA reassignments by email. Applicant transfer requests between two different services or agencies must be forwarded to your SPOC to coordinate the request appropriately with the TASS Program Office.

Note: DMDC requires that TAs not manage more than 100 active Applicants per TA.

4 Timeline to Complete Key TASS Procedures

In order for Applicants to gain approval for their applications, SPOCs, TASMs, TAs, and Applicants must complete their respective Business Process tasks within TASS in a timely and accurate manner.

Table 1 shows the length of time allotted to complete procedures for each phase of application submission and approval in the TASS Business Process.

Timeline for TASS Procedures

Procedure	Role	Description
First login	Applicant	Once a TA creates and submits an application, an Applicant has seven days to perform an initial login to TASS and begin the application process before TASS automatically disables the application.
Time to review application	Applicant	After the Applicant performs the initial login, the Applicant has up to 30 days to complete the application before TASS automatically disables the application.
Time to review application	TA	Once an Applicant submits an application, a TA has 30 days to review the application before TASS automatically disables the application.
Time to have CAC issued	Applicant	Once a TA approves an application, an Applicant has 90 days to have a card issued before TASS automatically disables the application.

Procedure	Role	Description
Time to reverify Applicant account	TA	<p>Every six months (180 days) after the issuance of a valid card, the TA must either reverify or revoke the application.</p> <p>TASS sends the TA and Applicant an email notification reminding the TA to review the application in intervals of 30, 20, and 10 days before the reverification due date.</p> <p>If the TA fails to reverify or revoke the application, the TA and Applicant receive an email notification that TASS has revoked the application. If the TA revokes the application, the TA and Applicant receive an email notification that TASS has revoked the application.</p> <p>If a TA has reverified an application, he or she must reverify the record again in six months, providing the card remains valid.</p>
TASS Certification Training	SPOC/TASMs/TAs	<p>SPOCs, TASMs, and TAs must complete the TASS Certification Training every year (365 days). Failure to comply within the 365-day requirement results in user lockout from the TASS application.</p>

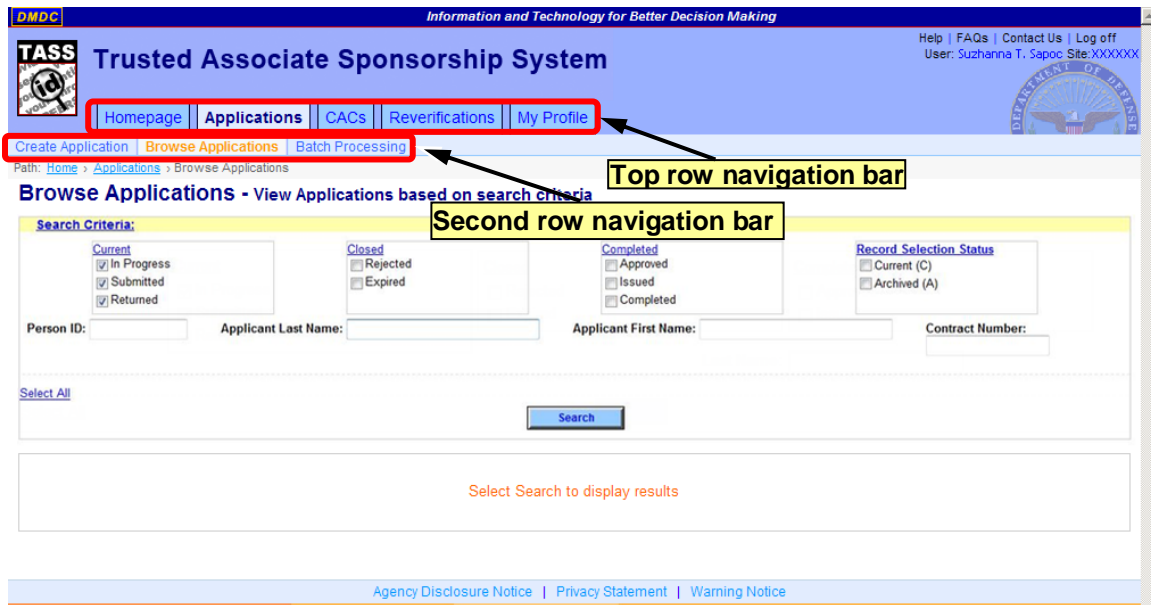
5 Definition of Terms

The following sections explain the terms used in the text within this document and the relationship of TASS screens to the role types.

5.1 Navigational References

The terms “Top row navigation” and “Second row navigation” are used throughout this document to refer to the standard tabular arrangement of links between pages (see Figure 1).

Figure 1. Navigational Layout



5.2 Figure Usage

Because TASMs and TAs share responsibilities, certain common screens may have the same format and information.

6 TASM User Guide

This section explains how an SPOC registers your site and registers you as a TASM, how you register a TA, and other duties of a TASM.

6.1 Site Registration

SPOCs start the TASS Business Process by registering a site. The following sections describe the TASS site registration process.

6.1.1 Site Definition

A TASS site (sometimes referred to as a site ID) is a logical collection of TASS users under the organizational control of a TASS TASM. Each TASM, in turn, reports to an SPOC.

Each TASM or TA has specific rights and privileges within the TASS application. For this reason, TASMs have administrative privileges only for TAs on their assigned sites. TASMs may not administer TAs from other sites.

6.1.2 SPOC Requests to DEERS

SPOCs initiate site registration for candidate sites under their control by completing the DD Form 2875, System Authorization Access Request (SAAR) (see **Appendix A**), and forwarding it to the DST. To register a site successfully, the SPOCs must complete all fields in the form. Once they complete the form for a site, they must use a digitally signed email message and forward it to the DST for processing.

Note: Use the *Optional Information* section, block 27 of DD Form 2875, to specify the details of your request.

Important: Never enter Personally Identifiable Information (PII) into any section of DD Form 2875. Provide any required PII data to the DST in a secure manner (i.e. encrypted email).

6.1.3 DEERS Turnaround

DEERS batch processes new requests and updates for site IDs and TASS users on a nightly basis. Allow at least 48 hours for the activation of new sites and accounts.

Note: Primary TASMs can call the DST to determine if a site is active or not, or they can log in to the newly created active TASS site, providing the SPOC has assigned the TASM to that site. Alternate TASMs must contact SPOCs or primary TASMs to verify that the new site has been activated.

6.1.4 Site ID Notification

After successfully registering a site, the DST notifies the SPOC of the new site ID number and account information.

6.2 TASM Registration

The following sections describe the TASM registration process.

6.2.1 TASM Registration Request

The SPOC registers TASMs for sites under his or her control. A primary TASM can register an alternate TASM at his or her site only. The new alternate TASM candidate fills out the DD Form 2875 (see **Appendix A**), and then sends it to the SPOC or primary TASM as an attachment to a digitally signed and encrypted email message.

Note: Use the *Optional Information* section, block 27 of DD Form 2875, to specify the details of your request.

Important: Never enter PII into any section of DD Form 2875. Provide any required PII data to the DST in a secure manner (i.e. encrypted email).

The SPOC or primary TASM reviews the DD Form 2875 for completeness and qualifications criteria.

- If the request does not meet the qualification or completeness requirements, the SPOC or primary TASM responds to the candidate with an explanation and coordinates the submission of a corrected request.

6.2.2 SPOC Request to DEERS

After the SPOC or primary TASM approves the DD Form 2875 for an alternate TASM, he or she forwards the request to the DST as an attachment to a digitally signed and encrypted email message.

If the SPOC or primary TASM requested the new alternate TASM account for an existing site, then he or she receives an email from the DST confirming the creation of the TASM registration account associated with the existing site ID.

If the SPOC requested a new primary TASM account simultaneous with a new site ID creation, the SPOC receives an email from the DST confirming the creation of the new TASM account and the new site ID.

Note: Only SPOCs can request new site IDs and primary or alternate TASMs. Primary TASMs can request SPOC approved alternate TASMs.

6.2.3 DEERS Turnaround

SPOCs should allow at least 48 hours for DEERS changes to become effective.

Note: Primary TASM can call the DST to determine if a site is active or not, or they can log in to the newly created active TASS site, providing the SPOC has assigned the TASM to that site. Alternate TASM must contact SPOCs or primary TASM to verify that the new site has been activated.

6.2.4 TASM Registration Notification

The TASM logs into DEERS Security Online to obtain the TA's User Account Code (i.e. username), presuming they have the appropriate access to DEERS Security Online. The TASM provides the TA with their username and site ID or the SPOC receive the alternate TASM account information (username and site ID) from the DST via a digitally signed and encrypted email message. Only new account holders receive username account information.

TASMs can also login to DEERS Security Online to find the TA's User Account Code (i.e. username), assuming they have the appropriate access to Security Online.

6.2.5 Updating TASM Information

If a TASM needs to update his or her demographic information (such as telephone number or address) in DEERS, he or she should route these requests through his or her SPOC for verification. The SPOC then submits the requested TASM account changes to the DST by digitally signed and encrypted email. Allow at least 48 hours for DEERS changes to take effect. Email address updates can be done by either visiting a RAPIDS Issuing Facility or accessing RSS from the **My Profile** tab from the TASS TASM *Homepage*; see **Section 6.6 (Changing a TASM User Profile)**.

Note: This process updates your personal information in DEERS, but it does not update the information stored on your CAC. To change the information stored on your CAC, you must return to a RAPIDS Issuing Facility.

6.2.6 Criteria and Procedures for TASM Removal

SPOCs remove or revoke TASM accounts by completing a DD Form 2875 (see **Appendix A**). A primary TASM, with SPOC approval, can request revocation of an alternate TASM account for his or her site only. He or she notes in block 27 that the action is to "Revoke" the TASM and submits the DD Form 2875 to the DST as an attachment to a digitally signed and encrypted email.

Note: Prior to revoking a TASM account, the SPOC or primary TASM must transfer any active Applicant records associated with the TASM's TA account to an active TA account.

Note: Use the *Optional Information* section, block 27 of DD Form 2875, to specify the details of your request.

Important: Never enter PII into any section of DD Form 2875. Provide any required PII data to the DST in a secure manner (i.e. encrypted email).

An SPOC revokes a TASM's TASS account and privileges if the TASM meets any of the following conditions:

- Is under investigation (or has been convicted) for any offense punishable by the Uniformed Code of Military Justice (UCMJ) or equivalent civilian law
- Has been relieved of duty
- Has left military service or civil service or has otherwise become disassociated with the service or agency
- Has transferred out of the organization

The SPOC must institute procedures for identifying TASMs who require removal. A primary TASM should consult with his or her SPOC on the removal of an alternate TASM.

Note: The SPOC must assign at least one active TASM to each site ID at all times to ensure management of all active TA accounts and associated Applicant records. The SPOC must manage TASM registration and revocations so that both a primary and an alternate TASM exist for every site under his or her service or agency.

The SPOC must coordinate with the DST to ensure timely TASM revocation using a procedure similar to the TASM registration procedure. Allow at least 48 hours for DEERS changes to take effect.

6.3 TA Registration

TAs have the following characteristics:

- Manage TASS applications for those individuals requesting a government credential for their service or agency only
- Receive on-the-job training from one of the site's TASMs or other personnel as designated
- Must complete the required annual TASS TA Certification Training
- Do not have TASS administrative privileges

6.3.1 TA Identification and Qualifications

Nominated TAs must meet minimum qualifications, as described in **Section 2.5.2 (TA Requirements)**. Once identified and approved by the SPOC, the TASM registers the TAs; see **Section 6.3 (TA Registration)**.

6.3.2 TA Registration Process

A site TASM registers TAs directly using the DEERS Security Online application; see **Section 6.7 (Creating a Trusted Agent Account)** for specific TA registration instructions. TASMs can also log in to DEERS Security Online to find the TA's User Account Code (i.e. username). If the TA's account becomes suspended, he or she needs to provide the username and TASS Site ID to the DSC to have the account reactivated. Accounts deactivate after 120 days of inactivity.

Note: DMDC requires that TAs not manage more than 100 active Applicants per TA.

6.3.3 Updating TA Information

If a TA needs to update his or her personal information (such as name or date of birth) in DEERS, he or she should submit a DEERS records correction to the DMDC Support Office (DSO) along with any required supporting documentation; contact number 1-800-361-2508. Sample forms for changes to DoB, Name, and Person Identifier (i.e., SSN, FIN, etc.) can be found under the **My Profile** tab by selecting the *Contact* link from the *Quick Links* menu. From the *TA Edit Contact Info* screen, you can access the RSS portal to change your email address. You should also have the site TASM make any necessary changes in DEERS Security Online (such as email address or name).

Note: This process updates your personal information in DEERS, but it does not necessarily update the information stored on your government credential. To change the information stored on your card, you must return to a RAPIDS Issuing Facility or use RSS; you may need to have a new card issued, depending on the type of changes made.

6.3.4 Criteria and Actions for TA Removal

Remove a TA from the TASS application and revoke his or her privileges if the TA meets any of the following conditions:

- Is under investigation (or has been convicted) for any offense punishable by the UCMJ or equivalent civilian law
- Has been relieved of duty
- Has left military or civil service or has otherwise become disassociated with the service or agency
- Has transferred out of the organization

Note: Prior to revoking a TA account, the SPOC or TASM must reassign any active Applicant records associated with the TA account to an active TA account.

6.4 Logging in as a TASM

This section goes through the steps to log in to the TASS application as a TASM.

6.4.1 Prerequisites

Before you can log in to the TASS application, you must meet the following prerequisite conditions:

- Have access to the TASS application with approval granted by an SPOC
- Hold a valid CAC
- Complete the required annual TASS TASM Certification Training

If you do not meet all of these prerequisites, you cannot log in to the TASS application.

Note: Under no circumstances can a TASM also be enrolled in TASS as a Contractor.

6.4.2 CAC Login

As a TASM, you must use your CAC to log in. You cannot use your username and password.

As a new TASM, you must complete the TASS Certification Training before the first time you log in to TASS. If you attempt to log in before taking the training, the login fails and TASS prompts you to take the training.

To log in to the TASS application as a TASM, perform the following steps:

1. Insert your CAC into the CAC reader.
 2. Open a web browser (such as Internet Explorer).
 3. Navigate to the TASS application (<https://www.dmdc.osd.mil/tass/>).
- Result: The *Consent to Monitor* screen appears (see Figure 2).

Figure 2. TASS Consent to Monitor Screen

DMDC Serving Those Who Serve Our Country

TASS Trusted Associate Sponsorship System

Standard Mandatory DoD Notice and Consent

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests - not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Acknowledgement Of Responsibilities Of Receiving And Maintaining Privacy Act Data

DATA YOU ARE ABOUT TO ACCESS COULD POTENTIALLY BE PROTECTED BY THE PRIVACY ACT OF 1974. You must:

- Have completed the necessary training with regards to Security Awareness and safe-guarding Personally Identifiable Information.
- Ensure that data is not posted, stored or available in any way for uncontrolled access on any media.
- Ensure that data is protected at all times as required by the Privacy Act of 1974 (5 USC 552a(1)(3)) as amended and other applicable DOD regulatory and statutory authority; data will not be shared with offshore contractors; data from the application, or any information derived from the application, shall not be published, disclosed, released, revealed, shown, sold, rented, leased or loaned to anyone outside of the performance of official duties without prior DMDC approval.
- Delete or destroy data from downloaded reports upon completion of the requirement for their use on individual projects.
- Ensure data will not be used for marketing purposes.
- Ensure distribution of data from a DMDC application is restricted to those with a need-to-know. In no case shall data be shared with persons or entities that do not provide documented proof of a need-to-know.
- Be aware that criminal penalties under section 1106(a) of the Social Security Act (42 USC 1306(a)), including possible imprisonment, may apply with respect to any disclosure of information in the application(s) that is inconsistent with the terms of application access. The user further acknowledges that criminal penalties under the Privacy Act (5 USC 552a(1)(3)) may apply if it is determined that the user has knowingly and willfully obtained access to the application(s) under false pretenses.

OK

4. Click **OK**.

➤ Result: The TASS *Login* screen appears (see Figure 3).

Figure 3. TASS Login Screen

DMDC Information and Technology for Better Decision Making

TASS Trusted Associate Sponsorship System

Help | FAQs | Contact Us

Please select your login method:

Applicant Login

Applicant Login

Select this option if you are applying for a CAC (Common Access Card) and a TA has provided you with a **username and password** to complete your application.

Operator Login

CAC Login

Select this option if you are a **TA, TASM, SPOC, or an applicant with a CAC**

Agency Disclosure Notice | Privacy Statement | Warning Notice

5. Click **CAC Login**.

- Result: The *Registered User Logon* screen appears (see Figure 4).

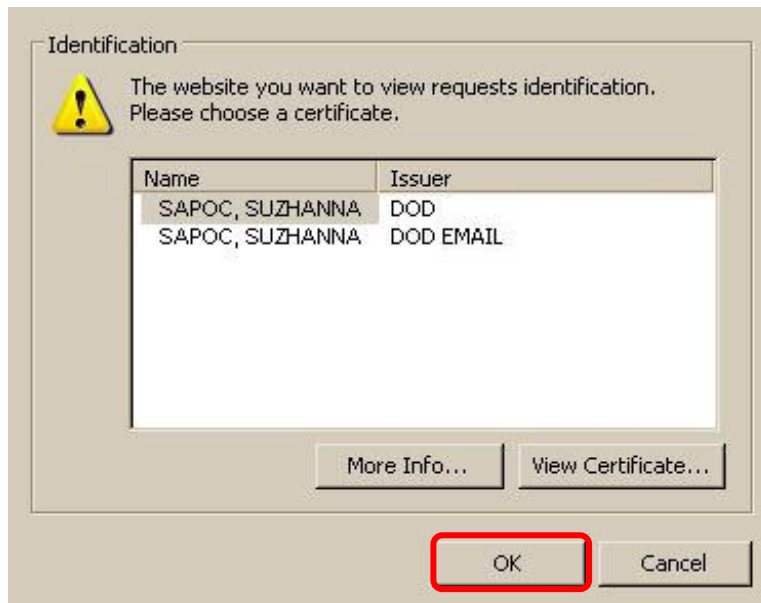
Figure 4. Registered User Logon Screen

6. Select the Common Access Card radio button.

7. Click **Continue**.

- Result: A *Certificate Selection Message* window opens, (see Figure 5).

Figure 5. Certificate Selection Message



8. Highlight the appropriate certificate.

9. Click **OK**.

- Result: An *ActivClient Login* window opens, prompting you to enter your CAC PIN (see Figure 6).

10. Type your CAC PIN.

- Result: The *Login Select Role* screen appears (see Figure 7).

Figure 6. CAC Login Box



Figure 7. Login—Select Role Screen



Note: The user interface screen you see and the privileges you have in the system vary depending on the role you choose.

11. Click **TASM**.

- Result: The *TASM Homepage* screen appears.

6.4.3 Login Failure

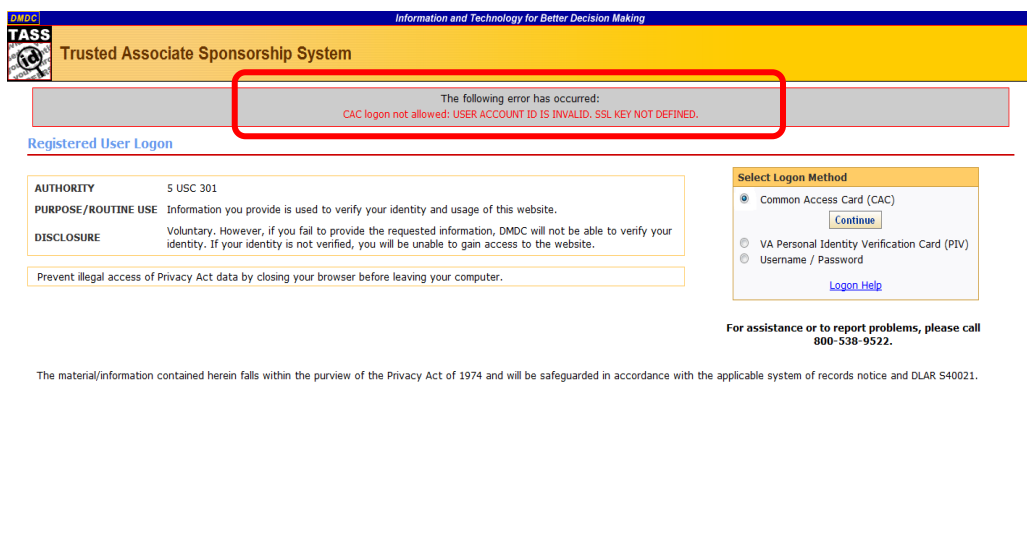
Login may fail in the following circumstances:

- Your account is suspended
- You have not accessed the account for 120 days or more
- You enter an incorrect URL
- You submit an incorrect CAC PIN
- You have not completed the required annual TASS Certification Training
- Your CAC has expired
- Your certificates have been terminated

The TASS application times out after 20 minutes of inactivity or if the page you are viewing for an application is out of synchronization with the actual status of the application.

For support with login failure, contact the DSC. With login or other failures, an error detection notification may appear on the *Login* screen (see Figure 8). If the error message indicates that you have not successfully completed the annual TASS Certification Training, go to <http://learning.dmdc.osd.mil> to take the required courses; see **Section 3.3 (TASM/TA TASS Training)** for more information.

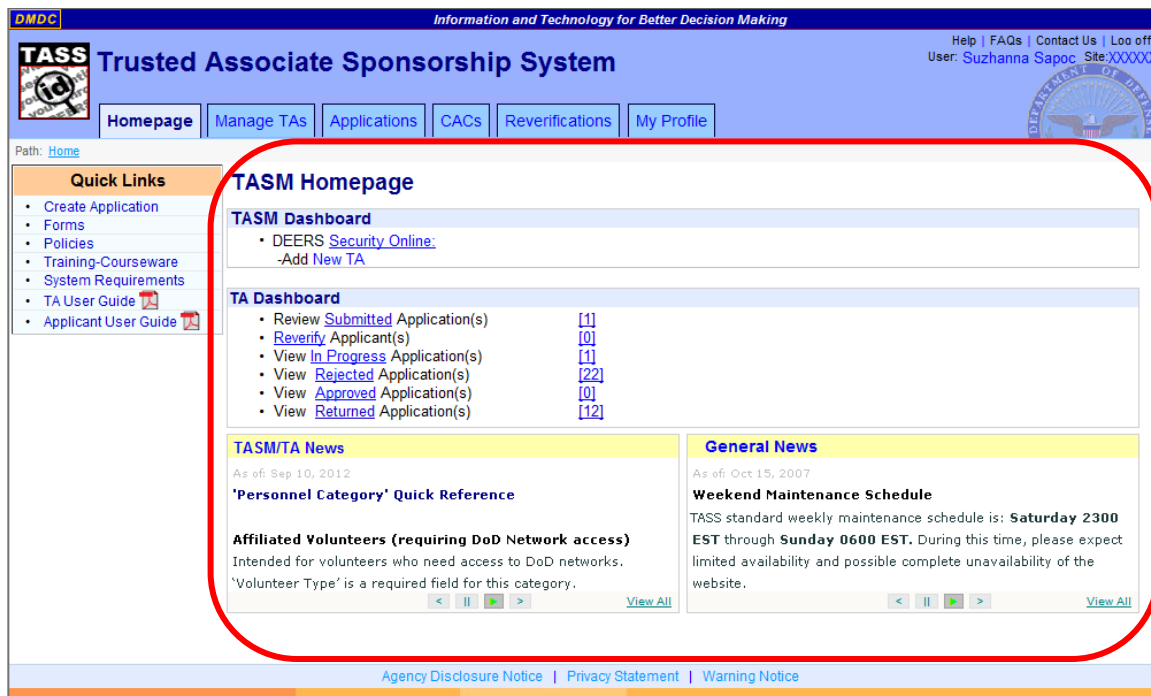
Figure 8. Login Screen—Login Failure



6.5 TASM Homepage

Use the *TASM Homepage* (Figure 9) to link to TASM and TA tasks, and to read news about TASS. You can access the *TASM Homepage* at any time by clicking the **Homepage** tab (see Figure 9).

Figure 9. TASM Homepage



The *TASM Homepage* has the following sections:

TASM Dashboard

Use the **DEERS Security Online** or **New TA** links on the *TASM Dashboard* to access the DEERS Security Online application.

TA Dashboard

Use the *TA Dashboard* to link to TA tasks; see **Section 7.2 (TA Homepage)**.

TASM/TA News

Use the *TASM/TA News* to read the most current messages about the TASS application related to TASM and TAs.

General News

Use the *General News* to read the most current general messages about the TASS application.

6.6 Changing a TASM User Profile

Use the *TASM Profile* screen to view your certification and site information, make changes to your contact information or password, and change authorized roles if applicable.

6.6.1 Changing TASM Contact Information

To change your TASM profile, perform the following steps:

1. Click the **My Profile** tab.
 - Result: The *TASM Profile* screen appears (see Figure 10).

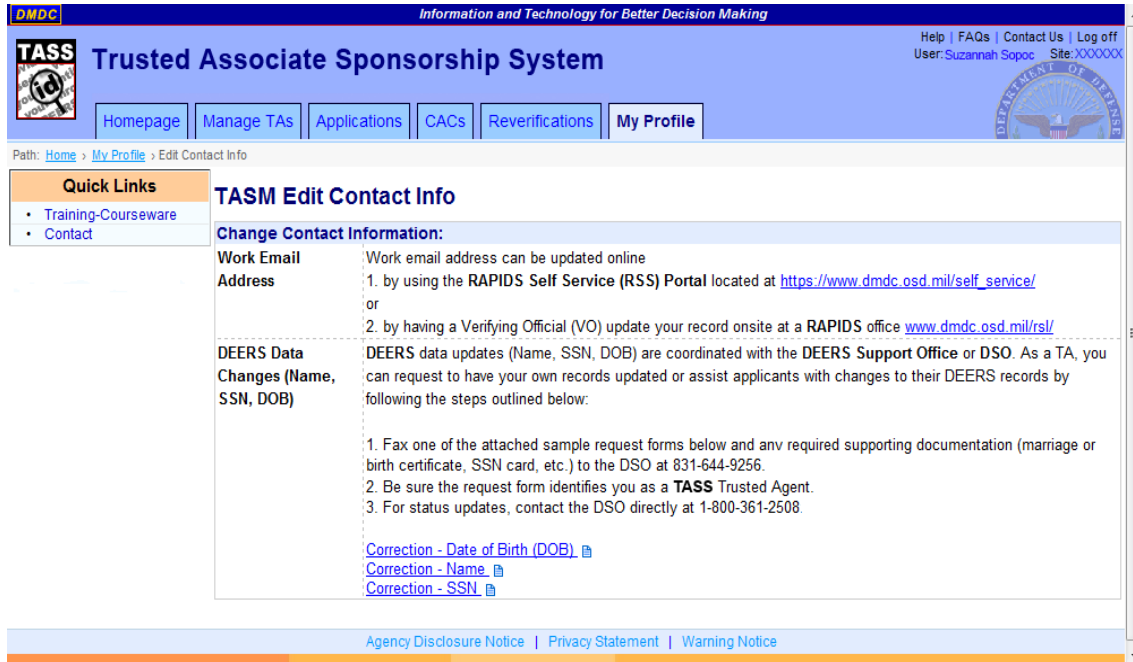
Figure 10. TASM Profile Screen



2. Click **Contact**.

- Result: The *TASM Edit Contact Info* screen appears (see Figure 11).

Figure 11. TASM Edit Contact Info Screen

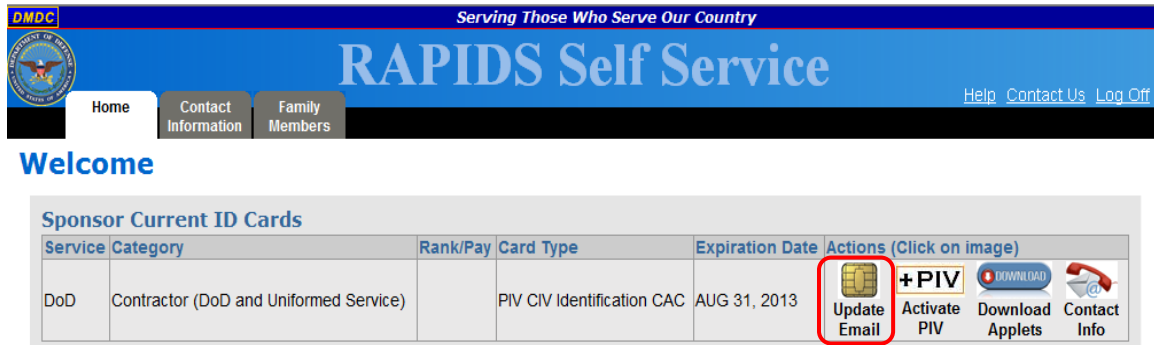


In the *Change Contact Information* area, you can change your email address through the RAPIDS Self Service (RSS) portal at (https://www.dmdc.osd.mil/self_service/) or by setting an appointment at a RAPIDS Issuing Facility (www.dmdc.osd.mil/rs1/).

To change your email address in the RSS portal:

3. Click the www.dmdc.osd.mil/self_service/ link.
4. Click **Sign On**.
 - Result: The RSS portal will launch in a new window.
5. Click **OK** to accept the Consent to Monitor Agreement.
 - Result: The CAC login page appears.
6. Enter your PIN in the *ActivClient Login* window.
 - Result: The RSS application Homepage opens.
7. Click the Update Email icon on the RSS Homepage (see Figure 12).

Figure 12. RSS Portal Actions



8. Follow the prompts to enter and save your email information.
9. When done, select **Log Off** before exiting RSS.

Note: You must notify your service or agency SPOC and submit a DEERS records correction to the DSO (contact number 1-800-361-2508) to update your personal information (such as name or date of birth) in DEERS, along with any required supporting documentation. Sample forms for changes to DoB, Name, and Person Identifier (i.e., SSN, FIN, etc.) can be found under the **My Profile** tab by selecting the *Contact* link from the *Quick Links* menu (see **Appendix H**). You should also have the site TASM make any necessary changes in DEERS Security Online (such as email address or name).

Note: This process updates your personal information in DEERS, but it does not necessarily update the information stored on your CAC. To change the information stored on your CAC, you must return to a RAPIDS Issuing Facility or use RSS; you may need to have a new card issued, depending on the type of changes made.

6.7 Creating a Trusted Agent Account

Use the DEERS Security Online application to create a new TA account in TASS. To register a TA, DEERS Security Online prompts for a Person ID or the TA's SSN, referred to as Type Code.

6.7.1 Prerequisites

Before you can create a new TA account, the following prerequisites must be met:

- The TA must be enrolled in DEERS
- The TA must be a DoD uniformed service member or DoD civilian
- You must have the following information about the TA:
 - Person ID (e.g. SSN)
 - Email address

- First name
- Last name

Note: Under no circumstances can a TA also be enrolled in TASS as a Contractor.

6.7.2 Creating a New TA Account

To create a new TA account from the *TASM Homepage* in TASS, perform the following steps:

1. Click **Add New TA**.

- **Result:** The DEERS Security Online *Registered User Log In* screen appears in a new browser window (see Figure 13).

Note: If you click the DEERS Security Online link (instead of the Add New TA link) from the TASM Homepage, a consent screen appears. You must click OK on the consent screen to advance to the DEERS Security Online Registered User Log In screen.

Figure 13. DEERS Security Online Registered User Log In Screen

DMDC Information and Technology for Better Decision Making

DEERS Security Online

Registered User Logon

AUTHORITY	5 USC 301
PURPOSE/ROUTINE USE	Information you provide is used to verify your identity and usage of this website.
DISCLOSURE	Voluntary. However, if you fail to provide the requested information, DMDC will not be able to verify your identity. If your identity is not verified, you will be unable to gain access to the website.

Prevent illegal access of Privacy Act data by closing your browser before leaving your computer.

Select Logon Method

Common Access Card (CAC) **Continue**

VA Personal Identity Verification Card (PIV)

Username / Password

[Logon Help](#)

For assistance or to report problems, please call 800-538-9522.

The material/information contained herein falls within the purview of the Privacy Act of 1974 and will be safeguarded in accordance with the applicable system of records notice and DLAR S40021.

2. Select either the **Common Access Card (CAC)** or **Username/Password** radio button.

3. Click **Continue**. Follow the prompts for any additional login information.

- **Result:** The *Welcome To Site Security Manager* screen appears (see Figure 14).

Note: Site Security Manager (SSM) is the similar role in RAPIDS to a TASM. In using DEERS Security Online or in the required TASS TASM Certification Training, you may see the SSM role referenced, but should understand that in the context of TASS, the information applies to the TASM role.

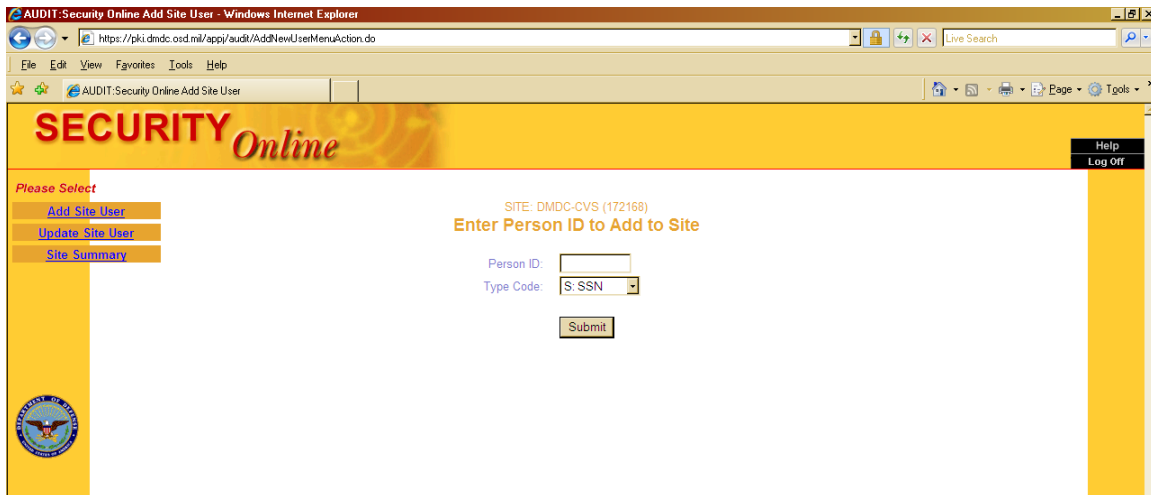
Figure 14. DEERS Security Online Welcome To Site Security Manager Screen



4. Click **Add Site User**.

➤ Result: The *Enter Person ID to Add to Site* screen appears (see Figure 15).

Figure 15. DEERS Security Online Enter Person ID Screen



5. Type the TA's SSN in the **Person ID** field and select **S: SSN** in the **Type Code** field.

6. Click **Submit**.

➤ Result: The *Add Site User* screen appears (see Figure 16).

Figure 16. DEERS Security Online Add Site User Screen

AUDIT: Security Online Update Site User - Windows Internet Explorer

https://pki.dmdc.osd.mil/app/audit/PuLSiteUserAction.do?requestType=ADD

AUDIT: Security Online Update Site User

SECURITY Online Help Log Off

Please Select

- Add Site User
- Update Site User
- Site Summary

SITE: DMDC-CVS (172168)
Add Site User

Position:

Email Address:

Title (Mr, Ms, LTC, etc.):

First Name: *

Middle Name:

Last Name: *

Cadency (Jr, Sr, III, etc.):

* required for new operators

Application Access:

Select/Revoke application(s) for this person.

Active	ID	Name (Type)	Access Code / Description
<input type="checkbox"/>	0229	CVSIUD KB (L)	00 / Trusted Agents
<input type="checkbox"/>	0229	CVSIUD KB (L)	01 / Trusted Agent Security Manager
<input type="checkbox"/>	0229	CVSIUD KB (L)	02 / Service Point of Contact
<input type="checkbox"/>	0229	CVSIUD KB (L)	03 / System Admin

Submit Cancel

Done Trusted sites 100%

7. Type the TA's required information in the following fields:

- **Email Address**

Note: DEERS Security Online does not show this as a required field. However, to create a TA account successfully, you must enter a valid work email address for the TA. If the TA's email address changes, you must update the email address in Security Online.

- **First Name**
- **Last Name**

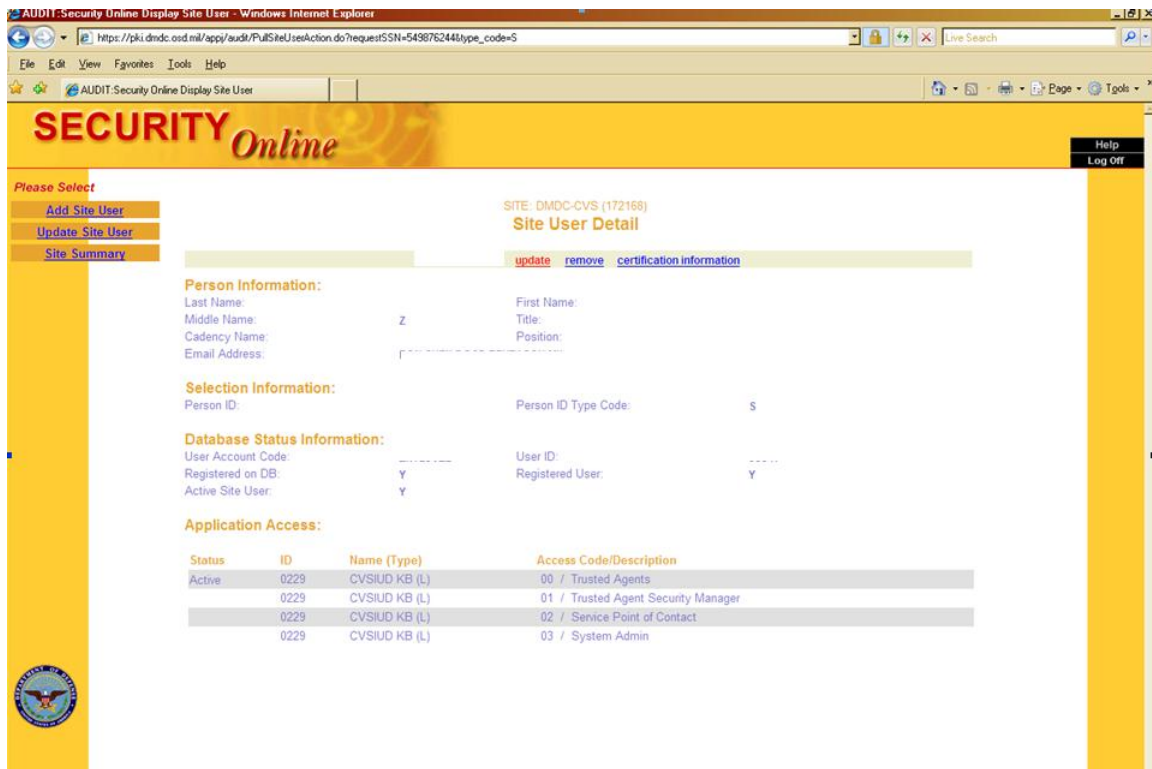
8. **Optional:** If available, type the TA's optional information in the remaining fields.

9. Select the **Active** check box for Application ID 0229, Access Code / Description 00 / Trusted Agents only.

10. Click **Submit**.

- **Result:** The *Update Site User* detail screen appears (see Figure 17).

Figure 17. DEERS Security Online Update Site User Detail Screen



- Review the information and make any corrections by clicking **update**.
- After you have verified the accuracy of the information, click **Log Off** in the right hand top corner of the screen.

Note: The application can take up to 48 hours to create and activate a TA account. Access the TA username information from the Site Summary under **User Account Code** once the account is active, and provide this information to the TA, along with the TASS Site ID information. If the TA has problems logging in, he or she must contact the DSC to ensure the DST activated the account. If the TA's account ever becomes suspended, the TASM will need to reactivate the account in DEERS Security Online. The TA may need to provide account information (User Account Code and TASS Site ID) to the DSC to have the account unlocked.

6.8 Managing TA Accounts

The TASM's Manage TAs tab now has two tabs (By TASM/TA and By Applicant) in the second row navigation bar. The By TASM/TA navigation tab opens the View Trusted Agents search screen and allows you to run a query for records by the TASM or TA's last name, role, or status. The added By Applicant navigation tab opens the Browse Applicants search screen which allows you to run a query for records by an Applicant's person ID, last name, first name, or contract number.

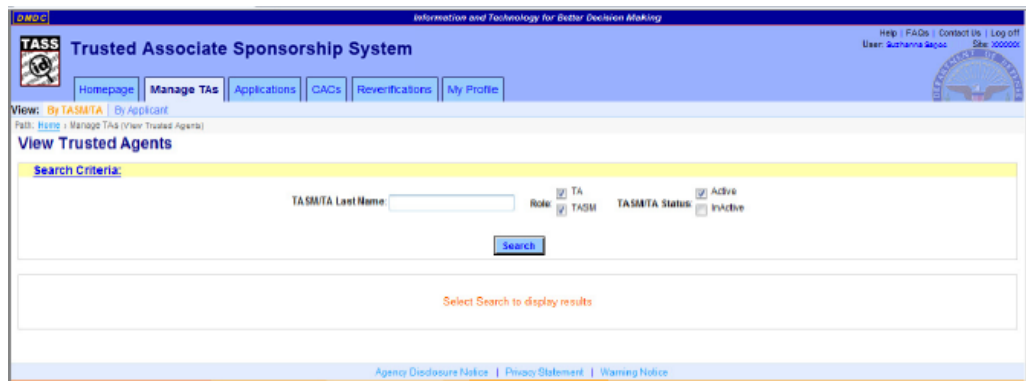
6.8.1 Viewing Trusted Agents

From the *View Trusted Agents* screen, you can search for, email, and sort your TAs. You can also reassign a TA's Applicant records to another TA at your site.

To view your TAs, perform the following steps:

1. Click the **Manage TAs** tab.
2. In the second row navigation bar, note that the **By TASM/TA** option is highlighted as the default selection.
 - Result: The *View Trusted Agents* screen appears (see Figure 18).

Figure 18. View Trusted Agents Screen



3. Choose one or more of the following *Search Criteria* options:
 - Type a full or partial last name in the **TASM/TA Last Name** field
 - Select the **TA Role** check box
 - Select the **TASM Role** check box
 - Select the **TASM/TA Status Active** check box
 - Select the **TASM/TA Status InActive** check box

Note: Optionally you can leave the Last Name field blank to access a list of all TA names.

4. Click **Search**.
 - Result: The *View Trusted Agents* search results screen appears (see Figure 19).

Figure 19. View Trusted Agents Screen—Search Results

The screenshot shows the TASS (Trusted Associate Sponsorship System) interface. At the top, there's a navigation bar with tabs: Homepage, Manage TAs, Applications, CACs, Reverifications, and My Profile. Below this, there's a search criteria section with a text input for 'TASM/TA Last Name', checkboxes for 'Role' (TA, TASM), and 'TASM/TA Status' (Active, InActive). A 'Search' button is present. Below the search criteria, it says '2 Records found, displaying all Records.' A table follows with columns: TASM/TA Name, Role, TASM/TA Status, and Links. The table contains two rows: one for 'True, Beatrice' (Role: TA, Status: Active) and one for 'Trust, Peter' (Role: TASM, Status: Active). In the 'Links' column, the first row has 'Application' and 'CACs' links, both highlighted with red boxes. Arrows point from these boxes to callout boxes below the table: 'Click link to reassign applications' and 'Click link to reassign CACs'. The page footer includes 'DMDC Information and Technology for Better Decision Making', 'Help | FAQs | Contact Us | Log off', and 'User: Suzhanna Sapoc Site: XXXXXX'.

Note: From the View Trusted Agents screen, you can reassign Applicants applying for government credentials or Applicants who already hold a credential to a different TA; see **Section 6.8.2 (Reassigning Applicants)** and **Section 6.8.4 (Reassigning CAC Holders to a New TA)**.

6.8.2 Browse Applicants Screen

From the *Browse Applicants* screen, you can manage TA accounts by searching for the account by Applicant.

To browse your Applicants, perform the following steps:

1. Click the **Manage TAs** tab.
 2. In the second row navigation bar, select **By Applicant**.
- Result: The *Browse Applicants* screen appears (see Figure 20).

Figure 20. Browse Applicants Screen

DMDC Information and Technology for Better Decision Making

Help | FAQs | Contact Us | Log off
User: Suzhanna Sapoc Site: XXXXXX

TASS Trusted Associate Sponsorship System

Homepage | Manage TAs | Applications | CACs | Reverifications | My Profile

View: By TASM/TA | By Applicant

Path: Home > Manage TAs > Browse Applicants

Browse Applicants

Search Criteria:

Current
 In Progress
 Submitted
 Returned

Closed
 Rejected
 Expired

Completed
 Approved
 Issued
 Completed

Record Selection Status
 Current (C)
 Archived (A)

Person ID: Applicant Last Name: Applicant First Name: Contract Number:

Select All

TASS handles numerous Applicant records for DoD.
In order to minimize wait time please enter:

Required Criteria

- Person ID, and/or
- Applicant Last Name (partial name can be entered), and/or
- Contract Number

Select **Search Applicants** to display results

Agency Disclosure Notice | Privacy Statement | Warning Notice

3. You can select one of the *Search Criteria* options for **Current**, **Closed**, **Completed** or **Record Selection Status**, or one or more of the following *Search Criteria* options:

- **Person ID (SSN, etc.)**
- **Applicant Last Name**
- **Applicant First Name**
- **Contract Number**

4. Click **Search Applicants**.

- Result: The *Browse Applicants* search results screen appears (see Figure 21).

Note: By clicking the Search Applicants button you can view the first set of Applicant records for a TA, without selecting any Search Criteria.

Figure 21. Browse Applicants Screen—Search Results

Search Criteria:

Current
 In Progress
 Submitted
 Returned

Closed
 Rejected
 Expired

Completed
 Approved
 Issued
 Completed

Record Selection Status
 Current (C)
 Archived (A)

Person ID: Applicant Last Name: Applicant First Name: Contract Number:

[Select All](#)

8 Records found, displaying all Records.

Select	Applicant Name	Person ID	Status	Status Date	Contract Number	Eligibility Expiration Date	Verified	TA
<input type="checkbox"/>	Tanner, Tammy		Returned (C)	2011-Mar-15	XXXXXXXXXX	2012-Mar-20		Suzhanna Sapoc
<input type="checkbox"/>	Taylor, Tern		Returned (C)	2010-Jul-23	XXXXXXXXXX	2012-Feb-20		Suzhanna Sapoc
<input type="checkbox"/>	Test, June		Returned (C)	2011-Nov-17	XXXXXXXXXX	2012-Feb-20		Suzhanna Sapoc
<input type="checkbox"/>	Tims, Larry		Returned (C)	2011-Apr-22	XXXXXXXXXX	2012-Feb-20		Suzhanna Sapoc
<input type="checkbox"/>	Tone, Tony		Returned (C)	2011-Feb-17	XXXXXXXXXX	2012-Feb-20		Suzhanna Sapoc
<input type="checkbox"/>	Tranca, Lance		Returned (C)	2010-Jun-18	XXXXXXXXXX	2011-Mar-20		Suzhanna Sapoc
<input type="checkbox"/>	Trupe, Jodi		Returned (C)	2011-Nov-29	XXXXXXXXXX	2011-Mar-20		Suzhanna Sapoc
<input type="checkbox"/>	Truth, Honesty		Returned (C)	2010-Sep-30	XXXXXXXXXX	2011-Mar-20		Suzhanna Sapoc

To: Per page:

8 Records found, displaying all Records.

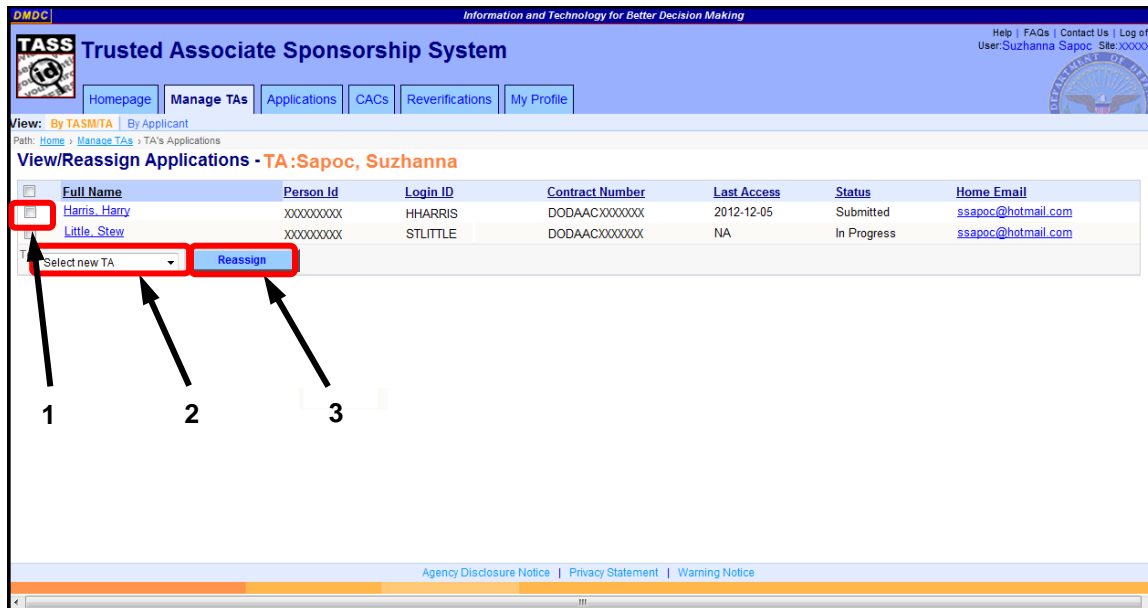
[Agency Disclosure Notice](#) | [Privacy Statement](#) | [Warning Notice](#)

6.8.3 Reassigning Applicants

To reassign Applicant records to a different TA, perform the following steps:

1. Complete the steps listed above in **Section 6.8.1** (Viewing Trusted Agents).
2. Click **Applications**.
 - Result: The *View/Reassign Applications* screen appears (see Figure 22).

Figure 22. View/Reassign Applications Screen



3. Select the check box next to the Applicant name(s) that you want to assign to a new TA (see Figure 22, #1).

Note: You can sort the Applicant information by clicking on any of the column headers on the *View/Reassign Applications* screen.

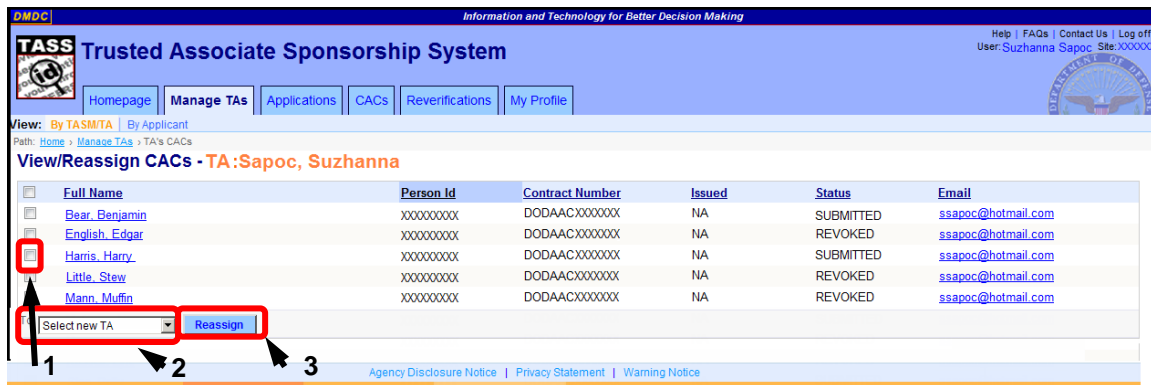
4. **Optional:** View an Applicant's application by clicking on the Applicant's name (see Figure 22).
5. From the **Select new TA** drop-down list, select a new TA to reassign the selected Applicant(s) to (see Figure 22, #2).
6. Click **Reassign** (see Figure 22, #3).
 - Result: A confirmation screen appears, and the TASS application sends an email to the formerly assigned TA, the newly assigned TA, and the Applicant.

6.8.4 Reassigning CAC Holders to a New TA

To reassign CAC holders to a different TA, perform the following steps:

1. Complete the steps listed above in **Section 6.8.1**(Viewing Trusted Agents).
2. Click **CACs**.
 - Result: The *View/Reassign CACs* screen appears (see Figure 23).

Figure 23. View/Reassign CACs Screen



3. Select the check box next to the Applicant name(s) that you want to assign to a new TA (see Figure 23, #1).

Note: You can sort the Applicant information by clicking on any of the column headers on the *View/Reassign CACs* screen.

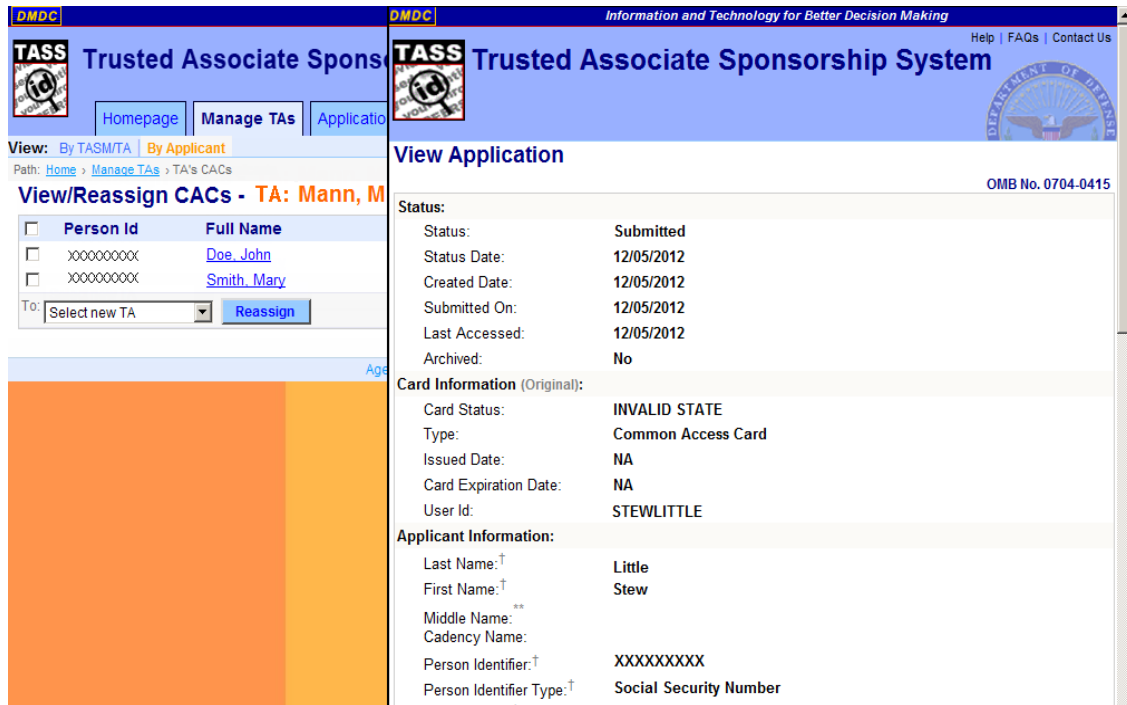
4. **Optional:** View an Applicant's application by clicking on the Applicant's name (see Figure 23).

5. From the **Select new TA** drop-down list, select a new TA to reassign to the selected Applicant(s) to (see Figure 23, #2).

6. Click **Reassign** (see Figure 23, #3).

- **Result:** A confirmation screen appears, and the TASS application sends an email to the formerly assigned TA, the newly assigned TA, and the Applicant.

Figure 24. TASM View Application Screen



Note: Figure 24 provides an example of the *View Application* popup screen when you have selected the Applicant information from the Full Name column header.

7 TA User Guide

Use this section to find out how to perform the duties of a TA.

7.1 Logging in as a TA

Use the information in this section to log in to the TASS application as a TA.

7.1.1 Prerequisites

Before you can log in to the TASS application, you must meet the following prerequisites:

- Have access to the TASS application granted by a TASM
- Hold a valid CAC
- Complete the required annual TASS Certification Training

If you do not meet all of these prerequisites, you cannot log in to the TASS application.

Note: Under no circumstances can a TA also be enrolled in TASS as a Contractor.

7.1.2 CAC Login

After your TASM creates your TASS TA account, he or she provides you with your TASS username and site ID. If you encounter issues with initial login, call the DSC to have your account activated. If your account ever becomes suspended, the TASM will need to reactivate the account in DEERS Security Online. You may need to provide account information (User Account Code and TASS Site ID) to the DSC to have the account unlocked.

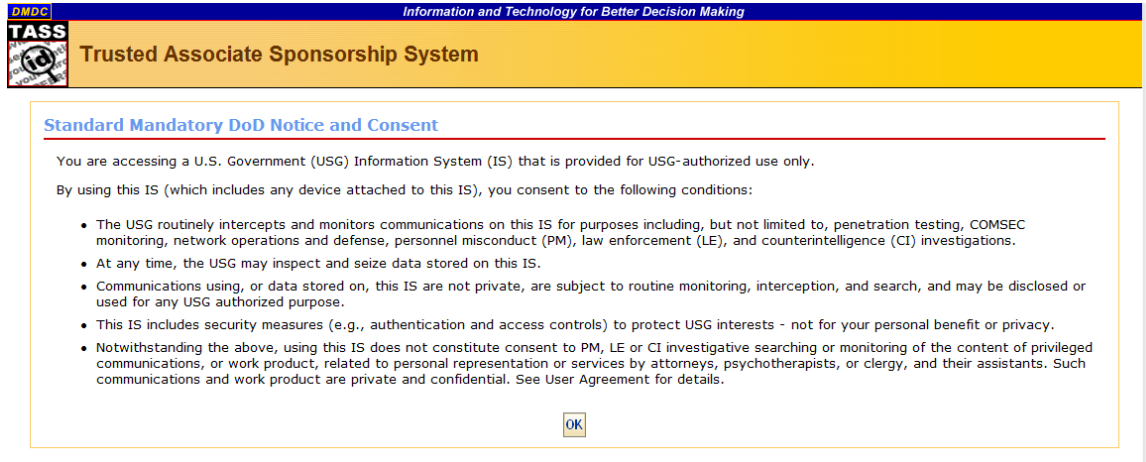
Note: As a TA, you must use your CAC to log in. You cannot use your username and password.

As a new TA, you must complete the TASS Certification Training before you are able to access the TASS application. When you attempt to log in before completing the training, TASS will prompt you to take the training required for your role.

To log in to the TASS application as a TA, perform the following steps:

1. Insert your CAC into the CAC reader.
2. Open a web browser (such as Internet Explorer).
3. Navigate to the TASS application (<https://www.dmdc.osd.mil/tass>).
 - Result: The *Consent to Monitor* screen appears (see Figure 25).

Figure 25. TASS Consent to Monitor Screen



4. Click **OK**.

➤ Result: The TASS *Login* screen appears (see Figure 26).

Figure 26. TASS Login Screen



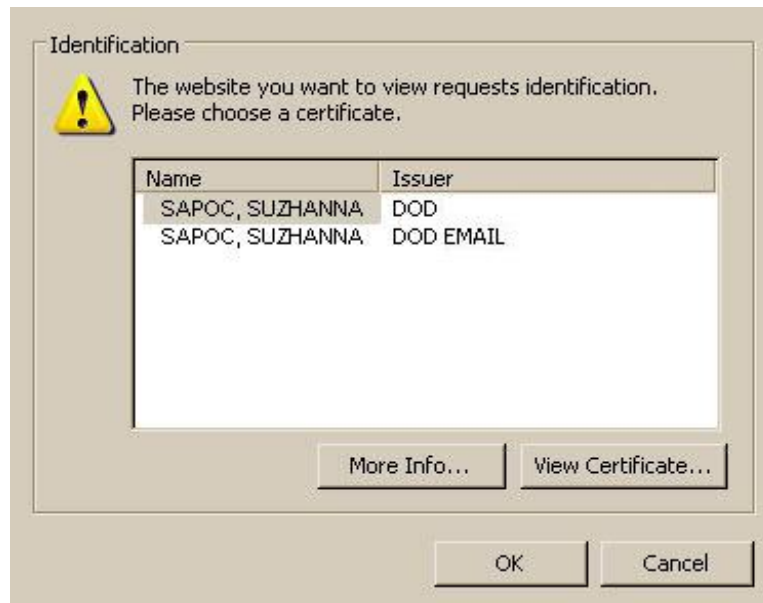
5. Click **CAC Login**.

➤ Result: The *Registered User Logon* screen appears (see Figure 27).

Figure 27. Registered User Logon Screen

6. Select the Common Access Card radio button.
7. Click **Continue**.
 - Result: A *Certificate Selection Message* window opens (see Figure 28).

Figure 28. Certificate Selection Message



8. Highlight the appropriate certificate.
9. Click **OK**.
 - Result: An *ActivClient Login* window opens, prompting you to enter your CAC PIN (see Figure 29).

10. Type your CAC PIN.

- Result: If you have more than one role in TASS, the *Login Select Role* screen appears (see Figure 30). If you only have a TA role, the *TA Homepage* appears (see Figure 32).

Figure 29. CAC Login Box

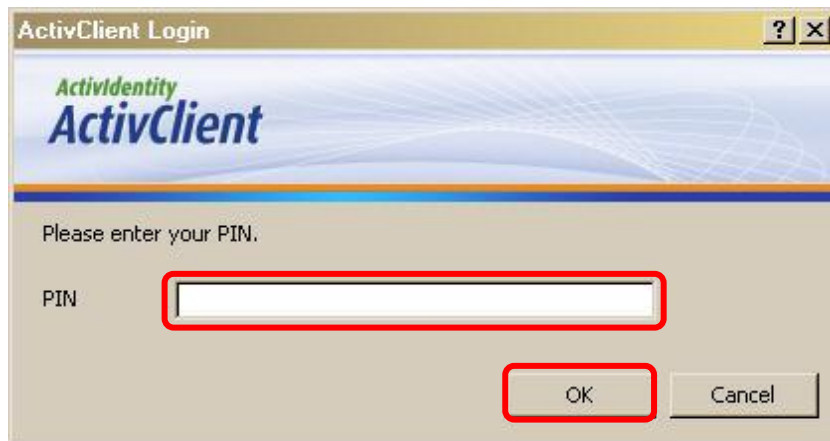


Figure 30. Login—Select Role Screen



11. Click **TA**, if applicable.

- Result: The *TA Homepage* screen appears (see Figure 32).

Note: The first time you log in, the TA Profile screen appears.

7.1.3 Login Failure

Login may fail in the following circumstances:

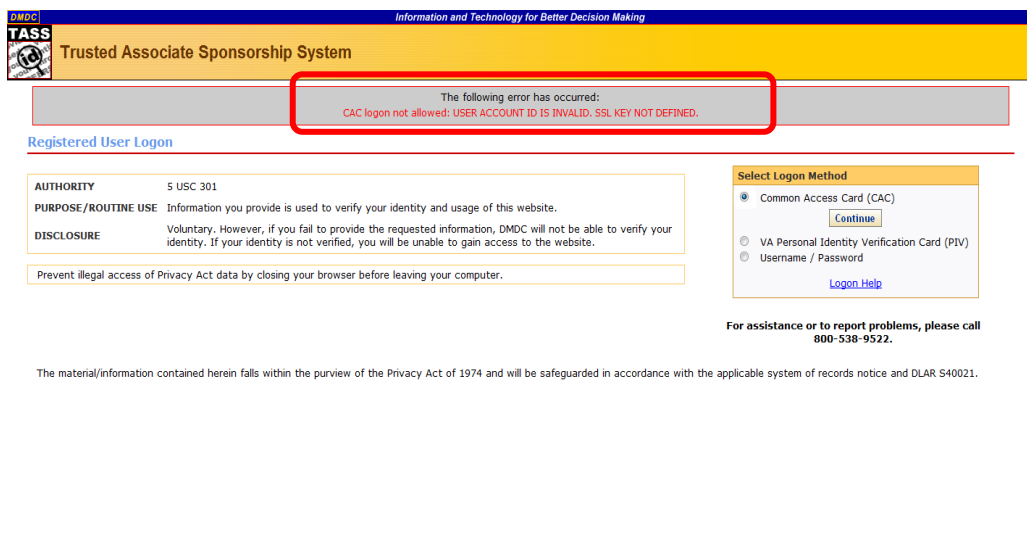
- Your account is suspended
- You have not accessed the account for 120 days or more

- You enter an incorrect URL
- You submit an incorrect CAC PIN
- You have not completed the required annual TASS Certification Training
- Your CAC has expired
- Your certificates have been terminated

The TASS application times out after a 20 minute period of inactivity or if the page you are viewing for an application is out of synchronization with the actual status of the application.

For support with login failure, contact the DSC. With login or other failures, an error detection notification may appear on the *Login* screen (see Figure 31). If the error message indicates that you have not taken the annual TASS Certification Training, go to <http://learning.dmdc.osd.mil> to take the required courses; see **Section 3.3 (TASM/TA TASS Training)** for more information.

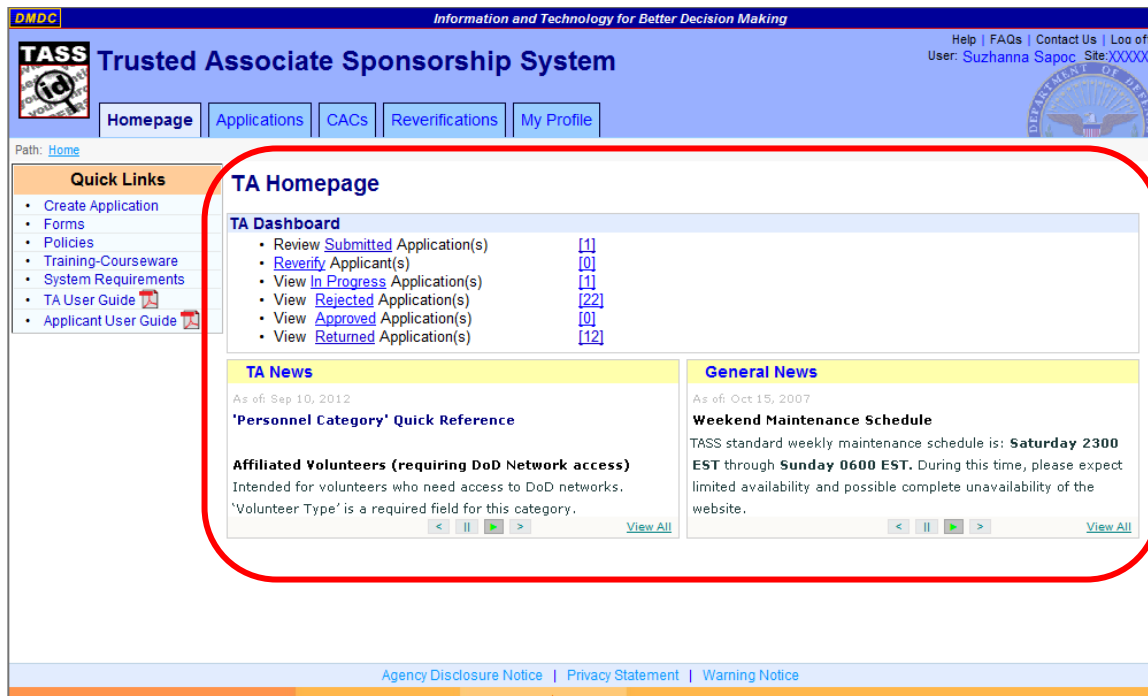
Figure 31. Login Screen—Login Failure



7.2 TA Homepage

Use the *TA Homepage* to perform TA tasks and to read news about TASS. The *TA Homepage* also provides news regarding TASS operations. You can return to the *TA Homepage* at any time by clicking the **Homepage** tab (see Figure 32).

Figure 32. TA Homepage



The *TA Homepage* has the following sections:

TA Dashboard

Use the *TA Dashboard* to link to TA tasks. You can perform the following tasks from the *TA Dashboard*:

- Review submitted applications
- Reverify Applicants
- View in-progress applications
- View rejected applications
- View approved applications
- View returned applications

TA News

Use the *TA News* to read the most current messages about the TASS application related to TAs.

General News

Use the *General News* to read the most current general messages about the TASS application.

7.3 Updating Your TA Profile

Use the *TA Profile* screen to access your training and courseware or contact information or view certification and site information, and change authorized roles if applicable.

7.3.1 Changing TA Contact Information

To update your contact information, perform the following steps:

1. Select the **My Profile** tab.

➤ Result: The *TA Profile* screen appears (see Figure 33).

Figure 33. TA Profile Screen

The screenshot displays the 'TA Profile' screen. At the top, there is a header with the DMDC logo and the text 'Information and Technology for Better Decision Making'. Below this is the TASS logo and the title 'Trusted Associate Sponsorship System'. The navigation menu includes 'Homepage', 'Applications', 'CACs', 'Reverifications', and 'My Profile'. The 'My Profile' tab is selected. On the left, a 'Quick Links' menu has 'Contact' highlighted with a red box and an arrow pointing to the main content area. The main content area is titled 'TA Profile' and contains sections for 'Certification Information', 'Site(s) Information', 'Miscellaneous Information', and 'Authorized Role(s)'. The 'Certification Information' section shows 'Status: A (Active)', 'Train By Date: 20200101 (YYYYMMDD)', 'Message Type: Training is Current', and 'Message: Certification Training has been completed for this period'. The 'Site(s) Information' section shows 'Organization: Department Of Defense' and 'Site: DMDC-TASS'. The 'Miscellaneous Information' section shows 'You are authorized to perform Batch Upload'. The 'Authorized Role(s)' section shows 'TA'.

2. Click **Contact** in the *Quick Links* menu at the left of the *TA Profile* screen.

➤ Result: The *TA Edit Contact Info* screen appears (see Figure 34).

Figure 34. TA Edit Contact Info Screen

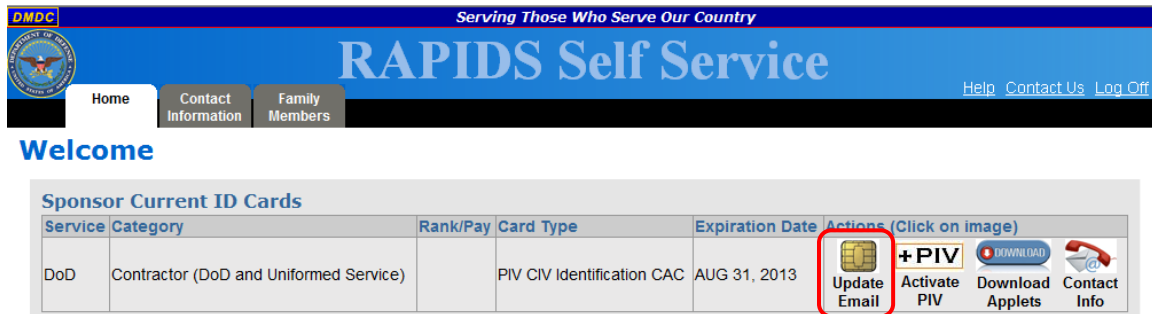


In the *Change Contact Information* area, you can change your email address through the RAPIDS Self Service (RSS) portal at (https://www.dmdc.osd.mil/self_service/) or by setting an appointment at a RAPIDS Issuing Facility (www.dmdc.osd.mil/rsl/). The RSS application URL will launch a new window, separate from TASS.

To change your email address in the RSS portal:

3. Click the **www.dmdc.osd.mil/self_service/** link.
 - Result: The RSS portal will launch in a new window.
4. Click **Sign On**.
5. Click **OK** to accept the Consent to Monitor Agreement.
 - Result: The CAC login page appears.
6. Enter your PIN in the *ActivClient Login* window.
 - Result: The RSS application Homepage opens.
7. Click the Update Email icon on the RSS Homepage (see Figure 35).

Figure 35. RSS Portal Actions



8. Follow the prompts to enter and save your email information.
9. When done, select **Log Off** before exiting RSS.

Note: You must notify your service or agency SPOC and submit a DEERS records correction to the DSO (contact number 1-800-361-2508) to update your personal information (such as name or date of birth) in DEERS, along with any required supporting documentation. Sample forms for changes to DoB, Name, and Personal Identifier (i.e., SSN, FIN, etc.) can be found under the My Profile tab by selecting the Contact link from the Quick Links menu. You should have the site TASM make any necessary changes in DEERS Security Online (such as email address or name).

Note: This process updates your personal information in DEERS, but it does not necessarily update the information stored on your government credential. To change the information stored on your card, you must return to a RAPIDS Issuing Facility or use RSS; you may need to have a new card issued, depending on the type of changes made.

7.4 Creating a New Application

Use this section to create new applications for Applicants seeking government credentials. For more information on the actions that Applicants perform during the application process, see the TASS Applicant User Guide and reference the *Quick Links* section of the TASS application.

7.4.1 Prerequisites

Before you can create a new application, you must perform the following prerequisite steps:

- Determine and verify the Applicant has a valid requirement for a government credential

- Perform necessary actions and checks according to DoD instructions and installation policies, guidelines, and procedures
- Know the following information about the Applicant:
 - Last Name
 - First Name
 - Middle Name
 - Cadency Name
 - Person Identifier (SSN, Foreign Identification Number [FIN], ITIN)
 - Date of Birth
 - Primary Email
 - Personnel Category
 - Organization
 - Eligibility Expiration Date
 - Contract number and end date, if applicable

Note: Under no circumstances can a Contractor also be enrolled in TASS as a TASM or TA.

Note: TASS verifies contract numbers through PIVS (see Figure 36). The TA is not restricted from completing the application if a PIV contract number is not entered.

Figure 36. Example of TASS/PIV Verification Warning Notice

Contract Information:	
Contract Number:	XXXXXX-XX-X-XXXX
Contract End Date:	08/30/2013 (MM/DD/YYYY)
Sponsor (TA):	
TA (Trusted Agent):	Parikh, Aseem
Organization:	Department Of Defense
Telephone Number:	8005551111
Office Name:	Beauregard
Street Address 1:	123 Fake St
Street Address 2:	
City:	Alexandria
State:	VA
Zip Code:	22311
Last four Zip Code:	0000
Country:	US

Warnings/Messages
Please notice messages below and view existing data using provided link(s).
<ul style="list-style-type: none">• CONTRACT NUMBER VALIDATION SERVICE: The contract number you entered could not be matched to an agency. Please ensure your contract number is correct before continuing.• An application already exists with this Person Identifier with 'Expired' status. [This is not the CAC status]• This person exists in DEERS.• Please review their DEERS records.
View existing Application for Cooper, Sheldon [Also to check/see CAC status if available] Use DEERS Compare to see more data.

7.4.2 Creating an Application

To create a new application, perform the following steps:

1. Click the **Applications** tab.

2. Click the **Create Application** link from the second row navigation bar.

➤ The *Create New Application Account* screen appears (see Figure 37).

Note: You can also access the **Create Application** link from the *Quick Links* menu from the *TA Homepage*.

Figure 37. Create New Application Account Screen

Create Application | [Browse Applications](#) | [Batch Processing](#)

Path: [Home](#) > [Applications](#) > Create New

Create New Application Account

[Instructions](#) (Help with this form) OMB No. 0704-0415

Application Data

Applicant Information:

Last Name:† Gable

First Name:† Eric

Middle Name: **

Cadency Name: None

Person Identifier:† Social Security Number

Date Of Birth:† MM/DD/YYYY

Primary Email:†*

Personnel Category:†

- Affiliated Volunteers (requiring DoD Network access)
- DoD and Uniformed Service Contractor
- Foreign Affiliate
- Non-DoD Civil Service Employee
- Non-Federal Agency Civilian Associate
- Non-US Non-Appropriated Fund (NAF) Employee
- OCONUS Hire
- Other Federal Agency Contractor

Note: TASS will track all TAs associated to a given Applicant record. However, TASS will only display the information of up to **three** TAs, if applicable. Only the present or current TA will be able to view the information of the TA that created the initial or original application, the TA information that possessed the record directly before them, and the present TA (their own) information.

3. Complete the following required Applicant fields on the *Create New Application Account* page:

- **Last Name**
- **First Name**
- **Person Identifier (SSN, etc.)**

Note: TASS now accepts 800 series Social Security Numbers as a Person Identifier.

- **Primary Email**
- **Date Of Birth**

4. **Optional:** Complete the following optional fields:

- **Middle Name**

- **Cadency Name**

Note: If the Applicant does not have a middle name, leave the field blank. TASS does not recognize entries such as “N/A” or “No Middle Name.”

5. Select the appropriate **Personnel Category** radio button. Select from the following Personnel Categories:

- *Affiliated Volunteers (requiring DoD Network access)* - The Affiliated Volunteers allows you to process and track Volunteers who need access to DoD networks. You must select a Volunteer Type for this category. *Examples of Affiliated Volunteers (requiring DoD Network access) include:*
 - American Red Cross Volunteer
 - Boy Scout Affiliate
 - Civil Air Patrol (CAP)
 - Education
 - Family Support
 - Girl Scout Affiliate
 - Legal Assistance
 - Medical Interns at MTFs
 - Military Treatment Facilities (MTF)
 - Religious
 - Student Intern

Note: If you enter a Foreign Identification Number (FIN) as an Applicant's personal identifier, he or she can NOT be assigned to the Affiliated Volunteer or Non-Federal Agency Civilian Associate Personnel Categories.

- *DoD and Uniformed Service Contractor* - DoD and Uniformed Service Contractor is the default Personnel Category setting.

Important: This category is appropriate for DoD and Uniformed Service, which also includes NOAA, Public Health Service Contractors, and Federally Funded Research and Development Center employees. Do not use this category for non-DoD contractors. This will cause incorrect data to populate to DEERS and you will have to restart the application process over. For non-DoD contractors, use the Other Federal Agency Contractor Personnel Category.

Important: When you select the *DoD and Uniformed Service Contractor* Personnel Category, the **Contractor Type** drop-down menu will appear with “Contractor Type Not Applicable” shown as the default option. Only if the Applicant is a Federally Funded Research and Development Center employee, select FFRDC employee from the drop-down menu.

Note: You must enter a **Contract Number** and **Contract End Date** for this category.

- *Foreign Affiliate* – The Foreign Affiliate category refers to a non-U.S. citizen (military, civilian or contractor) who is sponsored by a country other than the United States as part of an official visit or assignment to work on a DoD facility.

- *Non-DoD Civil Service Employee* - This category should be selected for a Non-DoD Civil Service employee. You must select a **Government Agency** for this category. Examples of Non-DoD Civil Service Employee categories include:
 - Department of Justice
 - Department of Labor
 - Department of State
 - Department of Interior
 - Department of Treasury

Important: Do not select this category for a non-DoD contractor. This will cause incorrect information to populate in DEERS and you will have to restart the application process over. For non-DoD contractors, use the Other Federal Agency Contractor Personnel Category.

- *Non-Federal Agency Civilian Associate* - The Non-Federal Agency Civilian Associate category allows you to track certain affiliated agencies who directly support the Uniformed Services, as well as other categories of personnel who have a direct affiliation with the Uniformed Services but are not otherwise identified in the other Personnel Categories. You must select a **Civilian Associate Type** and **Organization** for this category. **Associate Types** for the Non-Federal Agency Civilian Associates Personnel Category include:
 - American Red Cross Employees
 - Boy and Girl Scout Professionals
 - Intergovernmental Personnel Act (IPA)
 - National Guard State Employees
 - United Service Organization (USO)

Note: For Boy and Girl Scout Professionals, the **Army** is the only sponsoring organization option available.

- *Non-US Non-Appropriated Fund (NAF) Employee* - The Non-US Non-Appropriated Fund (NAF) Employee category allows you to track NAF employees who are non-US citizens using only a FIN or ITIN as the Person Identifier.
- *OCONUS Local Hire* – The OCONUS Local Hire category is intended for U.S. citizens residing in the host country that may be recruited locally by NAFIs in foreign areas, in accordance with established status of forces agreements.
- *Other Federal Agency Contractor* - The Other Federal Agency Contractor category is used for non-DoD contracted employees who are connected with a non-DoD Agency to complete a contract. You must select a **Government Agency** and enter a **Contract Number** and **Contract End Date** for this category.

Important: Do not select this category for a non-DoD Civil Service Employee.

This will cause incorrect information to populate in DEERS and you will have to restart the application process over. For non-DoD contractors, use the Non-DoD Civil Service Employee Personnel Category.

6. In the **Eligibility Expiration Date** field (card expiration date), type the appropriate date.

Note: If the Applicant already has a valid government credential with the same expiration date, you will receive a warning message in TASS.

7. If applicable, type the contract number and contract end date in the **Contract Number** and **Contract End Date** fields.

Note: If you select the Personnel Category Affiliated Volunteer, Non-DoD Civil Service Employee, Foreign Affiliate, OCONUS Local Hire, or Non-Federal Agency Civilian Associate, the **Contract Number** and **Contract End Date** fields will not appear on the form.

You should use the following recommended DODAAC contract number 13-character format; this only applies to DODAAC contract numbers:

- DODAAC (6 character alphanumeric)
- Fiscal year (2 character numeric)
- Procurement instrument type code (1 character alphabetic)
- Serialized identifier (4 character alphanumeric)

Note: If you do not use the recommended 13-character format, TASS gives you a warning message. However, TASS will allow you to proceed with the application process.

Important: Not all contract numbers fit the 13-character format.

Note: As a TA you are authorized to edit the Contract Number and Duty Location for an “Approved” or “Issued” record under the following conditions:

- Applicant’s Personnel Category remains unchanged
- No change to the Sponsoring Organization
- Eligibility expiration date and other personal information in the application remains unchanged
- “Issued” CACs must have a remaining validity of more than 30 days

8. Review the information for accuracy.

Note: The Applicant cannot change fields marked with a cross (“†”) once you submit the application. In order to make application changes you need to return the application back to the Applicant prior to approval.

9. Click **Submit**.

- Result: The *Create New Application Account—Confirm* screen appears (see Figure 38).

Figure 38. Create New Application Account—Confirm Screen

Application Data

Applicant Information:

Last Name:	Smith
First Name:	Mary
Middle Name:	
Cadency Name:	
Person Identifier:	XXXXXXXX (Social Security Number)
Date Of Birth:	02/03/1984 (MM/DD/YYYY)
Primary Email:	smith_mary@gov.com
Personnel Category:	DoD and Uniformed Service Contractor
Organization:	D
Eligibility Expiration Date:	10/14/2013 (MM/DD/YYYY)

Contract Information:

Contract Number:	XXXXXX
Contract End Date:	10/14/2013 (MM/DD/YYYY)

Sponsor (TA):

Organization:	Department Of Defense
Telephone Number:	5075551234
Office Name:	Sponsor Office
Street Address 1:	Main Street
Street Address 2:	
City:	Rochester
State:	MN
Zip Code:	0
Last four Zip Code:	0
Country:	US

No information was found in the DoD Person Data Repository for this contractor. Please review the **Name**, **Date of Birth**, and **Person Identifier** and confirm that to the best of your knowledge this contractor has had no previous affiliation with the DoD. Possible affiliations would include:

- Current Contractor requesting a CAC re-issuance.
- Contractor for another DoD Service or Agency.
- Current or previous Reserve/Guard Member.
- Military Retiree.
- Current or previous DoD Civilian Employee.
- Dependent of Military Member.

If this contractor is, to the best of your knowledge, new to the DoD, please click (Confirm) below.

Common Access Card (CAC) Applicants: I verify that an FBI fingerprint check with favorable results has been completed and a National Agency Check with Inquiries (NACI), or a DoD determined equivalent investigation, or greater, has been submitted to the Office of Personnel and Management (OPM). For Non-U.S. Persons - a successfully adjudicated NACI or equivalent has been completed.

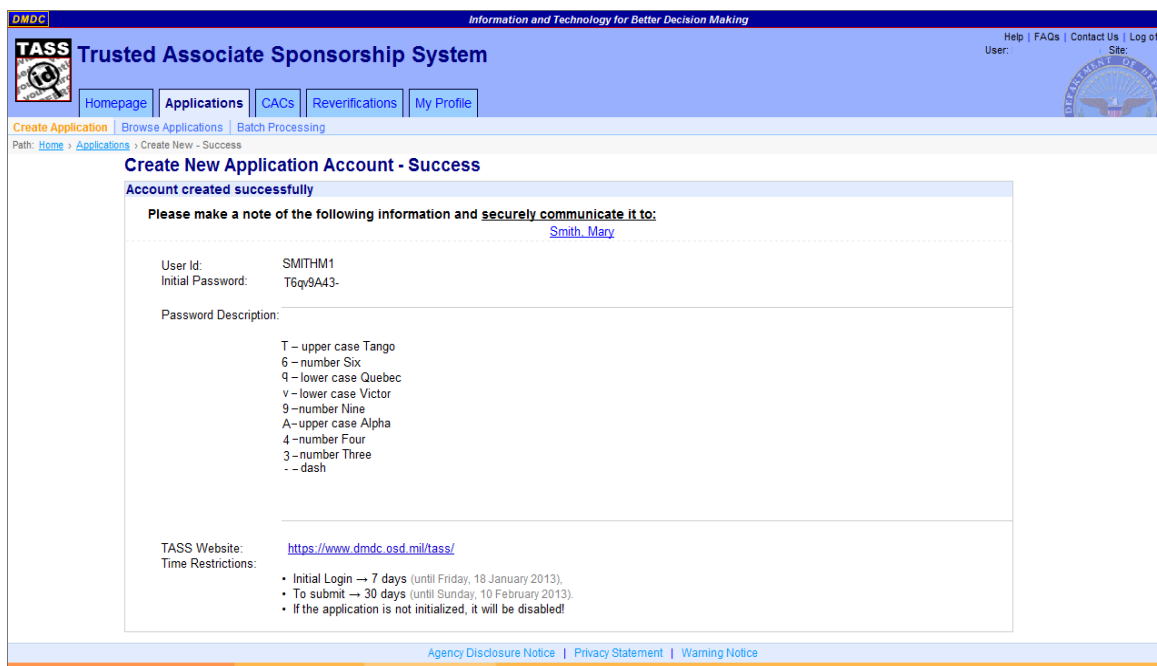
Volunteer Logical Access Credential (VoLAC) Applicants: I verify that an FBI fingerprint check with favorable results has been completed and a National Agency Check (NAC) has been submitted to the OPM.

Teslin Card Applicants: I verify that the appropriate level of identity and/or background vetting has been completed consistent with the organizational mission.

Note: TASS will track all TAs associated with a given record. However, TASS will only display the information of up to **three** TAs, if applicable. Only the present or current TA will be able to view the information of the TA that created the initial or original application, the TA information that possessed the record directly before them, and the present TA (their own) information.

10. Review the application for accuracy, and click **Edit** to return to the previous screen to make any needed changes (see Figure 38).
 11. Click the check box to certify that you have verified the Applicant's vetting.
 12. After you have confirmed the accuracy of the information, click **Confirm**.
- **Result:** The *Create New Application Account—Success* screen appears (see Figure 39). TASS responds by providing critical login (user ID and password) information for the Applicant. It is important to make note of the information on this screen and to securely communicate this information to the Applicant, including the following:
- Applicant's user ID
 - Applicant's password
 - Number of days that the Applicant has to login to TASS
 - Length of time allotted to complete and submit the application

Figure 39. Create New Application Account—Success Screen



Note: If the attempt to create a new account fails, the *Create Account Failure* screen appears (see Figure 40). This screen provides an explanation of the failure. Scroll to the bottom of the screen to see a **Reset** button to clear the typed changes.

Figure 40. Create Account Failure



13. The Applicant must log in to TASS and complete the newly created application. In a secure manner, notify the Applicant of the TASS application URL (<https://www.dmdc.osd.mil/tass>) and the information (user ID and initial password) noted in step 12 from the *Create New Application Account—Success* screen.

Note: Use the alphanumeric character translation table, **Appendix G**, to securely communicate Applicant password information.

Note: TASS does not automatically notify the Applicant by email when you create his or her account. Once you create the application, the Applicant has seven days to conduct an initial log in to TASS; otherwise, the TASS application automatically disables the account. If that occurs and the Applicant still has a valid requirement for a government credential you must create a new application. After his or her first login, the Applicant has 30 days to submit the application, or the TASS application automatically disables the account.

7.5 Reusing an Existing Application to Create a New Application

Use this section to create new applications for Applicants seeking government credentials based on existing applications.

7.5.1 Prerequisites

Before you can reuse an existing application to create a new application, you must perform the following prerequisite steps:

- Determine and verify the Applicant has a valid requirement for a government credential
- Perform necessary actions and checks according to DoD instructions and installation policies, guidelines, and procedures
- Identify an existing application to reuse
- Confirm the following Applicant information:
 - Last Name
 - First Name
 - Middle Name
 - Cadency Name
 - Person Identifier (SSN, FIN, ITIN)
 - Date of Birth
 - Primary Email
 - Personnel Category
 - Eligibility Expiration Date
 - Organization
 - Contract number and end date, if applicable

Note: Under no circumstances can a Contractor also be enrolled in TASS as TASM or TA.

7.5.2 Reusing an Application

To reuse an existing application as the basis to create a new application, perform the following steps:

1. Click the **Applications** tab.
2. Select the following search criteria check boxes:
 - **Expired**
 - **Issued**
 - **Current (C)**
 - **Archived (A)**

Note: TASS supports the ability to archive old records and to conduct a search of archived records.

3. Click **Search**.
- Result: The *Browse Applications* search results screen appears (see Figure 41).

Figure 41. Browse Applications Screen—Search Results

The screenshot shows the TASS interface with search criteria for 'Expired' status. Below the search criteria is a table with 2 records found. The table has columns: Full Name, Person ID, Status, Status Date, Contract Number, Eligibility Expiration Date, and Links. The 'Expired' status is highlighted in the search criteria, and the 'Reuse' link in the table is also highlighted with a red box.

Full Name	Person ID	Status*	Status Date	Contract Number	Eligibility Expiration Date	Links (Reset Password, Disable, ...)
Brown, Jane	XXXXXXXXXX	Expired	2010-Jan-12	XXXXXXXXXX	2010-Dec-31	DEERS Compare
Doe, John	XXXXXXXXXX	Expired	2010-May-04	XXXXXXXXXX	2010-Dec-31	DEERS Compare , Reuse

4. Choose the application eligible to reuse by clicking the **Reuse** link.

Note: TASS only displays a Reuse link for those records applicable for reuse.

- Result: The *Reuse Old Record to Create New Application* screen appears (see Figure 42).

Figure 42. Reuse Old Record to Create New Application Screen

The screenshot shows the 'Reuse Old Record to Create New Application' screen. It includes a 'Messages' section with three bullet points: 'Existing data has been reused to pre-populate form', 'Note some data fields have been reset (e.g. Expiration date, Contract Number)', and 'Other data may need to be updated by Applicant'. Below the messages is the 'Application Data' form with fields for Applicant Information and Personnel Category.

Messages:

- Existing data has been reused to pre-populate form
- Note some data fields have been reset (e.g. Expiration date, Contract Number)
- Other data may need to be updated by Applicant

Application Data

Applicant Information:

Last Name:† Jones
 First Name:† John
 Middle Name:†
 Cadency Name: Please Select
 Person Identifier:† XXXXXXXX Social Security Number
 Date Of Birth:† 02/03/1984
 Home Email:† jones_john@gov.com
 Work Email:† jones_john@gov.com

Personnel Category:†

- Affiliated Volunteers (requiring DoD Network access)
- DoD and Uniformed Service Contractor
- Foreign Affiliate
- Non-DoD Civil Service Employee
- Non-Federal Agency Civilian Associate
- Non-US Non-Appropriated Fund (NAF) Employee
- OCONUS Hire
- Other Federal Agency Contractor

Note: TASS will track all TAs associated with a given record. However, TASS will only display the information of up to **three** TAs, if applicable. Only the present or current TA will be able to view the information of the TA that created the initial or original application, the TA information that possessed the record directly before them, and the present TA (their own) information.

5. Edit the information as necessary and click **Submit**.

Note: If the Applicant already has a valid government credential with the same expiration date, you will receive a warning message in TASS and will not be able to create the application.

- Result: The *Reuse Old Record to Create New Application—Confirm* screen appears (see Figure 43).

Figure 43. Reuse Old Record to Create New Application—Confirm Screen

DMDC Information and Technology for Better Decision Making

TASS Trusted Associate Sponsorship System

Help | FAQs | Contact Us | Log off
User:Suzhanna T. Sapoc Site:XXXXXX

DEPARTMENT OF DEFENSE

Homepage Applications CACs Reverifications My Profile

Create Application Browse Applications Batch Processing

Path: Home > Browse Applications > Reuse/Create New

Reuse Old Record to Create New Application - Confirm

[Instructions](#) (Help with this form) OMB No. 0704-0415

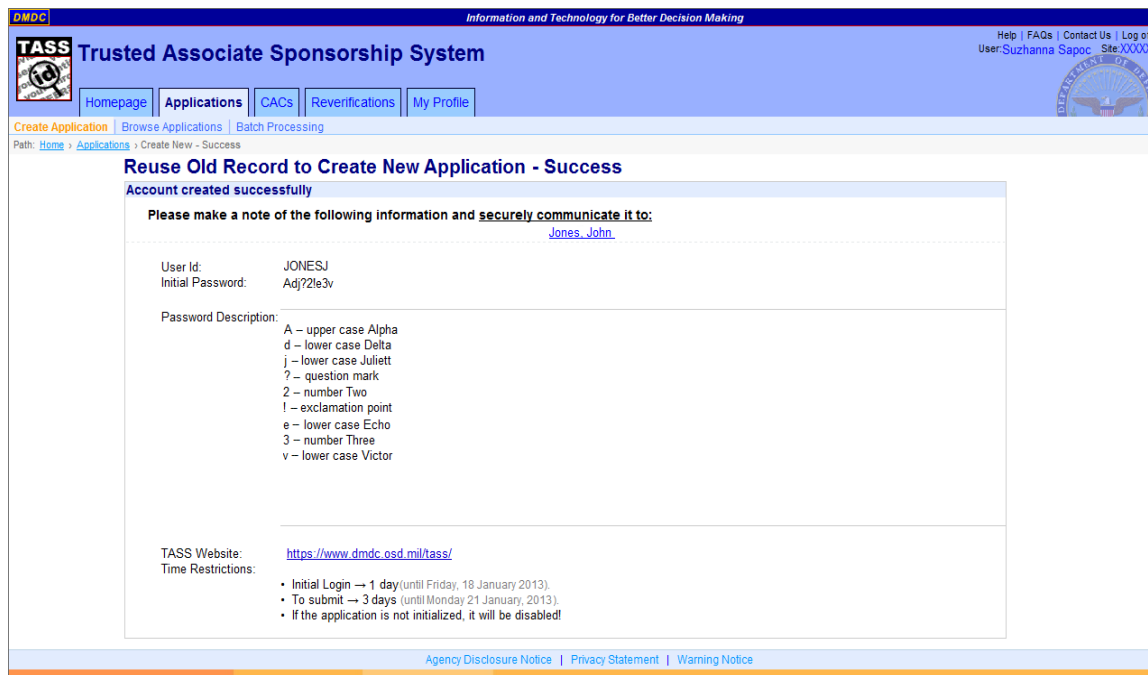
Application Data	
Applicant Information:	
Last Name:†	Jones
First Name:†	John
Middle Name:	
Cadency Name:	
Person Identifier:†	XXXXXXXX
Person Identifier Type:†	Social Security Number
Date Of Birth:†	02/03/1984
Home Email:†	jones_john@gov.com
CAC certificate Email:†	jones_john@gov.com
Personnel Category:†	DoD and Uniformed Service Contractor
Organization:	Department Of Defense
Eligibility Expiration Date:	01/19/2013
Contract Information:	
Contract Number:	XXXXXX
Contract End Date:	01/19/2013 (MM/DD/YYYY)
Sponsor (TA):	

6. Review the application for accuracy. Scroll to the bottom of the screen and click **Edit** to return to the previous screen to make any needed changes.
7. Click the check box to certify that you have verified the Applicant's vetting.
8. After you have confirmed the accuracy of the information, click **Confirm**.

- Result: The *Reuse Old Record to Create New Application—Success* screen appears (see Figure 44). TASS responds by providing critical login (user ID and password) information for the Applicant. It is important to make note of the important information on this screen, and securely communicate it to the Applicant, including the following:

- Applicant's user ID
- Applicant's password
- TASS website
- Number of days that the Applicant has to log in to TASS
- Length of time allotted to complete and submit the application

Figure 44. Reuse Old Record to Create New Application—Success Screen



9. In a secure manner, notify the Applicant of the TASS application URL (<https://www.dmdc.osd.mil/tass>) and the information noted in step 8 from the *Reuse Old Record to Create New Application—Success* screen (see Figure 44).

Note: Use the alphanumeric character translation table, **Appendix G**, to securely communicate Applicant password information.

Important: TASS does not automatically notify the Applicant by email when you create his or her account. Once you create the application, the Applicant has seven days to conduct an initial log in to TASS; otherwise, the TASS application automatically disables the account. If that occurs and the Applicant still has a valid requirement for a government credential, you must create a new application. After his or her first login, the Applicant has 30 days to submit the application, or the TASS application automatically disables the account.

7.6 Browsing Applications

This section provides information on how to search for and view applications.

7.6.1 Searching for an Application

To search for an application, perform the following steps:

1. Click the **Applications** tab.
 - Result: The *Browse Applications* screen appears with search results displayed for the **Search Criteria** default options already selected (see Figure 45).

Figure 45. Browse Applications Screen

2 Records found, displaying all Records.

Full Name	Person ID	Status	Status Date	Contract Number	Eligibility Expiration Date	Links [Reset Password, Disable, ...]
Ripp, Dennis		In Progress (C)	2013-Jan-11	XXXXXXXXXX	2014-Feb-20	Maintenance
Strawberry, Suzie		Submitted (C)	2012-Dec-20	XXXXXXXXXX	2013-Feb-20	Maintenance , Approve

2 Records found, displaying all Records.

Agency Disclosure Notice | Privacy Statement | Warning Notice

2. To change the results, choose one or more of the following *Search Criteria* options:

- Select one or more of the **Current**, **Closed**, **Completed**, or **Record Selection Status** check boxes
- Click **Select All** to select all of the application status check boxes
- Type a full or partial last name in the **Last Name** field

Note: TASS supports the ability to archive old records and to conduct a search of archived records.

3. Click **Search**.

- Result: The *Browse Applications* search results screen appears, (see Figure 46).

Note: You can control the number of records shown on the page by choosing a number from the **Per page** drop-down box (see Figure 46).

Figure 46. Browse Applications Screen—Search Results

The screenshot shows the TASS (Trusted Associate Sponsorship System) interface. At the top, there is a navigation bar with links for Home, Applications, CACs, Reverification, and My Profile. Below this is a search criteria section with four groups of checkboxes: Current (In Progress, Submitted, Returned), Closed (Rejected, Expired), Completed (Approved, Issued, Completed), and Record Selection Status (Current (C), Archived (A)). There are input fields for Person ID, Applicant Last Name (R), Applicant First Name, and Contract Number. A 'Search' button is located below the search criteria. Below the search results, there is a table with columns: Full Name, Person ID, Status, Status Date, Contract Number, Eligibility Expiration Date, and Links. The table contains two rows of data: Ripp, Dennis (In Progress (C), 2013-Jan-11) and Ryan, Kelly (Submitted (C), 2012-Dec-20). A red box highlights the 'Per page: 100' dropdown menu, and an arrow points to a callout box that says 'Adjusts the number of records displayed per page'.

4. Use the *Browse Applications* search results screen to do the following:
 - View an application, as described in **Section 7.6.2 (Viewing an Application)**
 - Compare an application with the Applicant’s record in DEERS, as described in **Section 7.6.3 (Comparing an Application with DEERS)**
 - Change the status of an application, as described in **Section 7.7 (Maintaining an Application)**

7.6.2 Viewing an Application

You cannot change the status of an application from the *View Applications* screen; see **Section 7.7 (Maintaining an Application)**.

To view an application, perform the following steps:

1. Complete the steps in **Section 7.6.1 (Searching for an Application)**.
2. Click the **Full Name** of the application.

➤ **Result:** The *View Application* screen appears (see Figure 47).

Note: From this screen, you can compare an Applicant's record with the DEERS record by clicking **DEERS Compare**. You can perform a **DEERS Compare** for all Search Criteria collection types (Current, Closed, Completed, Record Selection Status) by selecting the Applicant's **Full Name** column from the Applicant's record. DEERS may or may not contain data to compare.

Figure 47. View Application Screen

DMDc
Help | FAQs | Contact Us

Trusted Associate Sponsorship System

View Application
OMB No. 0704-0415

Status:	
Status:	Submitted
Status Date:	12/05/2012
Created Date:	12/05/2012
Submitted On:	12/05/2012
Last Accessed:	12/05/2012
Archived:	No
Card Information (Original):	
Card Status:	INVALID STATE
Type:	Common Access Card
Issued Date:	NA
Card Expiration Date:	NA
User Id:	STEWLITTLE
Applicant Information:	
Last Name: [†]	Little
First Name: [†]	Stew
Middle Name: ^{**}	
Cadency Name:	
Person Identifier: [†]	XXXXXXXXXX
Person Identifier Type: [†]	Social Security Number
Date Of Birth: [†]	01/01/1970 (MM/DD/YYYY)
Sex:	Male
Country of Citizenship:	US
U.S. Citizenship Status:	U.S. Citizen
Birth State:	AL
Birth Country:	US
Personnel Category: [†]	Non-DoD Civil Service Employee
Government Agency: [†]	Department of Justice
Organization:	Army
Eligibility Expiration Date:	01/01/2015 (MM/DD/YYYY)
Home Address:	
Street Address 1:	5555 Kings Park Rd
Street Address 2:	
City:	Forrest
State:	AL
Zip Code:	12345
Last four Zip Code:	1234
Country:	US
Contact Information:	
Primary Email: ^{†*}	ssapoc@hotmail.com
Duty Location:	
City:	Forrest
State:	AL
Country:	US
Sponsor (TA): (TASS displays only up to 3 sponsor transfers)	
Current TA:	Sapoc_Suzhanna
Effective Date:	12/05/2012
Organization:	Department Of Defense
Telephone Number:	2345678901
Office Name:	KBR
Street Address 1:	1111 Ben Dr.
Street Address 2:	
City:	Houston
State:	TX
Zip Code:	23456
Last four Zip Code:	1111
Country:	US

DEERS Compare
Close Window

[†] To correct these errors the application would need to be Disabled or Rejected, and a new application created (with corrected values).

^{*} Email address used for TASS notifications to Applicant.

^{**} Leave this field blank if the applicant has no middle name.

[Agency Disclosure Notice](#) | [Privacy Statement](#) | [Warning Notice](#)

7.6.3 Comparing an Application with DEERS

New Applicants who have never received a government credential may not appear in the DEERS database until their TA approves their application.

To compare an Applicant's record with the DEERS record, perform the following steps:

1. Complete the steps in **Section 7.6.1 (Searching for an Application)**.
 2. Click **DEERS Compare**.
- Result: The *Compare to DEERS* screen appears (see Figure 48).

Figure 48. Compare to DEERS Screen

	TASS Data:	DEERS Data:
Applicant Information:		
Last Name:	Doe	Doe
First Name:	John	John
Middle Name:		
Cadency Name:		
Person Identifier:	XXXXXXXX	XXXXXXXX
Person Identifier Type:	Social Security Number	Social Security Number
Organization:	Department Of Defense	D
Date Of Birth:	01/01/1970 (MM/DD/YYYY)	01/01/1970
Sex:	Male	M
U.S. Citizenship Status:	U.S. Citizen	U.S. Citizen
Birth Country:	US	N/A
Personnel Category: (Government Agency)	DoD and Uniformed Service Contractor (Unspecified)	DoD and Uniformed Service Contractor (Department of Defense)
Home Address:		
Street Address 1:	1313 Mockingbird Lane	1313 Mockingbird Lane
Street Address 2:		
City:	Rochester	Rochester
State:	MN	MN
Zip Code:	00000	00000
Country:	US	US

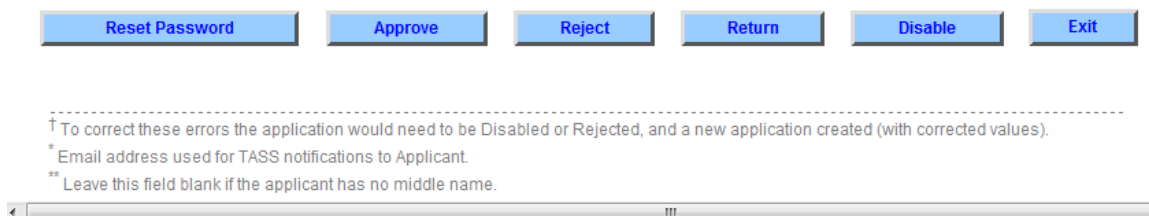
7.7 Maintaining an Application

You can maintain and change the status of an application from the *Application View/Maintenance* screen. To view this screen, click **Maintenance** from the *Links* column on the *Browse Applications* screen. Use the buttons at the bottom of the *View/Maintenance* screen to change the status of an application. The actions available depend on the application’s status (see Table 2, “Actions Available According to Application Status,” and Figure 49).

Actions Available According to Application Status

		Status of the Application							
		In Progress	Approved	Submitted	Returned	Completed	Rejected	Issued	Expired
Buttons/Actions	Disable	Yes	Yes	Yes	Yes	Yes	No	No	No
	Approve	No	No	Yes	No	Yes	No	No	No
	Return	No	No	Yes	No	Yes	No	No	No
	Reject	No	No	Yes	No	Yes	No	No	No
	Reuse	No	No	No	No	No	No	Yes	Yes
	Reset Password	Yes	Yes	Yes	Yes	Yes	No	No	No

Figure 49. Button Row—Submitted Application



7.7.1 Approving an Application

To approve an application, perform the following steps:

1. Click the **Applications** tab.
 - Result: The *Browse Applications* screen appears.
2. Select the **Submitted** check box and click **Search**.
 - Result: The search results display in the record list at the bottom of the *Browse Applications* screen (see Figure 50).

Note: TASS supports the ability to archive old records and to conduct a search of archived records.

Note: You can adjust the number of records shown per page by changing the number in the **Per page** drop-down list.

Figure 50. Browse Applications Screen—Submitted Applications

The screenshot shows the TASS web interface. At the top, there is a navigation bar with 'Home', 'Applications', 'CACs', 'Reverifications', and 'My Profile'. Below this is a search criteria section with four filters: 'Current' (checked for In Progress, Submitted, Returned), 'Closed' (unchecked for Rejected, Expired), 'Completed' (unchecked for Approved, Issued, Completed), and 'Record Selection Status' (checked for Current (C), unchecked for Archived (A)). Search fields for Person ID, Applicant Last Name (R), Applicant First Name, and Contract Number are present. A 'Search' button is located below the fields. Below the search section, a table displays 2 records. The table has columns for Full Name, Person ID, Status, Status Date, Contract Number, Eligibility Expiration Date, and Links. The 'Approve' link in the 'Links' column for the second record is highlighted with a red box and an arrow.

Full Name	Person ID	Status	Status Date	Contract Number	Eligibility Expiration Date	Links (Reset Password, Disable, ...)
Ripp, Dennis		In Progress (C)	2013-Jan-11	XXXXXXXXXX	2014-Feb-20	Maintenance
Ryan, Kelly		Submitted (C)	2012-Dec-20	XXXXXXXXXX	2013-Feb-20	Maintenance Approve

3. DMDC strongly recommends that you click **Maintenance** from the Links column and make all required data verifications and checks before clicking **Approve**.

4. Click **Approve**.

➤ Result: The *Confirm Application Approval* screen appears (see Figure 51).

Figure 51. Confirm Application Approval

Application Data

Applicant Information:
 Last Name:† Smith
 First Name:† John
 Middle Name: James
 Cadency Name:
 Person Identifier:† XXXXXXXX (Social Security Number)
 Date Of Birth:† 01/01/1966 (MM/DD/YYYY)
 Primary Email:†+ smith_john@gov.com
 Personnel Category:† DoD and Uniformed Service Contractor
 Service: Department Of Defense
 Organization: D
 Eligibility Expiration Date: 12/31/2011 (MM/DD/YYYY)

Contract Information:
 Contract Number: XXXX-XXXXX
 Contract End Date: 12/31/2011 (MM/DD/YYYY)

Sponsor (TA):
 Organization: Department Of Defense
 Telephone Number: 5075551234
 Office Name: Sponsor Office
 Street Address 1: Main Street
 Street Address 2:
 City: Rochester
 State: MN
 Zip Code: 0
 Last four Zip Code: 0
 Country: US

No information was found in the DoD Person Data Repository for this contractor. Please review the **Name**, **Date of Birth**, and **Person Identifier** and confirm that to the best of your knowledge this contractor has had no previous affiliation with the DoD. Possible affiliations would include:

- Current Contractor requesting a CAC re-issuance.
- Contractor for another DoD Service or Agency.
- Current or previous Reserve/Guard Member.
- Military Retiree.
- Current or previous DoD Civilian Employee.
- Dependent of Military Member.

If this contractor is, to the best of your knowledge, new to the DoD, please click (Approve) below. Approving this application will add this contractor to the DoD Person Data Repository and authorize them to receive a Common Access Card.

I Accept And Agree
 The government issued credential is the property of the U.S. Government and shall not be retained by the cardholder upon expiration, replacement, or when the DoD affiliation of the employee has been terminated. The Contractor and TA have the responsibility to ensure the government issued credential is retrieved in accordance with local command or installation procedures. Unauthorized possession of an official credential, like a CAC, can be prosecuted criminally under [section 701, title 18, United States Code](#).

I Accept And Agree
Common Access Card (CAC) Applicants: I verify that an FBI fingerprint check with favorable results has been completed and a National Agency Check with Inquiries (NACI), or a DoD determined equivalent investigation, or greater, has been submitted to the Office of Personnel and Management (OPM). For Non-U.S. Persons - a successfully adjudicated NACI or equivalent has been completed.

I Accept And Agree
Volunteer Logical Access Credential (VoLAC) Applicants: I verify that an FBI fingerprint check with favorable results has been completed and a National Agency Check (NAC) has been submitted to the OPM.

Teslin Card Applicants: I verify that the appropriate level of identity and/or background vetting has been completed consistent with the organizational mission.

5. Read United States Code section 701, title 18, and, if you accept and agree, select the **I Accept And Agree** check box.

6. Click the check box to certify that you have verified the Applicant's vetting.
 7. Click **Approve**.
- Result: The *Application Approval Status* screen appears (see Figure 52).

Figure 52. Application Approval Status Screen



Note: TASS sends an email to the Applicant and a copy to you stating that the application was approved and instructing the Applicant to go to the nearest RAPIDS Issuing Facility with two forms of identification for card issuance (see Figure 53).

Figure 53. Email to Applicant Following Approval



At the RAPIDS issuance workstation, an operator updates the DEERS database once the Applicant receives his or her card.

A TASS offline process provides DEERS updates to the TASS database with the appropriate information. For example, when a card is issued, this process changes the TASS application status from 'Approved' to 'Issued.'

Note: TAs are authorized to edit the Contract Number and Duty Location for an "Approved" or "Issued" record under the following conditions:

- Applicant's Personnel Category remains unchanged

-
- No change to the Sponsoring Organization
 - Eligibility expiration date and other personal information in the application remains unchanged
 - An “Issued” CAC has a remaining validity of more than 30 days

7.7.2 Returning an Application

If you find incorrect or incomplete information on a submitted application, you can return the application to the Applicant for corrections. To return an application to an Applicant, perform the following steps:

1. Click the **Applications** tab.
 - Result: The *Browse Applications* screen appears with search results displayed for the **Search Criteria** default options already selected.
2. This process allows flexibility in selecting various options. For example, if you want to select only the applications that have been submitted, select only the **Submitted** check box and click **Search**.
 - Result: The search results display in the lower portion of the *Browse Applications* screen (see Figure 54).

Note: TASS supports the ability to archive old records and to conduct a search of archived records.

Figure 54. Browse Applications Screen—Submitted Applications

The screenshot shows the TASS 'Browse Applications' interface. At the top, there are navigation tabs: 'Homepage', 'Applications', 'CACs', 'Reverifications', and 'My Profile'. Below the tabs, there are search criteria sections for 'Current', 'Closed', 'Completed', and 'Record Selection Status'. The 'Current' section has 'Submitted' checked. Below the search criteria are input fields for 'Person ID', 'Applicant Last Name', 'Applicant First Name', and 'Contract Number'. A 'Search' button is located below these fields. Below the search area, a table displays search results. The table has columns: 'Full Name', 'Person ID', 'Status', 'Status Date', 'Contract Number', 'Eligibility Expiration Date', and 'Links'. One record is shown for 'Jones, John' with status 'Submitted' and a 'Maintenance' link highlighted in a red box. An arrow points from the 'Maintenance' link to the right.

Full Name	Person ID	Status	Status Date	Contract Number	Eligibility Expiration Date	Links
Jones, John	XXXXXXXXXX	Submitted	2009-Dec-17	12355	2010-Dec-31	Maintenance Approve

3. Click **Maintenance**.

- Result: The *Application View/Maintenance* screen appears (see Figure 55).

Figure 55. Application View/Maintenance Screen

DMDC Information and Technology for Better Decision Making

TASS Trusted Associate Sponsorship System

Help | FAQs | Contact Us | Log off
User: Suzhanna Sapoc Site: xxxxxx

Homepage Applications CACs Reverifications My Profile

Create Application Browse Applications Batch Processing

Path: Home > Applications > Browse Applications > Application Maintenance

Application View/Maintenance

[Instructions \(Help with this form\)](#) OMB No. 0704-0415

Status:

Status:	Submitted
Status Date:	12/05/2012
Created Date:	12/05/2012
Submitted On:	12/05/2012
Last Accessed:	12/05/2012
Archived:	No

Card Information (Original):

Card Status:	INVALID STATE
Type:	Common Access Card
Issued Date:	NA

Sponsor (TA): (TASS displays only up to 3 sponsor transfers)

Current TA:	Sapoc, Suzhanna
Effective Date:	12/05/2012
Organization:	Department Of Defense
Telephone Number:	2345678901
Office Name:	KBR
Street Address 1:	1111 Ben Dr.
Street Address 2:	
City:	Houston
State:	TX
Zip Code:	23456
Last four Zip Code:	1111
Country:	US

[Reset Password](#) [Approve](#) [Reject](#) [Return](#) [Disable](#) [Exit](#)

† To correct these errors the application would need to be Disabled or Rejected, and a new application created (with corrected values).
* Email address used for TASS notifications to Applicant.
** Leave this field blank if the applicant has no middle name.

4. Scroll to the bottom of the screen and click **Return**.

➤ Result: The *Return Application* screen appears (see Figure 56).

Figure 56. Return Application Screen

The screenshot shows the TASS web interface. At the top, there's a navigation bar with 'Home', 'Applications', 'CACs', 'Reverifications', and 'My Profile'. The main content area is titled 'Return Application' and contains a form for returning an application to an applicant for corrections. The form has two radio buttons for selecting a reason. The second option is selected. Below the radio buttons is a text area for optional comments, which is highlighted with a red box. At the bottom of the form are three buttons: 'Return Application', 'Reset', and 'Cancel'. The footer of the page contains links for 'Agency Disclosure Notice', 'Privacy Statement', and 'Warning Notice'.

5. Select the radio button that most closely describes the reason you are returning the application to the Applicant.
 6. **Optional:** Type any clarifying comments in the **Comments** field.
 7. Click **Return Application**.
- Result: TASS sends an email to the Applicant and a copy to you. The *Browse Applications* screen reappears.

7.7.3 Rejecting an Application

Rejecting an application permanently inactivates the application. To reject an application, perform the following steps:

1. Select the **Applications** tab.
- Result: The *Browse Applications* screen appears.
2. Select the **Submitted** check box and click **Search**.
- Result: The search results display in the lower portion of the *Browse Applications* screen (see Figure 54).
3. Click **Maintenance**.
- Result: The *Application View/Maintenance* screen appears (see Figure 55).
4. Click **Reject**.
- Result: The *Reject Application* screen appears (see Figure 57).

Figure 57. Reject Application Screen



5. Select the radio button that most closely describes the reason you are rejecting the application.
 6. **Optional:** Type any clarifying comments in the **Comments** field.
 7. Click **Reject Application**.
- Result: TASS deactivates the application and sends an email to the Applicant and a copy to you.

7.7.4 Disabling an Application

Disabling an approved application terminates the personnel segment in DEERS associated with the approved application. In addition, if a current valid card exists, the card is marked for termination and the associated certificates are marked for revocation.

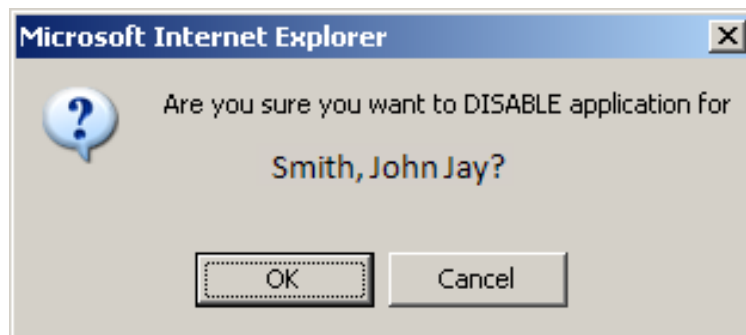
Note: After disabling an application, you can immediately create a new application for the Applicant; however, you must wait a day before approving the new application.

To disable an application, perform the following steps:

1. Select the **Applications** tab.
- Result: The *Browse Applications* screen appears.
2. Choose one or more of the following search criteria:
 - **Submitted** check box
 - **In Process** check box
 - **Approved** check box
 - Type a full or partial last name in the **Last Name** field
 3. Click **Search**.

- Result: The search results display in the lower portion of the *Browse Applications* screen (see Figure 54).
 4. Click the **Maintenance** link of the application you want to disable.
- Result: The *View/Maintenance* screen appears (see Figure 55).
 5. Click **Disable**.
- Result: The Disable Application confirmation message appears (see Figure 58).

Figure 58. Disable Application Message

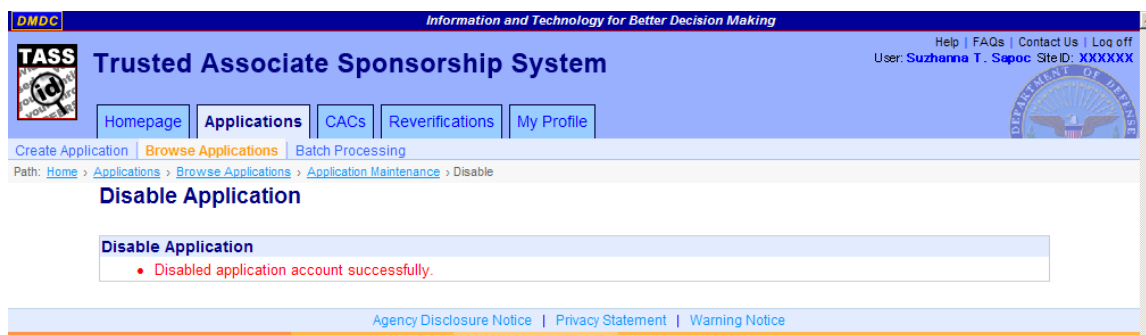


6. Click **OK**.

- Result: The *Disable Application* screen appears (see Figure 59).

Note: Disabling an application updates the corresponding DEERS personnel segment.

Figure 59. Disable Application Screen



7.7.5 Reusing an Application

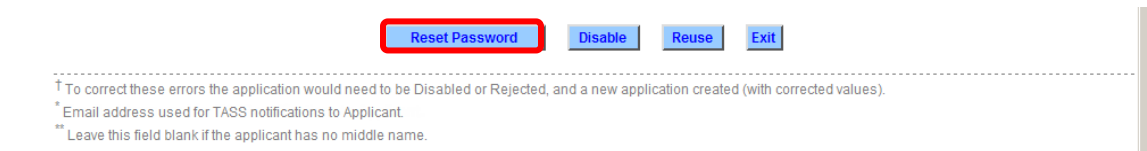
You can reuse an Issued or Expired application to create a new application; see **Section 7.5 (Reusing an Existing Application to Create a New Application)**.

7.7.6 Resetting an Applicant Password

To reset an Applicant password, perform the following steps:

1. Select the **Applications** tab.
 - Result: The *Browse Applications* screen appears.
2. Enter search criteria to locate the Applicant whose password you want to reset and click **Search**.
 - Result: The search results appear in the lower portion of the *Browse Applications* screen (see Figure 54).
3. Click the **Maintenance** link next to the record of the user whose password you want to reset.
 - Result: The *View/Maintenance* screen appears.
4. Click **Reset Password** at the bottom of the screen (see Figure 60).
 - The *Reset Password for Applicant* screen appears (see Figure 61).

Figure 60. Application View Maintenance Screen—Resetting a Password



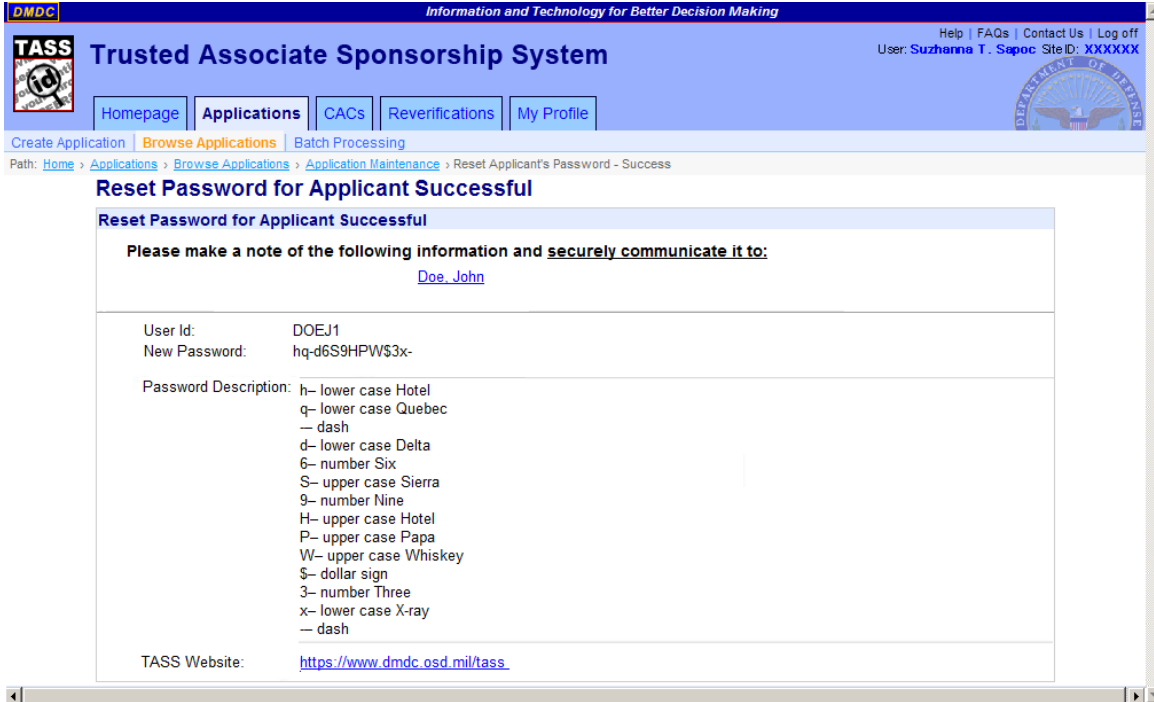
5. Note the name of the Applicant displayed on the *Reset Password for Applicant* screen (see Figure 61).

Figure 61. Reset Password for Applicant Screen



6. Click **Reset Password**.
 - The *Reset Password for Applicant Successful* screen appears (see Figure 62).

Figure 62. Successful Reset of Applicant Password



7. Note the new user ID and password and securely distribute it to the Applicant.

7.8 Maintaining a CAC

Use the information in this section to maintain the records of CAC (government credential) holders. For example, you can use this procedure to revoke a CAC, perform a DEERS Compare, or check the status of a CAC.

7.8.1 Searching for a CAC

To search for a CAC, perform the following steps:

1. Click the **CACs** tab.
 - Result: The *Browse CACs* screen appears (see Figure 63).

Figure 63. Browse CACs Screen

DMDC Information and Technology for Better Decision Making

TASS Trusted Associate Sponsorship System

Help | FAQs | Contact Us | Log off
User: Suzhanna Sapoc Site: XXXXXX

Homepage Applications CACs Reverification My Profile

Path: Home > CACs

Browse CACs - Approved Apps where CAC Issued

Search Criteria:

Last Name:

Issued Date From: To:

Card Status: VALID REVOKED NOT ISSUED EXPIRED

Record Selection Status: CURRENT (C) ARCHIVED (A)

No Records found. Modify your search and try again.

Agency Disclosure Notice | Privacy Statement | Warning Notice

2. Choose one or more of the following search criteria:

- Type a full or partial last name in the **Last Name** field
- Select a date range by entering a start date in the **Issued Date From** field and an end date in the **To** field
- Select one or more of the **Card Status** check boxes

Note: TASS supports the ability to archive old records and to conduct a search of archived records.

3. Click **Search**.

➤ Result: The *Browse CACs* search results screen appears (see Figure 64).

Figure 64. Browse CACs Screen—Search Results

Browse CACs - Approved Apps where CAC Issued

Search Criteria:

Last Name:

Issued Date From: To:

Card Status: VALID REVOKED NOT ISSUED EXPIRED

Record Selection Status: CURRENT (C) ARCHIVED (A)

2 Records found, displaying all Records.

Full Name	Person ID	Issued Date (Original)	Card Status	Eligibility Expiration Date	Contract Number	Verified	Links
Doe, John	XXXXXXXXXX		NOT ISSUED (C)	2014-Feb-20	XXXXXXXXXX		Revoke , DEERS Compare , Reuse
Smith, Mary	XXXXXXXXXX		NOT ISSUED (C)	2013-Feb-20	XXXXXXXXXX		Revoke , DEERS Compare , Reuse

Per page: 100

2 Records found, displaying all Records.

[Agency Disclosure Notice](#) | [Privacy Statement](#) | [Warning Notice](#)

The record list displays the following information:

- **Full Name**—the full name of the Applicant, formatted as last name, first name, middle name
- **Person ID**—the person identifier associated with the Applicant; for example, the Applicant’s SSN
- **Issued Date (Original)**—the date the card was issued
- **Card Status**—the card status: Revoked, Valid, Not Issued, or Expired
- **Eligibility Expiration Date**—the date on which the Applicant’s card expires
- **Contract Number**—the work contract number associated with the Applicant’s employment
- **Links**—context-specific links that allow you to view the Applicant’s DEERS record, reverify, revoke, or reuse the Applicant’s record

7.8.2 Reverifying a CAC

TASS requires you to reverify or revoke the Applicant CAC privileges by confirming and verifying the Applicant’s continued affiliation with the DoD and continued requirement for a government credential every 180 days for an active issued record. For information

on revoking a CAC, see **Section 7.8.3 (Revoking a CAC)**. If you do not reverify or revoke the record within 30 days of the expected reverification timeframe, TASS begins sending reverification notices 30 days prior to the CAC expiration date.

To reverify an Applicant's CAC record, perform the following steps:

1. Click the **Reverifications** tab.

➤ Result: The *Browse Reverifications* screen appears (see Figure 65).

Note: You can also click the *Reverify (Applicants)* link from the TA Dashboard section of the TA Homepage to access the *Browse Reverifications* screen.

Figure 65. Browse Reverifications Screen

DMDC Information and Technology for Better Decision Making

TASS Trusted Associate Sponsorship System

Help | FAQs | Contact Us | Log off
User: Suzhanna T. Sapoc Site:XXXXXX

Homepage Applications CACs **Reverifications** My Profile

Path: Home > Reverifications

Browse Reverifications

Search Criteria:

Last Name:

Reverify Due Date From: 10-19-2008 To: 12-18-2012 60 days from today: 12/18/2012 (set as default)

Status: Pending Revoked Reverified

Record Selection Status: Current (C) Archived (A)

Select Search to display results

Agency Disclosure Notice | Privacy Statement | Warning Notice

2. Choose one or more of the following search criteria:

- Type a full or partial last name in the **Last Name** field
- Select a date range by entering a start date in the **From** field and an end date in the **To** field
- Select one or more of the **Status** check boxes

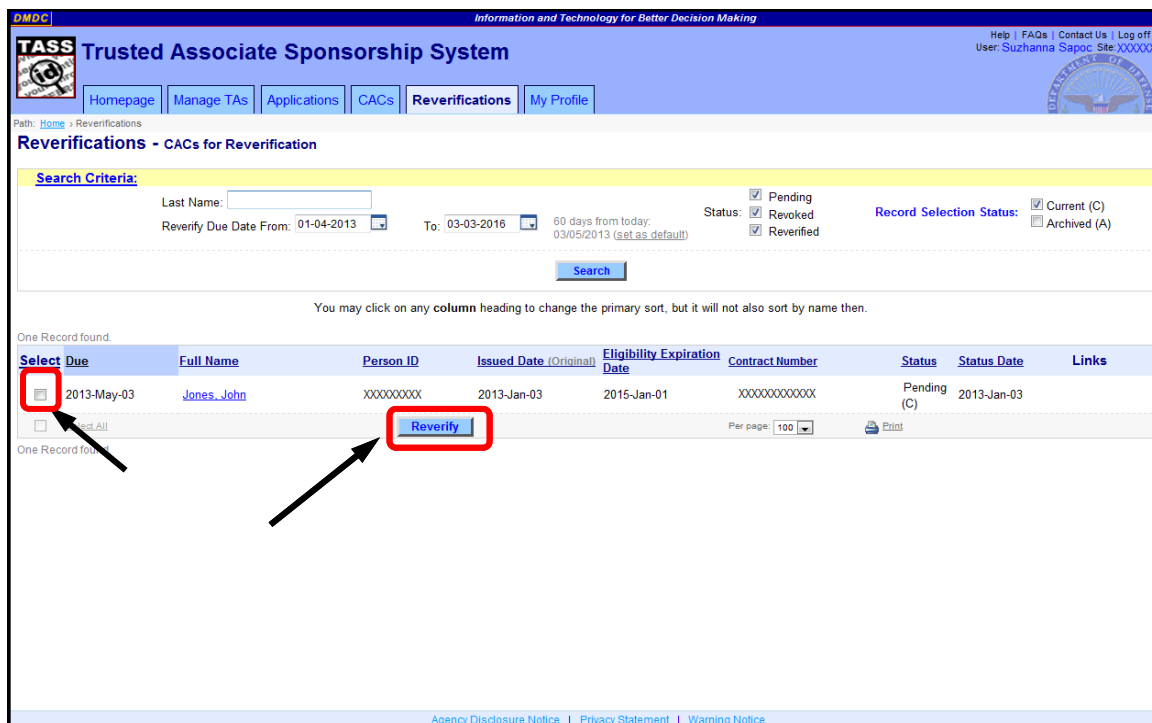
Note: TASS supports the ability to archive old records and to conduct a search of archived records.

3. Click **Search**.

➤ Result: The records meeting the search criteria appear in the lower half of the *Browse Reverifications* screen (see Figure 66).

Note: You can also search by the CAC record to locate Applicant records that require reverification; see **Section 7.8.1 (Searching for a CAC)**.

Figure 66. Reverification Screen—View Applicants

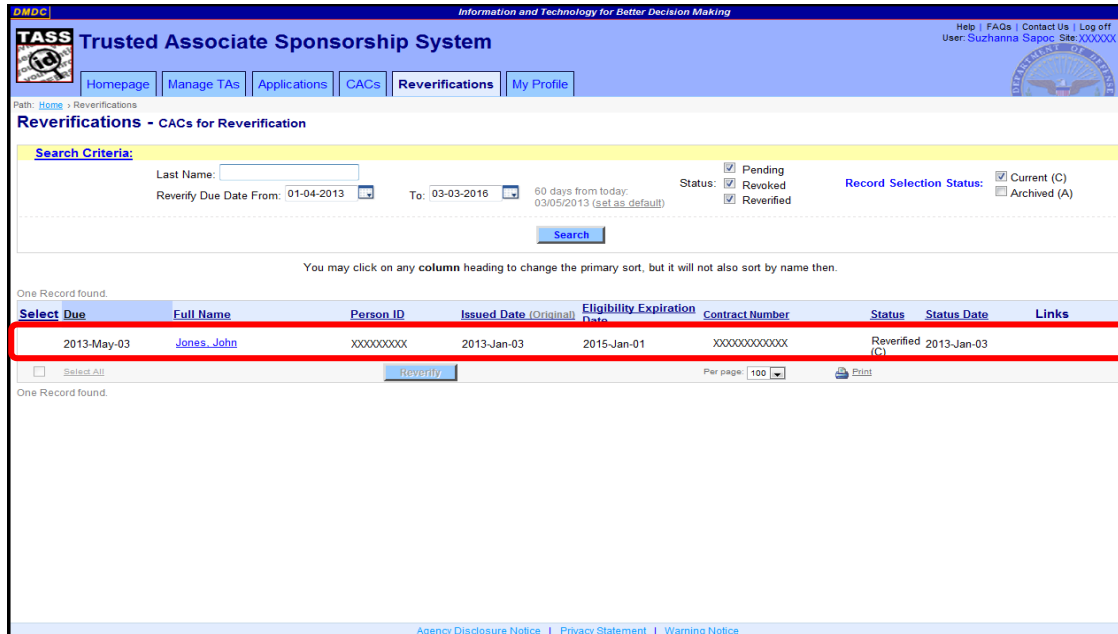


The record list displays the following information:

- **Due**—the reverification deadline
 - **Full Name**—the full name of the Applicant, formatted as last name, first name, middle name
 - **Person ID**—the person identifier associated with the Applicant, for example, the Applicant’s SSN
 - **Issued Date (Original)**—the date the card was issued
 - **Eligibility Expiration Date**—the date on which the Applicant’s card expires
 - **Contract Number**—the work contract number associated with the Applicant’s employer
 - **Links**—the **Revoke** link that allows you to mark the Applicant’s CAC record for revocation
 4. Select the check box to the left of the Applicant record(s) and click **Reverify**.
- **Result:** The Applicant’s status changes to ‘Reverified’ (see Figure 67).

Note: If, after 180 days, you have not reverified or revoked a record due for reverification, TASS will automatically revoke the CAC record.

Figure 67. Reverifications Screen—After Applicant Reverification



7.8.3 Revoking a CAC

After revoking an application, you can immediately create a new application for the Applicant; however, you must wait a day before approving the new application.

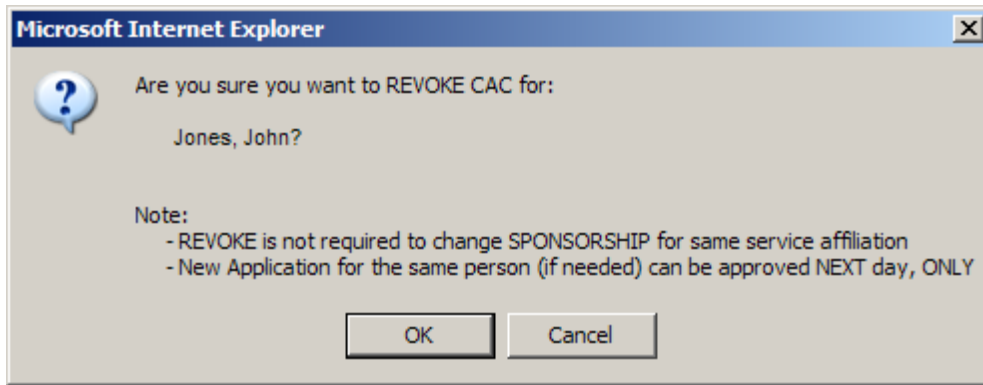
To revoke an Applicant's CAC record, perform the following steps:

1. Select the **Reverifications** tab.

Note: You can also search by CAC to locate Applicant records that require revocation; see **Section 7.8.1 (Searching for a CAC)**.

- Result: The *Browse Reverifications* screen appears (see Figure 65).
- 2. Select the **Select** check box for the Applicant and then click **Revoke** in the *Links* column.
- Result: A confirmation message appears (see Figure 68).

Figure 68. Confirm Revoke Request Message



3. Click **OK**.

➤ **Result:** The Applicant’s status changes to ‘Revoked’ (see Figure 69).

Note: An email notification will be sent to TAs and Applicants when an approved application is disabled.

Note: An email notification will be sent to TASMs, TAs, and Applicants when an issued application is expired, revoked, or terminated. The email notification shall note when the record was revoked and will give the reason for revocation, if available.

Figure 69. Reverifications Screen—Revoked CAC

Path: Home > Reverifications

Reverifications - CACs for Reverification

Search Criteria:

Last Name:

Reverify Due Date From: 01-04-2013 To: 03-03-2016 60 days from today: 03/05/2013 (set as default)

Status: Pending Revoked Reverified

Record Selection Status: Current (C) Archived (A)

You may click on any column heading to change the primary sort, but it will not also sort by name then.

One Record found.

Select	Due	Full Name	Person ID	Issued Date (Original)	Eligibility Expiration Date	Contract Number	Status	Status Date	Links
<input type="checkbox"/>	2013-May-03	Jones, John	XXXXXXXXXX	2013-Jan-03	2015-Jan-01	XXXXXXXXXXXXXX	Revoked (C)	2013-Jan-03	

Per page: 100 Print

One Record found.

Note: If, after 180 days, you have not reverified or revoked a record due for reverification, TASS will automatically revoke the CAC record.

7.9 High Volume Data Feed

This section describes how to use the High Volume Data Feed (HVDF) procedure within TASS. This procedure is also referred to interchangeably as the Batch Processing or Batch Upload feature. If your SPOC has approved your access, you can use HVDF to submit multiple new Applicant applications all at once using a DMDC predefined XML (eXtensible Mark-up Language) file.

Your SPOC requests access for you by nominating you to the DMDC TASS Program Office. Once DMDC accepts the nomination and establishes access capability, you have access to the Batch Processing function.

Batch Upload creates the new applications in your TASS TA account with a status of Submitted. You must review the applications to determine further action. You must revoke or reverify the active Applicant records every 180 days.

7.9.1 Prerequisites

Before you can use Batch Processing, you must meet the following prerequisite conditions:

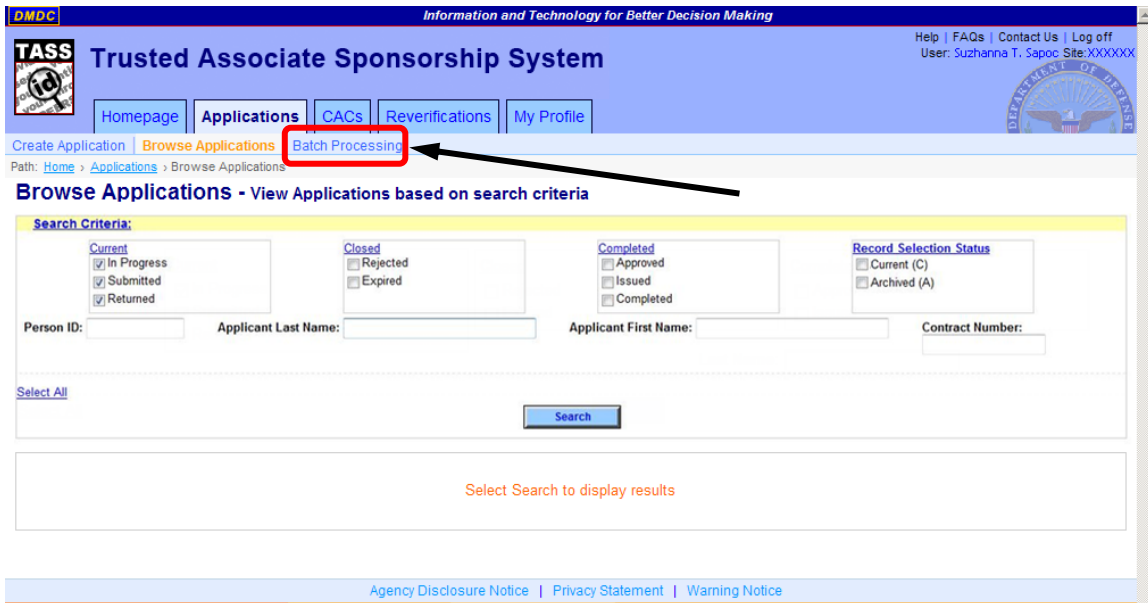
- Your SPOC must have approved and requested you Batch Processing access
- DMDC must have granted you Batch Processing access
- The contracting agency or your internal service or agency must provide you with a data XML file in the TASS predefined format, and you must save it on either your workstation or another form of media, such as a CD or DVD

Note: The TASS service or agency SPOC is responsible for validating the accuracy of data in all batch files uploaded into TASS.

7.9.2 Submitting Multiple Applications Using High Volume Data Feed

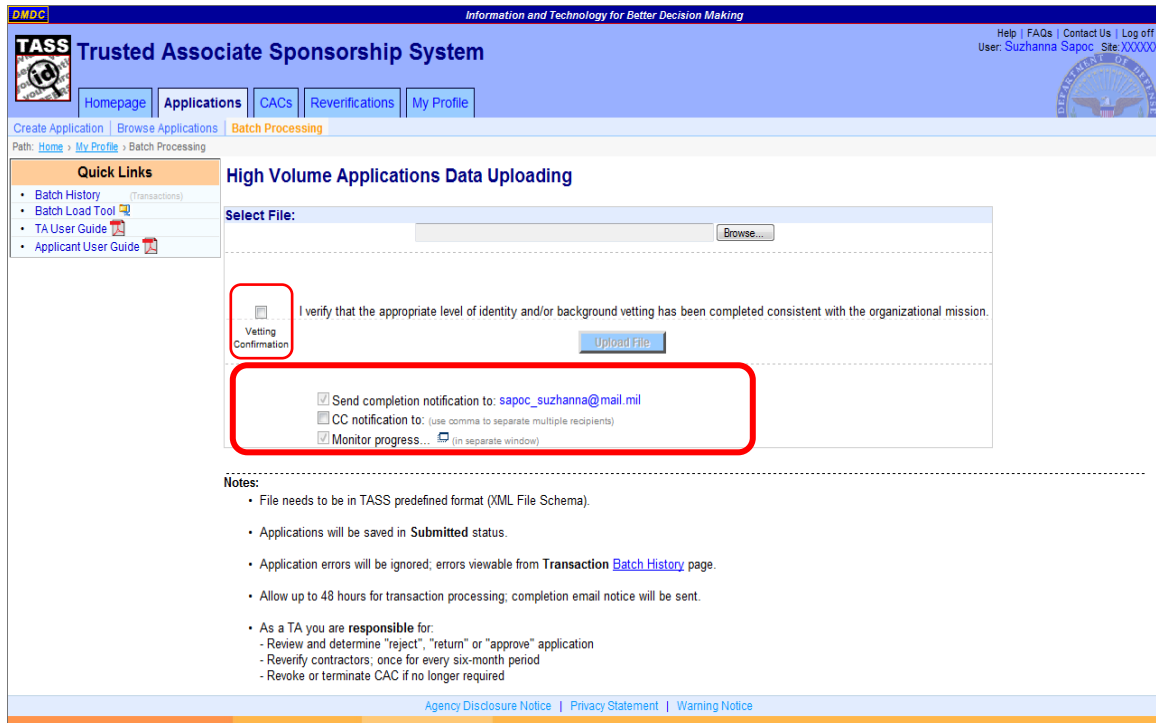
1. Select the **Applications** tab.
 - Result: The *Browse Applications* screen appears (see Figure 70).

Figure 70. Browse Applications Screen



2. Click the **Batch Processing** link from the second row navigation bar.
➤ Result: The *High Volume Applications Data Uploading* screen appears (see Figure 71).

Figure 71. High Volume Applications Data Uploading Screen



3. Select the **Vetting Confirmation** check box to verify that the appropriate level of vetting has been completed for the Applicant records submitted.

4. **Optional:** To send a copy of the completion notification email to an email address in addition to the one that appears next to the **Send completion notification to:** check box, click the **CC notification to:** check box.
- Result: A check appears in the check box next to **CC notification to:** and a textbox appears below the line (see Figure 72).

Figure 72. High Volume Data Uploading—CC Notification Section

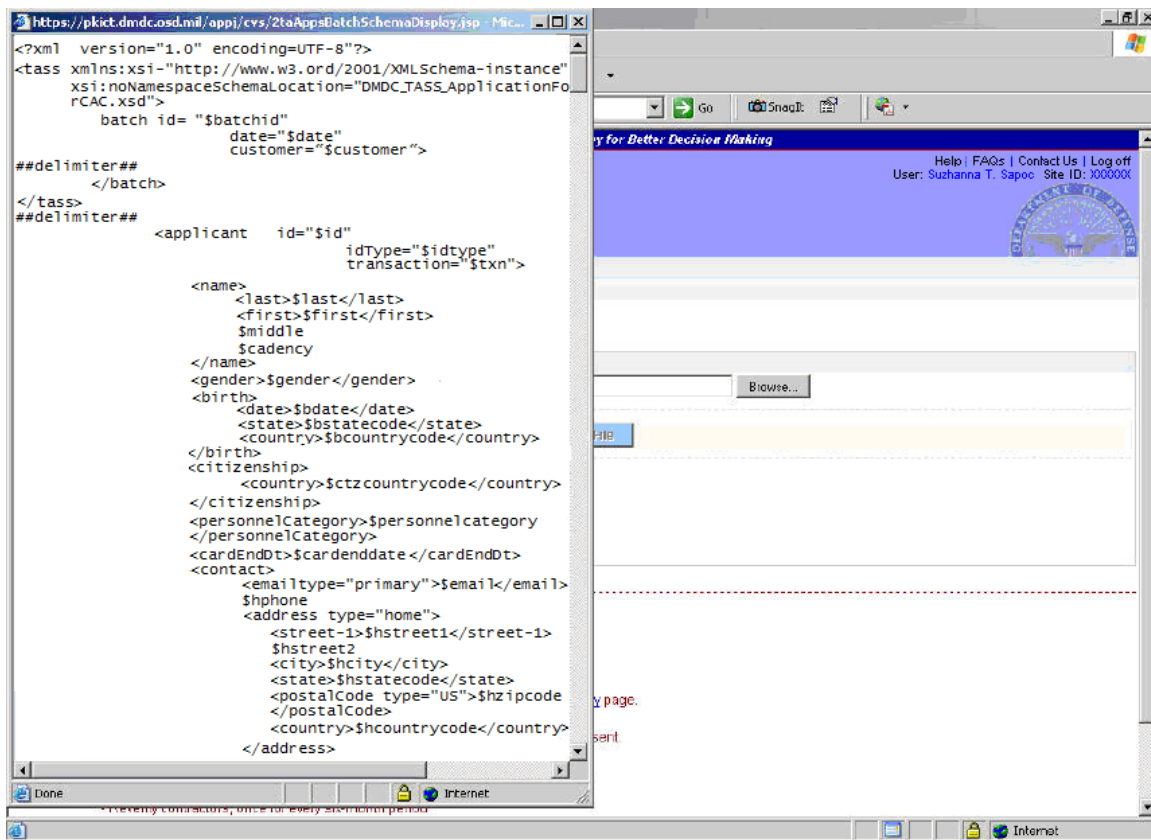
The screenshot shows the 'High Volume Applications Data Uploading' page in the TASS system. The page includes a navigation menu with 'Applications', 'CACs', 'Reverifications', and 'My Profile'. A 'Quick Links' sidebar on the left contains links for 'Batch History', 'Batch Load Tool', 'TA User Guide', and 'Applicant User Guide'. The main content area features a 'Select File:' field with a 'Browse...' button. Below this is a 'Vetting Confirmation' section with a checked checkbox and the text 'I verify that the appropriate level of identity and/or background vetting has been completed consistent with the organizational mission.' An 'Upload File' button is located below the vetting confirmation. A red box highlights the notification options: 'Send completion notification to: sapoc_suzhanna@mail.mil', 'CC notification to:' (checked), and 'Monitor progress...' (checked). Below the red box is a 'Notes' section with three bullet points: 'File needs to be in TASS predefined format (XML File Schema).', 'Applications will be saved in Submitted status.', and 'Application errors will be ignored; errors viewable from Transaction Batch History page.'

5. **Optional:** Type the email address of the additional person to whom you want to send the completion notification in the box.

Note: To utilize the HVDF files, you must download the **Batch Load Tool** from the *Quick Links* menu. Click the link for the Batch Upload Tool to open the .zip file. To execute the Batch Upload process:

1. Save the .zip file to your computer.
2. Open the “README.txt” document to review directions for use.
3. Follow the instructions in the “Tool High Volume Data Feed.docx” (Batch Tool User Manual) document to use the Batch Upload Tool.

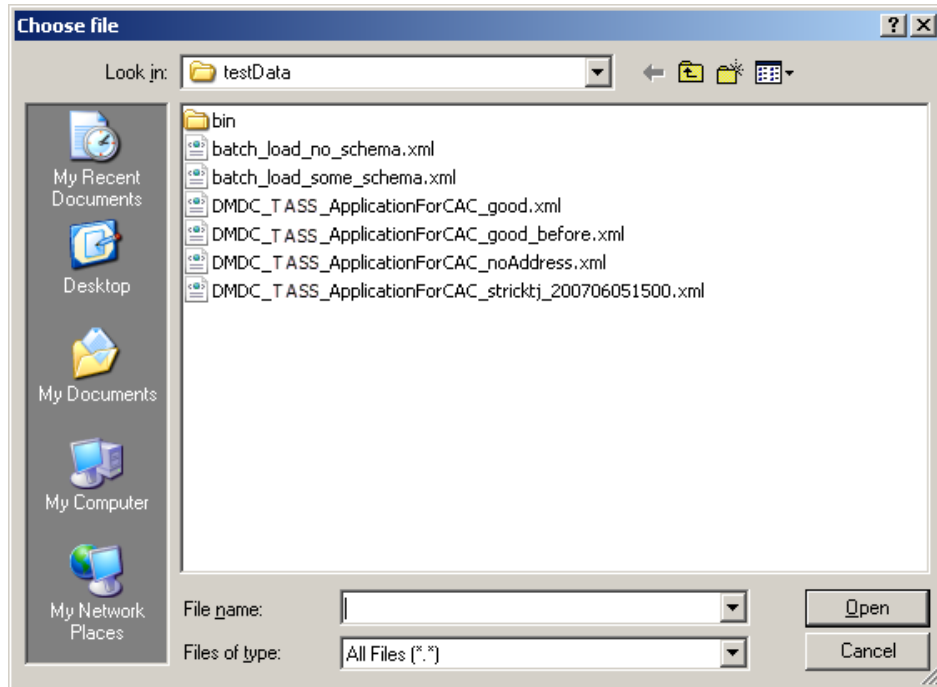
Figure 73. XML Schema Screen



6. To select a file to upload, click the **Browse** button to the right of the **Select File:** box.

➤ Result: The *Choose File* screen appears (see Figure 74).

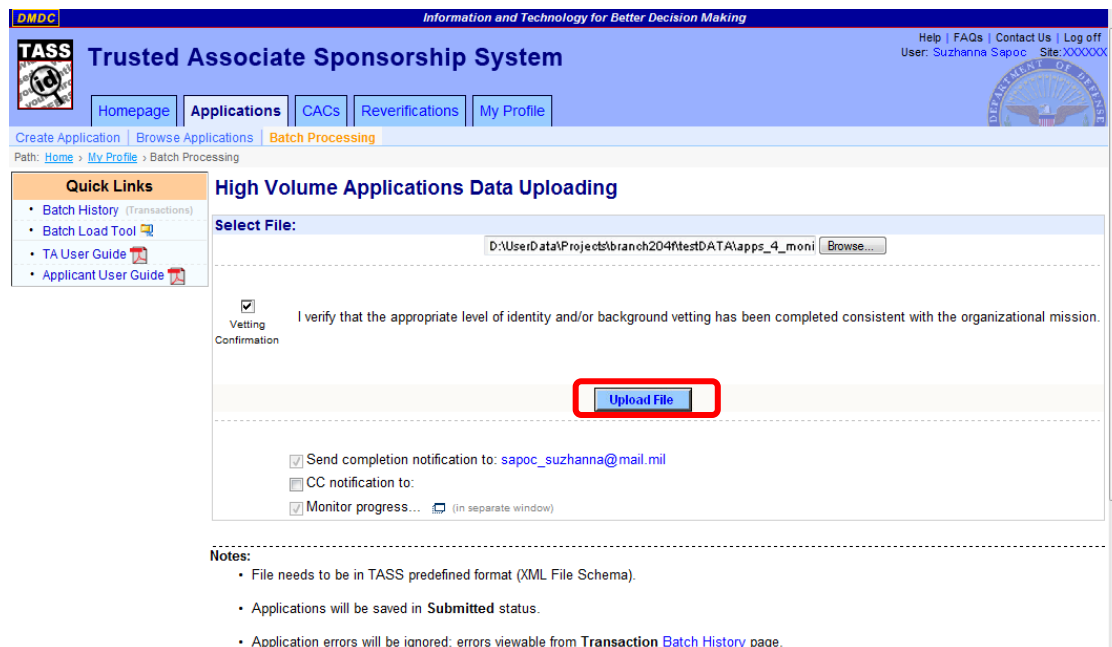
Figure 74. Choose File Screen



7. From the *Choose File* window, locate the XML file to upload from your workstation or other medium and click **Open**.

- Result: The file name appears in the **Select File** field and the **Upload File** button activates (see Figure 75).

Figure 75. High Volume Applications Data Uploading Screen—Ready to Upload



Note: You must select a file with an .xml file type or an error messages appears (see Figure 76). You cannot select the **Upload File** button unless you select an .xml file.

Figure 76. .xml File Must Be Selected Error Message



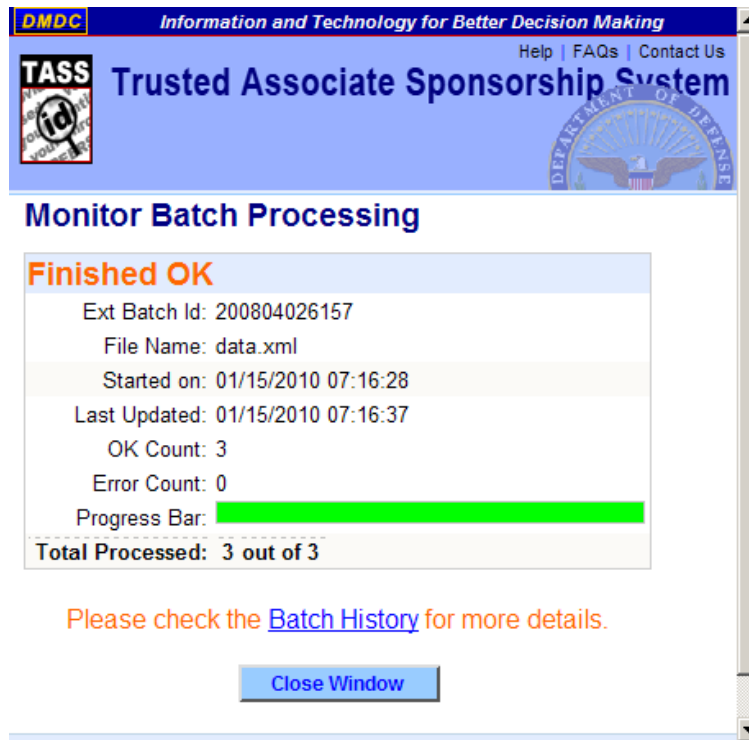
8. Click **Upload File**.

- **Result:** The **Upload File** button changes to **Processing** (see Figure 77), and the *Monitor Batch Processing* screen (see Figure 78), displays the progress of the upload.

Figure 77. High Volume Applications Data Uploading—Processing Upload

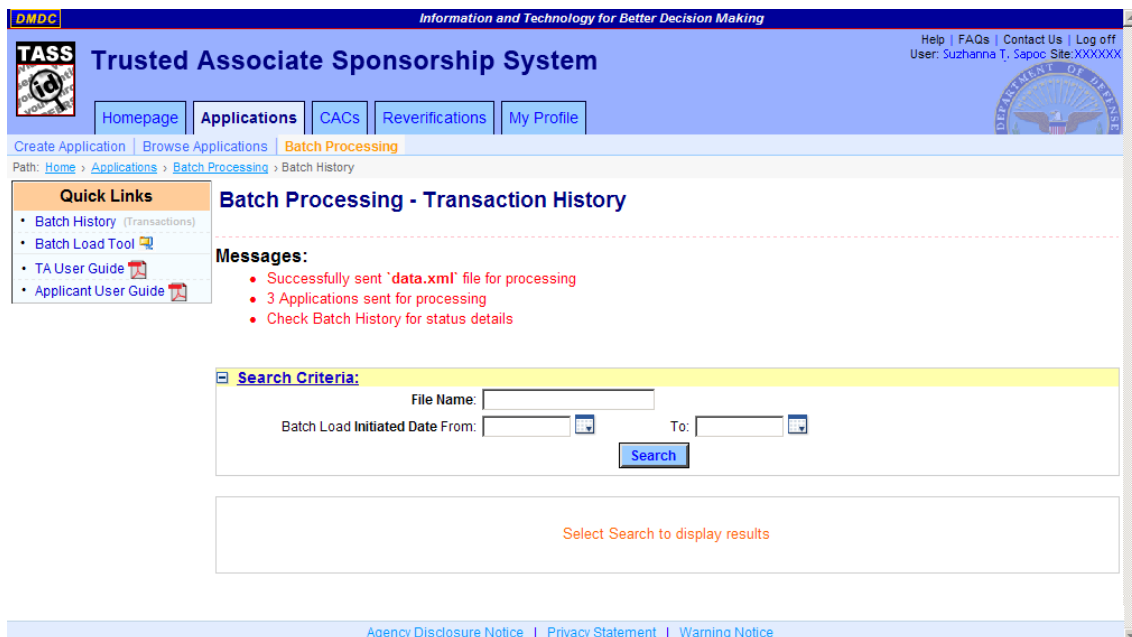


Figure 78. Monitor Batch Processing Screen



- Result: When the upload finishes, the *Batch Processing—Transaction History* messages screen appears (see Figure 79).

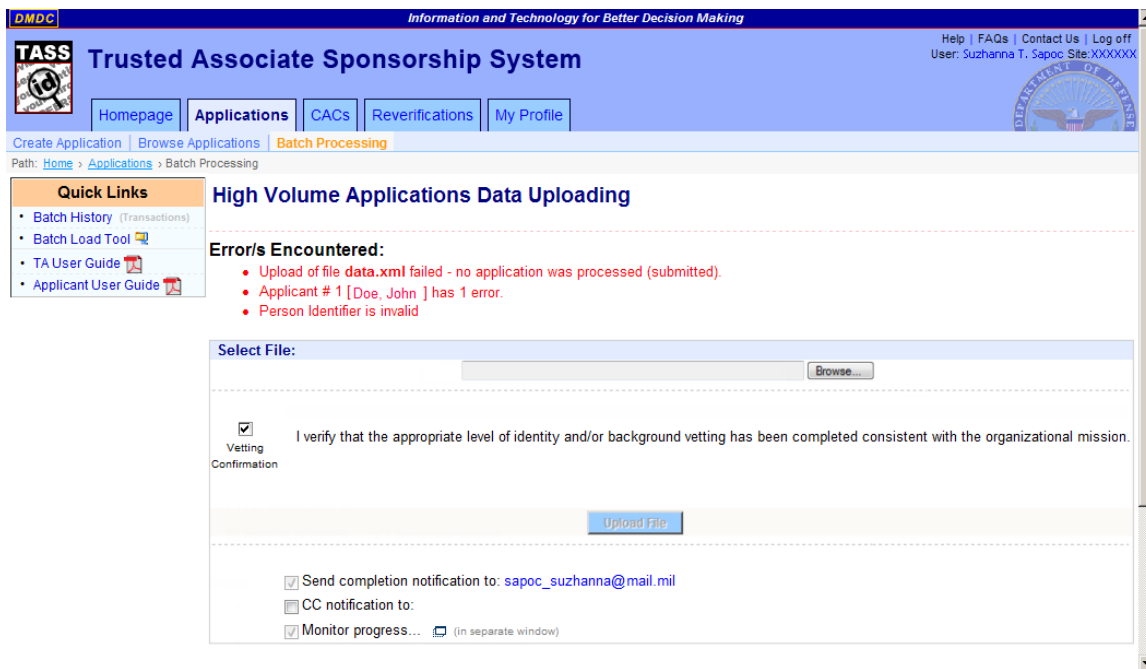
Figure 79. Batch Processing Screen—Transaction History



Note: When TASS completes the High Volume Data Feed process, TASS will send you an email confirming that the Batch File uploaded successfully (see **Appendix E**).

Note: If the system encounters any errors, the upload fails and the High Volume Data Applications Uploading error screen appears (see Figure 80). Correct any errors in the XML file and upload the file again.

Figure 80. High Volume Applications Data Uploading Screen—Error

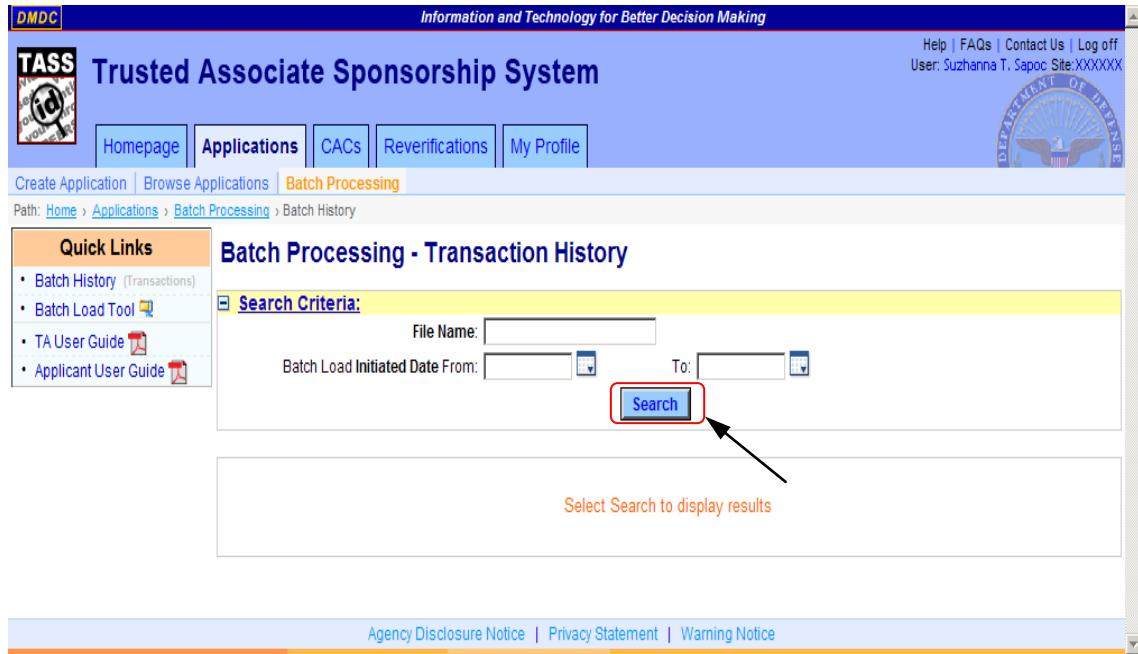


7.9.3 Searching for a Batch Processing Transaction History

To search for details about a batch's transaction history, perform the following steps:

1. Select the **Applications** tab.
 - Result: The *Browse Applications* screen appears (see Figure 70).
2. Click the **Batch Processing** link from the second row navigation bar.
 - Result: The *High Volume Applications Data Uploading* screen appears (see Figure 71).
3. Click the **Batch History** link in *Quick Links*.
 - Result: The *Batch Processing—Transaction History* screen appears (see Figure 81).

Figure 81. Batch Processing Screen—Transaction History



4. Enter the **Batch Upload Initiated Date From** and **To** dates to set the time period for the record search (see Figure 82).

Figure 82. Batch Processing—Transaction History Search Criteria



5. Click the **Search** button.
- Result: The search results display in the bottom part of the *Batch Processing—Transaction History* screen (see Figure 83).

Figure 83. Batch Processing—Transaction History Search Results

The screenshot displays the 'Batch Processing - Transaction History' page in the TASS system. At the top, there is a navigation bar with 'Home', 'Applications', 'Batch Processing', and 'Batch History' links. A 'Quick Links' sidebar on the left includes 'Batch History (Transactions)', 'Batch Load Tool', 'TA User Guide', and 'Applicant User Guide'. The main content area features a search form with a 'File Name' field, 'Batch Load Initiated Date From' and 'To' date pickers (both set to 01-15-2010), and a 'Search' button. Below the search form, a message states: 'You may click on any column heading to change the primary sort, but it will not also sort by name then.' The search results show 'One Record found.' and a table with the following data:

File Name	Batch ID	Recs OK	Err	Initiated	Status	Date	Links
data.xml	200804026157	3	0	01/15/10 07:16:28	Finished OK	01/15/10 07:16:37	

Below the table, there is a 'Per page: 25' dropdown and a 'Print' button. At the bottom of the page, there are links for 'Agency Disclosure Notice', 'Privacy Statement', and 'Warning Notice'.

8 TASS Application Features

Use the following sections to learn about the basic TASS application features.

8.1 Quick Links

The *Quick Links* menu is located on the left side of the *TA Homepage* (see Figure 84).

The TASS application contains various links that open additional screens as popup windows. You can access **Forms**, **Policies**, and **Training-Courseware**, as well as a link to **System Requirements** and an electronic copy of this guide, as well as the *TASS Applicant Guide*.

Figure 84. Quick Links Menu



8.1.1 Forms

The *Forms* screen contains links to access the following forms:

- **Form DD1172-2**—The standard application form for a DoD CAC
- **Form DD2842**—The PKI Subscriber Certificate Acceptance and Acknowledgement of Responsibilities form

You can also click on links to instructions for completing these forms. You can access *DD Form 1172-2* in HTML format.

To view the available forms, perform the following steps:

1. Click the **Forms** link in the *Quick Links* menu.
 - **Result:** The *Forms* screen appears (see Figure 85).

Figure 85. Forms Screen



2. Click the corresponding link to open the form you want to view, download, or print.

➤ Result: The document loads in a new browser window. From here, you can view or print the document.

3. Click the **X** button located at the top right corner of the browser window to close the form.

4. Click the **Close Window** button.

➤ Result: The *Forms* window closes.

8.1.2 Policies

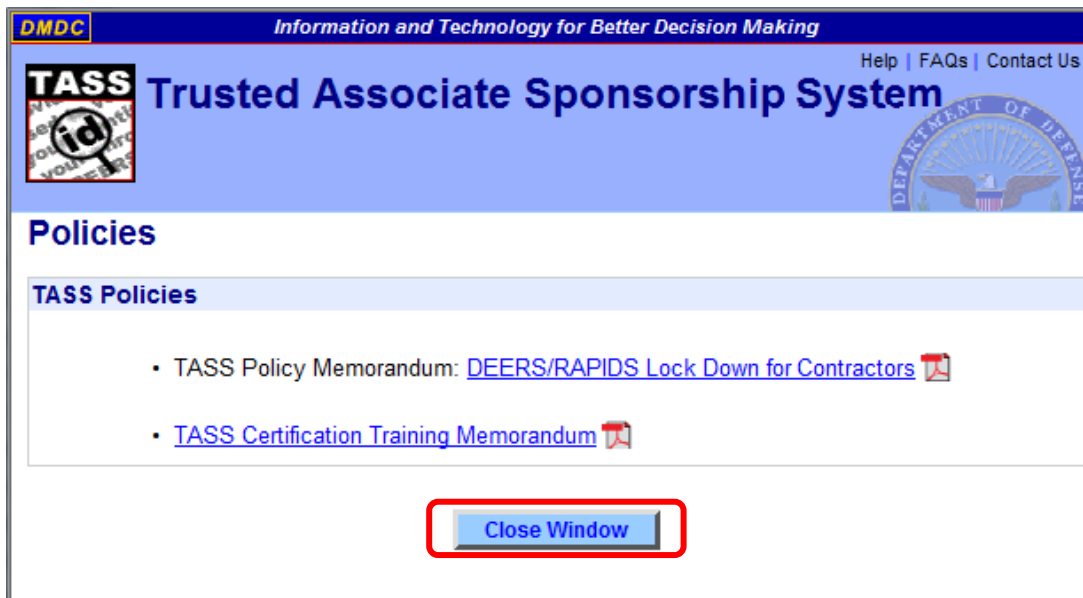
Use the *Policies* screen to display links to memorandum documents that provide information for TASS-based policies. You can open and view, download, and print.

To view TASS policy information, perform the following steps:

1. Click the **Policies** link in the *Quick Links* menu.

➤ Result: The *Policies* screen appears (see Figure 86).

Figure 86. Policies Screen



2. Click the corresponding link to open the policy you want to view, download, or print.
 - Result: The document loads in a new browser window. From that window, you can view or print the document.
3. Click the **X** button located at the top right corner of the browser window to close the policy.
4. Click the **Close Window** button.
 - Result: The *Policies* window closes.

8.1.3 Training-Courseware

The *Training-Courseware* screen, (see Figure 87), provides links to documentation and information for the TASS Certification Training Courses. You must complete these courses in order to access the TASS application and perform your duties.

To open the training and courseware information, perform the following steps:

1. Click **Training-Courseware** in *Quick Links* of the *TA Homepage*.
 - Result: The *Training-Courseware* screen appears (see Figure 87).

Figure 87. Training-Courseware



2. Click the word link of the applicable menu name to expand one of the *TASS Certification Training* expandable menus.

Training-Courseware has the following links:

- **Announcements**
- **Required Certification Courses**
- **Certification Instructions**

Announcements

Use **Announcements** to link to news about TASS Certification Training requirements and the DoD memorandum about TASS Certification Training. You can also link to the Fact Sheet, which answers frequently asked questions (FAQs) about the learning site, such as the type of training available, how to enroll, and accessibility.

Required Certification Courses

Required Certification Courses provides a link to the DMDC Training Site to access TASS Certification courses required for your role.

Certification Instructions

Certification Instructions provides a link to instructions on how to take your TASS Certification Training on the DMDC Learning Site and a link for details of how to check the completion status of your TASS Certification training

8.1.4 System Requirements

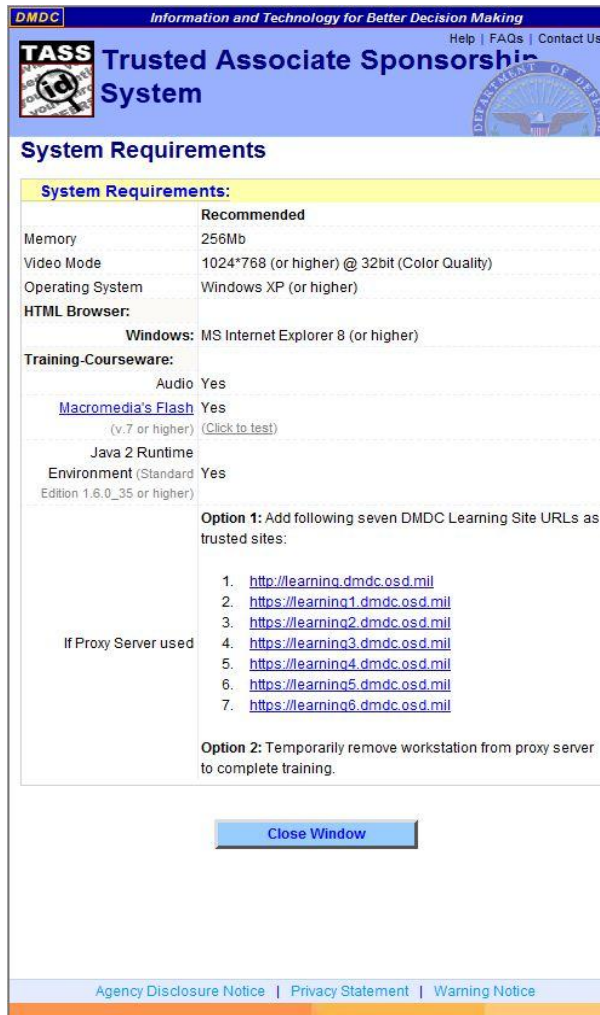
The **System Requirements** link, available on the *Quick Links* menu (see Figure 84), allows you to view the system requirements for running the TASS application from your computer.

To view the system requirements, perform the following steps:

1. Click the **System Requirements** link in the *Quick Links* menu.
 - Result: The *System Requirements* screen appears (see Figure 88).

Note: You can also access **System Requirements** from the **Help** link.

Figure 88. System Requirements Screen



8.2 Additional TASS Application Functions

The TASS application has additional functions and screens available to assist you with your day-to-day responsibilities.

8.2.1 Print

You can print from most screens that have search results.

The **Print** icon is located on the lower right of the screen (see Figure 89).

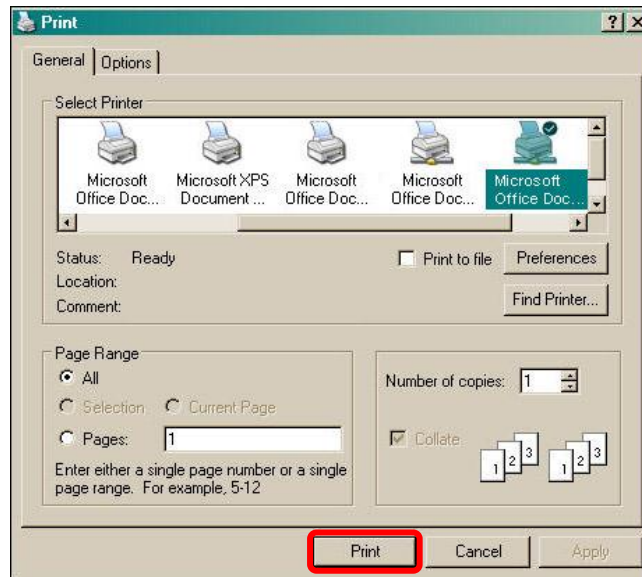
Figure 89. Print Icon



To print a hard copy of a screen, perform the following steps:

1. Click the **Print** icon.
 - Result: The *Print* screen appears (see Figure 90).

Figure 90. Print Screen



2. Click **Print**.

Note: When printing search results that display records of TASM's, TAs, and Applicants, you must protect PII. Follow your local service or agency's security policies and procedures for safeguarding PII data as well as the DoD Guidance on Protecting PII (<http://www.dod.gov/pubs/foi/privacy/policy.html>).

8.2.2 Per Page Display

You can change the number of results displayed per page during a search by using the **Per page** function. The **Per page** drop-down menu is located on the lower right of the screen, to the left of the **Print** icon (see Figure 91).

Figure 91. Per Page Display Drop-Down Menu



To change the number of records the screen displays, perform the following steps:

1. Click the **Per page** drop-down arrow.
 - Result: The drop-down menu options expand.

2. Select a new display number.

8.2.3 Page Number, Next, and Last

If your search returns numerous records, they may display in a multiple-page format, especially when searching for multiple Applicants. In these cases, **Page Number**, **Next**, and **Last** links display on the right of the screen just above the search result records (see Figure 92).

Figure 92. Page Number, Next, and Last Links



The TASS page number currently displayed on the screen is highlighted.

Click the page number to go to that page, click the **Next** link to go to the next page, or click the **Last** link to go to the last page.

8.3 Help

Click **Help** in the top right corner of the screen to access important links to information regarding training, user documentation, and system requirements (see Figure 93). You can access the Help link from every screen in the TASS application.

Figure 93. Help Screen



8.4 Frequently Asked Questions (FAQs)

Access the FAQs by clicking **FAQs** in the top right corner of the screen. The FAQs page provides answers to the most commonly asked questions about the TASS application and TASS policies. If you log in as a TASM, you will see the TASM, TA, and Applicant FAQs; if you log in as a TA, you will see the TA and Applicant FAQs. SPOCs and Applicants also have specific FAQ pages. The FAQs link is accessible from every screen in the TASS application.

8.5 Contact Us

Contact TASS by clicking **Contact Us** in the top right corner of the screen. The TASS Contact Us screen is accessible from every screen in the TASS application. This screen contains contact information for support for TASS issues.

8.6 DoD Policy

At the bottom of the TASS application screens, you can access the *DoD Policy* menu. This menu consists of the following three links that access screens with information on agency disclosure and privacy and DoD system policies:

- **Agency Disclosure Notice**

- **Privacy Statement**
- **Warning Notice** (see Figure 94).

Figure 94. Agency Disclosure Notice/Privacy Statement/Warning Notice Links



Agency Disclosure Notice

Click the **Agency Disclosure Notice** link to open the *Agency Disclosure Notice* screen (see Figure 95).

Figure 95. Agency Disclosure Notice Screen



DMDC Information and Technology for Better Decision Making Help | FAQs | Contact Us

TASS Trusted Associate Sponsorship System

AGENCY DISCLOSURE NOTICE

The public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Executive Services Directorate (0704-0415). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THIS ADDRESS.

RETURN COMPLETED FORM TO A REAL-TIME AUTOMATED PERSONNEL IDENTIFICATION SYSTEM WORK STATION

Agency Disclosure Notice | Privacy Statement | Warning Notice

This screen contains information regarding Agency Disclosure and the Agency Disclosure form, including where to return comments.

Privacy Statement

Click the **Privacy Statement** link to open the *Privacy Act Statement* screen (see Figure 96).

Figure 96. Privacy Act Statement Screen

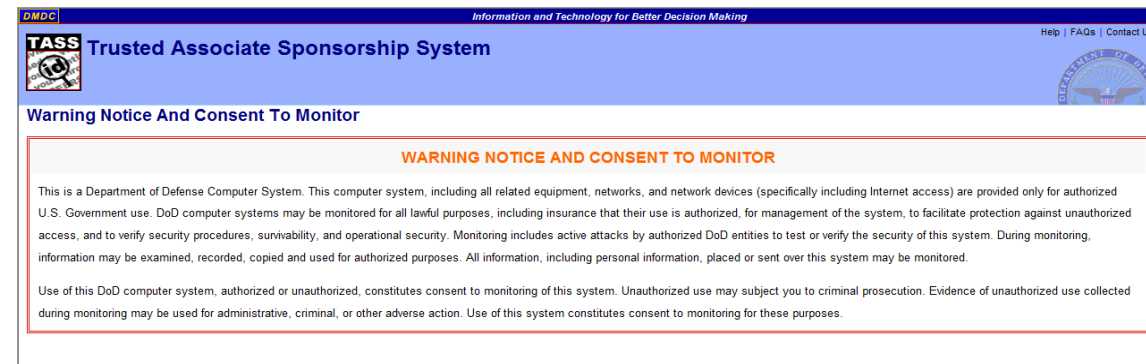


This screen contains information about the Privacy Act, which protects records that contain personal identifiers such as names and SSNs. The screen gives a synopsis of the purpose and uses of the Privacy Act.

Warning Notice

Click the **Warning Notice** link to open the *Warning Notice and Consent to Monitor* screen (see Figure 97).

Figure 97. Warning Notice and Consent to Monitor Screen



This screen displays information about the DoD policy for monitoring all DoD computer systems for harmful activity. Because TASS is a DoD system, this policy affects all TASS roles.

You can close *DoD Policy* menu screens by clicking **Close Window** at the bottom of the screen.

8.7 Log Off

Use the **Log off** link at the top right corner of the screen to log off of the TASS application.

Note: The Log off function is not available from all screens.

To log off the TASS application, perform the following steps:

1. Click **Log off**.

➤ Result: The *Log Off Successful* screen appears (see Figure 98).

Note: **Log in** appears to the right of the **Help** menu if you need to log in again.

Figure 98. Log Off Successful Screen



2. Click Close Window

Note: For security reasons, you must close the browser window.

➤ Result: A confirmation message box appears (see Figure 99).

Figure 99. Confirmation Message to Close Browser Window



3. Click **Yes**.

- Result: The browser window closes.




Appendix A DD Form 2875 System Authorization Access Request (SAAR)

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)				
PRIVACY ACT STATEMENT				
AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form. ROUTINE USES: None. DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.				
TYPE OF REQUEST <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID				DATE (YYYYMMDD)
SYSTEM NAME (Platform or Applications)			LOCATION (Physical Location of System)	
PART I (To be completed by Requestor)				
1. NAME (Last, First, Middle Initial)		2. ORGANIZATION		
3. OFFICE SYMBOL/DEPARTMENT		4. PHONE (DSN or Commercial)		
5. OFFICIAL E-MAIL ADDRESS		6. JOB TITLE AND GRADE/RANK		
7. OFFICIAL MAILING ADDRESS		8. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER	9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR	
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input type="checkbox"/> I have completed Annual Information Awareness Training. DATE (YYYYMMDD)				
11. USER SIGNATURE			12. DATE (YYYYMMDD)	
PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 10.)				
13. JUSTIFICATION FOR ACCESS				
14. TYPE OF ACCESS REQUIRED: <input type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED				
15. USER REQUIRES ACCESS TO: <input type="checkbox"/> UNCLASSIFIED <input type="checkbox"/> CLASSIFIED (Specify category) <input type="checkbox"/> OTHER				
16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input type="checkbox"/>		16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)		
17. SUPERVISOR'S NAME (Print Name)		18. SUPERVISOR'S SIGNATURE		19. DATE (YYYYMMDD)
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT		20a. SUPERVISOR'S E-MAIL ADDRESS		20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR		21a. PHONE NUMBER		21b. DATE (YYYYMMDD)
22. SIGNATURE OF IAO OR APPOINTEE		23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE (YYYYMMDD)

DD FORM 2875, AUG 2009

PREVIOUS EDITION IS OBSOLETE.

Adobe Professional 8.0

26. NAME (Last, First, Middle Initial)		
27. OPTIONAL INFORMATION (Additional Information)		
PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION		
28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION (YYYYMMDD)
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> LEVEL III
29. VERIFIED BY (Print name)	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE 
32. DATE (YYYYMMDD)		
PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION		
TITLE	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED (YYYYMMDD)	PROCESSED BY (Print name and sign) 	DATE (YYYYMMDD)
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign) 	DATE (YYYYMMDD)
DD FORM 2875 (BACK), AUG 2009		
		<input type="button" value="Reset"/>

Appendix B DD Form 2875 Instructions

INSTRUCTIONS	
The prescribing document is as issued by using DoD Component.	
<p>A. PART I: The following information is provided by the user when establishing or modifying their USER ID.</p> <p>(1) Name. The last name, first name, and middle initial of the user.</p> <p>(2) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).</p> <p>(3) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).</p> <p>(4) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.</p> <p>(5) Official E-mail Address. The user's official e-mail address.</p> <p>(6) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.</p> <p>(7) Official Mailing Address. The user's official mailing address.</p> <p>(8) Citizenship (US, Foreign National, or Other).</p> <p>(9) Designation of Person (Military, Civilian, Contractor).</p> <p>(10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.</p> <p>(11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).</p> <p>(12) Date. The date that the user signs the form.</p>	<p>(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.</p> <p>(21a) Phone Number. Functional appointee telephone number.</p> <p>(21b) Date. The date the functional appointee signs the DD Form 2875.</p> <p>(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.</p> <p>(23) Organization/Department. IAO's organization and department.</p> <p>(24) Phone Number. IAO's telephone number.</p> <p>(25) Date. The date IAO signs the DD Form 2875.</p> <p>(27) Optional Information. This item is intended to add additional information, as required.</p>
<p>C. PART III: Certification of Background Investigation or Clearance.</p> <p>(26) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).</p> <p>(26a) Date of Investigation. Date of last investigation.</p> <p>(26b) Clearance Level. The user's current security clearance level (Secret or Top Secret).</p> <p>(26c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).</p> <p>(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.</p> <p>(30) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.</p> <p>(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.</p> <p>(32) Date. The date that the form was signed by the Security Manager or his/her representative.</p>	
<p>(13) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.</p> <p>(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)</p> <p>(15) User Requires Access To: Place an "X" in the appropriate box. Specify category.</p> <p>(16) Verification of Need to Know. To verify that the user requires access as requested.</p> <p>(16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.</p> <p>(17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.</p> <p>(18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.</p> <p>(19) Date. Date supervisor signs the form.</p> <p>(20) Supervisor's Organization/Department. Supervisor's organization and department.</p> <p>(20a) E-mail Address. Supervisor's e-mail address.</p> <p>(20b) Phone Number. Supervisor's telephone number.</p>	<p>D. PART IV: This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.</p> <p>E. DISPOSITION OF FORM:</p> <p>TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.</p> <p>FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.</p>

DD FORM 2875 INSTRUCTIONS, AUG 2009

Appendix C DD Form 1172-2

APPLICATION FOR IDENTIFICATION CARD/DEERS ENROLLMENT					OMB No. 0704-0415 OMB approval expires Jan 31, 2014
Please read Agency Disclosure Notice, Privacy Act Statement, and instructions prior to completing this form.					
SECTION I - SPONSOR/EMPLOYEE INFORMATION					
1. NAME (Last, First, Middle)		2. GENDER	3. SSN OR DOD ID NO.	4. STATUS	5. ORGANIZATION
6. PAY GRADE	7. GEN. CAT	8. CITIZENSHIP	9. DATE OF BIRTH (YYYYMMDD)	10. PLACE OF BIRTH	
11. CURRENT HOME ADDRESS			12. CITY	13. STATE	14. ZIP CODE
16. PRIMARY E-MAIL ADDRESS			17. TELEPHONE NUMBER (Include Area Code/DSN)	18. CITY OF DUTY LOCATION	19. STATE OF DUTY LOCATION
				20. COUNTRY OF DUTY LOCATION	
SECTION II - SPONSOR/EMPLOYEE DECLARATION AND REMARKS					
21. REMARKS (Cite legal documentation, as applicable.)					NOTARY SIGNATURE AND SEAL
I certify the information provided in connection with the eligibility requirements of this form is true and accurate to the best of my knowledge. (If not signed in the presence of the authorizing/verifying official, the signature must be notarized.)					
22. SPONSOR/EMPLOYEE SIGNATURE					23. DATE SIGNED (YYYYMMDD)
SECTION III - AUTHORIZED BY					
24. SPONSORING OFFICE NAME				25. CONTRACT NUMBER	
26. SPONSORING OFFICE ADDRESS (Street, City, State, ZIP Code)		27. SPONSORING OFFICE TELEPHONE NUMBER (Include Area Code/DSN)	28. OFFICE EMAIL ADDRESS		29. OVERSEAS ASSIGNMENT (Country)
30. OVERSEAS ASSIGNMENT BEGIN DATE (YYYYMMDD)	31. OVERSEAS ASSIGNMENT END DATE (YYYYMMDD)	32. ELIGIBILITY EFFECTIVE DATE (YYYYMMDD)	33. ELIGIBILITY EXPIRATION DATE (YYYYMMDD)		
I certify the individual identified above, based on personal knowledge and available documentation, is in a status eligible for and requires an identification card in the performance of their duties with the Uniformed Services.					
34. SPONSORING OFFICIAL NAME (Last, First, Middle)			35. UNIT/ORGANIZATION NAME		
36. TITLE	37. PAY GRADE	38. SIGNATURE		39. DATE VERIFIED (YYYYMMDD)	
SECTION IV - DEPENDENT INFORMATION (Attach additional pages if necessary)					
A	40. NAME (Last, First, Middle)	41. GENDER	42. DATE OF BIRTH (YYYYMMDD)	43. RELATIONSHIP	44. SSN OR DOD ID NO.
45. CURRENT HOME ADDRESS					
46. CITY		47. STATE	48. ZIP CODE	49. COUNTRY	50. ELIGIBILITY EFFECTIVE DATE (YYYYMMDD)
					51. ELIGIBILITY EXPIRATION DATE (YYYYMMDD)
B	52. NAME (Last, First, Middle)	53. GENDER	54. DATE OF BIRTH (YYYYMMDD)	55. RELATIONSHIP	56. SSN OR DOD ID NO.
57. CURRENT HOME ADDRESS					
58. CITY		59. STATE	60. ZIP CODE	61. COUNTRY	62. ELIGIBILITY EFFECTIVE DATE (YYYYMMDD)
					63. ELIGIBILITY EXPIRATION DATE (YYYYMMDD)
SECTION V - RECEIPT					
Receipt of new card is acknowledged.					
64. SIGNATURE					65. DATE ISSUED (YYYYMMDD)

DD FORM 1172-2, APR 2012

PREVIOUS EDITION IS OBSOLETE.

This form valid for issue of DoD ID Card for 90 days from date of verification.

Reset

Adobe Professional 8.0

Appendix D DD Form 1172-2 Instructions

INSTRUCTIONS FOR COMPLETION OF DD FORM 1172-2, “APPLICATION FOR DEPARTMENT OF DEFENSE COMMON ACCESS CARD – DEERS ENROLLMENT”, August 2011 Version

The DD Form 1172-2 shall be used to apply for issuance of DD Forms 2 (Active, Reserve, Retired, and Reserve Retired), DD Form 1173, DD Form 1173-1, DD Form 2764, DD Form 2765, individuals eligible for a Common Access Card (CAC) who are not enrolled in DEERS, and for enrollment or update of eligible individuals into the DEERS data base. Retention and disposition of the DD Form 1172-2 shall be in accordance with uniformed services' regulatory instructions.

Note:

- DoD Sponsors enrolling their dependents in DEERS should complete Sections I, II, and IV.
- DoD Sponsors updating their own status or adding a personnel condition impacting benefits (e.g., overseas assignment) should complete Sections I and II.
- Eligible employees applying for a CAC should complete Sections I and II (and Section IV if a Foreign Affiliate on orders to the U.S. with authorized Dependents). The DD Form 1172-2 should then be provided to a DoD Sponsor for authorization and completion of Section III.
- DoD Sponsors authorizing a CAC for an employee should complete Section III.
- For certain populations a paper form will not be required. (Populations entered into RAPIDS via Contractor Verification System)
- For CAC applicants using a paper form, a DD Form 577 (Signature card) must be on file at the issuing site.
- This form shall be used only for its intended purpose, DEERS enrollment/updates.

SECTION I – SPONSOR/EMPLOYEE INFORMATION.

Block 1. Name. Enter the sponsor/employee's LAST name first, enter the FIRST name, and then enter the MIDDLE INITIAL or the full MIDDLE NAME. (Use no more than 51 characters.) The name field can include a designation of JR, SR, ESQ, or the Roman numerals I through X. To include that designation, enter the appropriate data after the middle initial. The name cannot contain any special characters nor is any punctuation permitted.

Block 2. Gender. Enter the sponsor/employee's gender from the valid codes listed in Table 1: (Use one character.)

Table 1. DD Form 1172-2 Block 2. Gender

CODE.	SEX
M	Male
F	Female

Block 3. Social Security Number (SSN) or DoD ID Number. Enter the sponsor/employees' SSN or DoD ID Number. In cases where an employee has not been issued an SSN or DoD ID Number, an ITIN can be provided. If neither number is available, a Foreign Identification Number (FIN) will be generated by the system. A FIN (assigned as 900-00-0000F and up) will be assigned and automatically generated for eligible foreign military and foreign nationals who do not have an SSN. A SSN or ITIN is the preferred identifier for initial enrollment. Only in cases where neither is available should an alternate be used.

For Verifying Officials: If a SSN or DoD ID Number is already registered in DEERS for another individual, STOP processing and verify the number. If verification confirms duplication of the SSN by the Social Security Administration, continue processing and the system shall automatically generate a duplicate control number for the additional sponsor.

Block 4. Status. Enter the sponsor/employee status from the valid codes listed in Table 2. If unsure of status, leave blank. (Use no more than six characters.)

Table 2. DD Form 1172-2 Block 4. Status

CODE	STATUS
ACADMY	Academy or Navy Officer Candidate School (OCS) Student
AD	Active duty (excluding Guard and Reserve on extended active duty for more than 30 days)
AD-DEC	Active duty deceased
CIV	Civilian
CONTR	Contractor
DAVDEC	100-percent disabled veteran deceased (either temporary (TMP) or permanent (PRM))
DAVPRM	100-percent disabled veteran, permanent disability
DAVTMP	100-percent disabled veteran, temporary disability
FP	Foreign military personnel
FMRMR	Former member who is in receipt of retired pay for non-regular service but who has been discharged from the Service and maintains no military affiliation
FMRDEC	A former member who qualified for retired pay for non-regular service at his or her sixtieth birthday, before his or her discharge from the Service, but died while in receipt of retired pay
GRD	National Guard (all categories)
GRDDEC	National Guard deceased
GRD-AD	Guard on extended active duty for more than 30 days
MH	Medal of Honor recipient
MH-DEC	Medal of Honor recipient deceased
OTHER	Non-DoD eligible beneficiaries (including credit union employees, and other civilians employed in support of U.S. forces overseas, who are authorized benefits and privileges)
PDRL	Retired member, on the Permanent Disability Retired List (PDRL)

PR-APL	Prisoner or Appellate leave
RCL-AD	Recalled to active duty
RES	Reserve (all categories)
RES-AD	National Guard and Reserve members who retire, but are not entitled to retired pay until age 60
RESDEC	Reserve deceased
RESRET	National Guard and Reserve members who retire, but are not entitled to retired pay until age 60
RET	Retired member entitled to retired pay
RETDEC	Deceased retired member entitled to retired pay. Code applies to active duty retired, Retired Reserve beginning on their 60th birthday, the TDRL, and the PDRL.
SSB	Special Separation Benefits (SSB) recipient member with 120 days medical benefits (CHAMPUS/TRICARE and MTF)
TDRL	Retired member, on the TDRL
TA-RES	Selected Reserve Transition Assistance Management Program members and their eligible dependents
TA-30	Involuntarily separated member of Reserve or Guard Component entitled to 30 days medical benefits (CHAMPUS/TRICARE and MTF)
TA-60	Involuntarily separated member with 60 days medical benefits (CHAMPUS/TRICARE and MTF)
TA-120	Involuntarily separated member with 120 days medical benefits (CHAMPUS/TRICARE and MTF)
VSI	Voluntary Separation Incentive (VSI) recipient with 120 days medical benefits (CHAMPUS/TRICARE and MTF)

Block 5. Organization. Enter the sponsor/employee’s organization or branch or service from the valid codes listed in Table 3. (Use no more than five characters.)

Table 3. DD Form 1172-2 Block 5. Organization

CODE	ORGANIZATION
USA	U.S. Army
USAF	U.S. Air Force
USN	U.S. Navy
USMC	U.S. Marine Corps
USCG	U.S. Coast Guard
USPHS	U.S. Public Health Service
NOAA	National Oceanic and Atmospheric Administration
DoD	Department of Defense
FED	Employee of an Agency other than DoD
OTHER	Used when the sponsor is not affiliated with one of the uniformed services listed above

Block 6. Pay Grade. Enter the sponsor/employee pay grade from the valid codes listed in Table 4. (Use no more than four characters.)

Table 4. DD Form 1172-2 Block 6. Pay Grade

CODE	BRANCH OF SERVICE
E1-E9	Enlisted pay grades 1 through 9
W1-W5	Warrant officer pay grades 1 through 5
STDT	Academy and/or Navy OCS student (ENTER PAY GRADE IF

	STDT RECEIVING PAY)
001-011	Officer pay grades 1 through 11 (011 is reserved)
GS01-GS18	Federal employees with General Schedule pay grades
NF1-NF6	Federal employees with Nonappropriated Fund pay grades
OTHER	Other (non-uniformed service) pay grades not defined above to include all contractors
N/A	Not applicable. Use this code with the Block 4 status codes of "FMRMR" or FMRDEC"

Block 7. GEN CAT (Geneva Convention Category). N/A. This block is automatically generated by DEERS/RAPIDS with the valid codes listed in Table 5.

Table 5. DD Form 1172-2 Block 7. GEN CAT

CODE	GEN CAT
I	Category I (pay grades E1 through E4)
II	Category II (pay grades E5 through E9)
III	Category III (pay grades W1 through 003 and/or Cadets and/or Midshipmen)
IV	Category IV (pay grades 004 through 006)
V	Category V (pay grades 007 through 011)
N/A	Not applicable (non-protected personnel)

Block 8. Citizenship. Enter the sponsor/employee's appropriate country of citizenship. (Use two characters.)

Table 6. DD Form 1172-2 Block 8. Citizenship

COUNTRY	CODE	COUNTRY	CODE	COUNTRY	CODE
Afghanistan	AF	Germany	GM	Nigeria	NI
Albania	AL	Ghana	GH	Niue	NE
Algeria	AG	Gibraltar	GI	Norfolk Island	NF
America Samoa	AQ	Glorioiso Islands	GO	Northern Mariana Islands	CQ
Andorra	AN	Greece	GR	Norway	NO
Angola	AO	Greenland	GL	Oman	MU
Anguilla	AV	Grenada	GJ	Pakistan	PK
Antarctica	AY	Guadeloupe	GP	Palmyra Atoll	LQ
Antigua and Barbuda	AC	Guam	GQ	Panama	PM
Argentina	AR	Guatemala	GT	Papua New Guinea	PP
Armenia	AM	Guernsey	GK	Paracel Islands	PF
Aruba	AA	Guinea	GV	Paraguay	PA
Ashmore and Cartier Islands	AT	Guinea-Bissau	PU	Peru	PE
Australia	AS	Guyana	GY	Philippines	RP
Austria	AU	Haiti	HA	Pitcairn Islands	PC
Azerbaijan	AJ	Heard Island and McDonald Islands	HM	Poland	PL

Bahamas, The	BF	Honduras	HO	Portugal	PO
Bahrain	BA	Hong Kong	HK	Puerto Rico	RQ
Baker Island	FQ	Howland Island	HQ	Qatar	QA
Bangladesh	BG	Hungary	HU	Reunion	RE
Barbados	BB	Iceland	IC	Romania	RO
Bassas Da India	BS	India	IN	Russia	RS
Belarus	BO	Indonesia	ID	Rwanda	RW
Belgium	BE	Iran	IR	St. Kitts and Nevis	SC
Belize	BH	Iraq	IZ	St. Helena	SH
Benin	BN	Ireland	EI	St. Lucia	ST
Bermuda	BD	Israel	IS	St. Pierre and Miquelon	SB
Bhutan	BT	Italy	IT	St. Vincent and the Grenadines	VC
Bolivia	BL	Ivory Coast	IV	San Marino	SM
Bosnia and Herzegovina	BO	Jamaica	JM	Sao Tome and Principe	TP
Botswana	BC	Jan Mayen	JN	Saudi Arabia	SA
Bouvet Island	BV	Japan	JA	Senegal	SG
Brazil	BR	Jarvis Island	DQ	Serbia	SR
British Indian Ocean Territory	IO	Jersey	JE	Seychelles	SE
British Virgin Islands	VI	Johnston Atoll	JQ	Sierra Leone	SL
Brunei	BX	Jordan	JO	Singapore	SN
Bulgaria	BU	Juan De Nova Island	JU	Slovakia	LO
Burkina	UV	Kazakhstan	KZ	Slovenia	SI
Burma	BM	Kenya	KE	Solomon Islands	BP
Burundi	BY	Kingman Reef	KQ	Somalia	SO
Cambodia	CB	Kiribati	KR	South Africa	SF
Cameroon	CM	Korea, Democratic	KN	South Georgia and the South Sandwich Islands	SX
Canada	CA	Korea, Republic of	KS	Spain	SP
Cape Verde	CV	Kuwait	KU	Spratly Islands	PG
Cayman Islands	CJ	Kyrgyzstan	KG	Sri Lanka	CE
Central African Republic	CT	Laos	LA	Sudan	SU
Chad	CD	Latvia	LG	Surinam	NS
Chile	CI	Lebanon	LE	Svalbard	SV
China	CH	Lesotho	LT	Swaziland	WZ
Christmas Island	KT	Liberia	LI	Sweden	SW
Clipperton Islands	IP	Libya	LY	Switzerland	SZ
Cocos (Keeling) Islands	CK	Liechtenstein	LS	Syria	SY
Colombia	CO	Lithuania	LH	Taiwan	TW
Comoros	CN	Luxembourg	LU	Tajikstan	TI
Cook Islands	CW	Macau	MC	Tanzania	TZ
Coral Sea Islands	CR	Macedonia	MK	Thailand	TH
Costa Rica	CS	Madagascar	MA	Togo	TO
Cote Dtvoire	IV	Malawi	MI	Tokelau	TL
Croatia	HR	Malaysia	MY	Tonga	TN
Cuba	CU	Maldives	MV	Trinidad and Tobago	TD
Cyprus	CY	Mali	ML	Tromelin Island	TE
Czech Republic	EZ	Malta	MT	Trust Territory of the Pacific Islands (Palau)	PS

Denmark	DA	Man, Isle of	IM	Tunisia	TS
Djibouti	DJ	Marshall Islands	RM	Turkey	TU
Dominica	DO	Martinique	MB	Turkmenistan	TX
Dominican Republic	DR	Mauritania	MR	Turks and Caicos Islands	TK
Ecuador	EC	Mauritius	MP	Tuvalu	TV
Egypt	EG	Mayotte	MF	Uganda	UG
El Salvador	ES	Mexico	MX	Ukraine	UP
Equatorial Guinea	EK	Midway Islands	MQ	United Arab Emirates	TC
Eritrea	ER	Moldova	MD	United Kingdom	UK
Estonia	EN	Monaco	MN	United States	US
Ethiopia	ET	Mongolia	MG	Uruguay	UY
Europa Island	EU	Montenegro	MW	Uzbekistan	UZ
Falkland Islands (Islas Malvinas)	FK	Montserrat	MH	Vanuatu	NH
Faroe Islands	FO	Morocco	MO	Vatican City	VT
Federated States of Micronesia	FM	Mozambique	MZ	Venezuela	VE
Fiji	FJ	Namibia	WA	Vietnam	VM
Finland	FI	Nauru	NR	Virgin Islands	VQ
France	FR	Navassa Island	BQ	Wake Island	WQ
French Guiana	FG	Nepal	NP	Wallis and Futuna	WF
French Polynesia	FP	Netherlands	NL	West Bank	WE
French Southern and Antarctic Lands	FS	Netherlands Antilles	NA	Western Sahara	WI
Gabon	GB	New Caledonia	NC	Western Samoa	WS
Gambia, The	GA	New Zealand	NZ	Yemen (Aden)	YM
Gaza Strip	GZ	Nicaragua	NU	Zambia	ZA
Georgia	GG	Niger	NG	Zimbabwe	ZI

Block 9. Date of Birth. Enter the sponsor/employee's date of birth in four-digit year, three alpha-character month, and two-digit day format (YYYYMMDD). (Use nine characters.)

Block 10. Place of Birth. Enter the sponsor/employee's place of birth (City, State, and Country, if outside the United States). Use State abbreviations provided in Table 7. If place of birth is a foreign country, use the appropriate abbreviation from Table 6.

Table 7. DD Form 1172-2 Block 10. Place of Birth

STATE	CODE	STATE	CODE	STATE	CODE
Europe & Canada	AE	Kansas	KS	Ohio	OH
Alabama	AL	Kentucky	KY	Oklahoma	OK
Pacific	AP	Louisiana	LA	Oregon	OR
Alaska	AK	Maine	ME	Pennsylvania	PA
American Samoa	AS	Maryland	MD	Puerto Rico	PR
Arizona	AZ	Massachusetts	MA	Rhode Island	RI
Arkansas	AR	Michigan	MI	South and Central America	AA
California	CA	Minnesota	MN	South Carolina	SC
Colorado	CO	Mississippi	MS	South Dakota	SD
Connecticut	CT	Missouri	MO	Tennessee	TN
Delaware	DE	Montana	MT	Federated States of Marshall	TT

				Islands, Palau	
District of Columbia	DC	Nebraska	NE	Texas	TX
Florida	FL	Nevada	NV	Utah	UT
Georgia	GA	New Hampshire	NH	Vermont	VT
Guam	GU	New Jersey	NJ	Virginia	VA
Hawaii	HI	New Mexico	NM	Virgin Islands	VI
Idaho	ID	New York	NY	Washington	WA
Illinois	IL	North Carolina	NC	West Virginia	WV
Indiana	IN	North Dakota	ND	Wisconsin	WI
Iowa	IA	Ohio	OH	Wyoming	WY

Block 11. Current Home Address. Enter the number and street of the sponsor/employee's current residence address. If sponsor is deceased or if address is unknown, leave blank. (Use no more than 27 characters.)

Block 12. City. Enter the sponsor/employee's current city of residence. If the sponsor's address is an Army Post Office (APO) or a Fleet Post Office (FPO), enter the designation APO or FPO. If the sponsor is deceased or city is unknown, leave blank. (Use no more than 18 characters.)

Block 13. State. Enter the correct U.S. postal code for the State of the sponsor/employee's residence from the valid codes listed in Table 7. If the sponsor's address is an APO or FPO, enter the correct APO or FPO State. If the sponsor lives outside of the 50 United States, the District of Columbia, or one of the listed trust territories, enter a default value of "XX." (Use two characters.) If the sponsor is deceased or if State is unknown, leave blank.

Block 14. ZIP Code. Enter the correct nine-digit ZIP Code of the sponsor's current residence address in the following format: "123456789." If the last four digits are unknown, enter four zeros (0000); e.g., "123450000." If the sponsor does not reside in one of the 50 United States, the District of Columbia, or one of the listed trust territories, enter the applicable foreign ZIP Code, or APO or FPO number. If the sponsor is deceased or if ZIP Code is unknown, leave blank. (Use no more than nine characters.)

Block 15. Country. Enter the employee's correct country of residence from the valid abbreviations listed in Table 6. If the sponsor/employee's address is an APO or FPO, the country must be "US" (use two characters). If country is unknown, leave blank.

Block 16. Primary e-mail address. Enter the sponsor/employee's office/work e-mail address as applicable. This block may be left blank.

Block 17. Telephone Number. Enter the sponsor's current residence, duty, or business telephone number beginning with the area code. Do not use punctuation to separate area code, prefix, and basic number. This block may be left blank. (Use no more than 10 characters.)

Block 18. City of Duty Location. Enter the city of the sponsor/employee's duty location.

Block 19. State of Duty Location. Enter the correct U.S. postal code for the State of the sponsor/employee's duty location from the valid codes listed in Table 7. If the sponsor's address is an APO or FPO, enter the correct APO or FPO State. If the sponsor lives outside of the 50 United States, the District of Columbia, or one of the listed trust territories, enter a default value of "XX." (Use two characters.) If the sponsor is deceased or if State is unknown, leave blank.

Block 20. Country of Duty Location. Enter the correct Country of the sponsor/employee's duty location from the valid codes listed in Table 6 (use two characters.) If the country is not listed, leave blank.

SECTION II – SPONSOR/EMPLOYEE DECLARATION AND REMARKS.

Block 21. Remarks. Enter the method of verification and further explanation of qualifying status, such as SF 52, sponsoring agency, and period of DEERS enrollment. Indicate other appropriate comments, such as particular work assignment. This section may be left blank, or prepopulated by the Verifying Official.

Block 22. Sponsor/Employee Signature. Block must contain the sponsor/employee's signature, with the following exceptions:

1. Unremarried or Unmarried former spouses shall sign for themselves.
2. When the sponsor is deceased the survivors shall sign for themselves.
3. When the sponsor is unavailable for signature, the verifying official shall ensure that the dependency between the sponsor and family member exists. Verifying official shall follow the guidance provided in the applicable Uniformed Service regulation.

When the DD Form 1172-2 is not signed in the presence of the authorizing or verifying official at the time of DEERS enrollment, the signature must be notarized. The notary seal and signature should be placed in the right margin of Block 21, above.

Block 23. Date Signed. Enter the date four-digit year, three alpha-character month, and two-digit day format (YYYYMMDD) that block 22 was signed on the DD Form 1172-2.

SECTION III – AUTHORIZED BY (DoD CAC Sponsors Only).

Block 24. Sponsoring Office Name. Enter the name of the organization the employee works for or is assigned to.

Block 25. Contract Number. Enter the contract number for the purposes of entry into the Contractor Verification System (CVS).

Block 26. Sponsoring Office Address. Enter the number and street, city, state, zip code, and country code (see Table 6 for country codes) of the employee's sponsoring office address.

Block 27. Sponsoring Office Telephone Number. Enter the sponsoring office telephone number beginning with the area code. Do not use punctuation to separate area code, prefix, and basic number. (Use no more than 14 characters.)

Block 28. Office Email Address. Enter the sponsor's office e-mail address as applicable..

Block 29. Overseas Assignment. Enter the employee's country of assignment from the valid list of abbreviations in Table 6.

Block 30. Overseas Assignment Begin Date. Enter the appropriate employee's effective begin date four-digit year, three alpha-character month, and two-digit day format (YYYYMMDD) for their overseas assignment. Obtain this information from the employee's personnel documents authorizing their employment overseas.

Block 31. Overseas Assignment End Date. Enter the appropriate employee's effective end date four-digit year, three alpha-character month, and two-digit day format (YYYYMMDD) of their overseas assignment. The period of employment may be obtained from the employee's orders authorizing their employment overseas.

Block 32. Eligibility Effective Date. Enter the date four digit year, three alpha-character month, and two-digit day format (YYYYMMDD) the employee's qualifying status began.

Block 33. Eligibility Expiration Date. Enter the appropriate employee effective end date, not to exceed three years. Use four-digit year, three alpha-character month, and two-digit day format (YYYYMMDD).

Block 34. Sponsoring Official Name. Enter the name of the sponsoring official. (Use no more than 51 characters.)

Block 35. Unit/Organization Name. Enter the unit and/or command name for the sponsoring official. (Use no more than 26 characters.)

Block 36. Title. Enter the sponsoring official's title. (Use no more than 24 characters.)

Block 37. Pay Grade. Enter the pay grade of the sponsoring official (Use no more than four characters.)

Block 38. Signature. The sponsoring official must sign in that block. The DoD sponsoring official shall be a uniformed service member, or civilian employee working for the sponsoring civilian organization.

Block 39. Date Verified. Enter the date four-digit year, three alpha-character month, and two-digit day format (YYYYMMDD) that block 38 was signed on the DD Form 1172-2.

SECTION IV – DEPENDENT INFORMATION

Section A (Block 40-51)

Block 40. Name. Enter the dependent's LAST name first, enter the FIRST name, and then enter the MIDDLE INITIAL or the full MIDDLE NAME. (Use no more than 51 characters.) The name field can include a designation of JR, SR, ESQ, or the Roman numerals I through X. To include that designation, enter the appropriate data after the middle initial. The name cannot contain any special characters nor is any punctuation permitted.

Block 41. Gender. Enter the dependent's gender from the valid codes listed in Table 1 (Use one character.)

Block 42. Date of Birth. Enter the dependent's date of birth in four-digit year, three alpha character month, and two-digit day format (YYYYMMMDD).

Block 43. Relationship. Enter the correct abbreviation to show the dependent's relationship to the sponsor from the valid abbreviations listed in Table 9.

Table 9. DD Form 1172 Block 43. Relationship

CODE	RELATIONSHIP STATUS
CH	Child
SC	Stepchild
URW	Unremarried Widow(er)
UMW	Unmarried Widow(er)
PL	Parent-in-law
SPL	Stepparent-in-law
PAR	Parent
STP	Stepparent
SP	Spouse
WARD	Legal Ward
DB	Designated Beneficiary

Block 44. SSN or DoD ID No. Enter the dependent's SSN, DoD ID number, ITIN or temporary identification number (TIN). A TIN will automatically be assigned and automatically generated by RAPIDS for categories of beneficiaries who do not yet have SSNs, such as newborns and foreign spouses, awaiting a SSN, or for those who do not have and are not eligible for a SSN. Medical benefits may be suspended if a SSN is not provided within 270 days. For initial enrollment a SSN, ITIN or TIN is preferred, and an alternate should not be used unless the SSN, ITIN or TIN is unavailable.

Block 45. Current Home Address. Enter the number and street of the dependent's current residence address.

Block 46. City. Enter the dependent's current city of residence. If the dependent's address is an Army Post Office (APO) or a Fleet Post Office (FPO), enter the designation APO or FPO.

Block 47. State. Enter the correct U.S. postal code for the State of the dependent's residence from the valid codes listed in for block 10.

Block 48. Zip Code. Enter the correct nine-digit ZIP Code of the dependent's current residence address in the following format: "123456789." If the last four digits are unknown, enter four zeros (0000); e.g., "123450000." If the dependent does not reside in one of the 50 United States, the District of Columbia, or one of the listed trust territories, enter the applicable foreign ZIP Code, or APO or FPO number.

Block 49. Country. Enter the dependent's correct country of residence from the valid abbreviations listed in the instructions for Block 8. If the dependent's address is an APO or FPO, the country must be "US" (use two characters). If country is unknown, leave blank.

Block 50. Eligibility Effective Date. Enter the date four digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) the dependent's qualifying status began.

Block 51. Eligibility Expiration Date. Leave blank

Section B. Enter information following the instructions of Section A.

SECTION V

Block 64. Signature. Recipient must sign in that block. If the recipient is incapable of signing, the condition must be indicated in that block.

Block 65. Date Issued. Enter the date four-digit year, three alpha-character month, and two-digit day format (YYYYMMMDD) of recipient's acknowledgment. (Use nine characters.)

Appendix E TASS Email Notifications

I. Schedule for Contractor Reverification Notifications

Reverification Required – Initial Notification – First transmitted 150 days after CAC issued/CAC last verified

Dear {TA},

This message has been sent to notify you that you need to reverify the contractor ({Contractor Name}) requires his/her CAC. Please complete the verification process at the link below.

Questions may be sent via email to: dodhra.dodc-mb.dmdc.mbx.contractor-verification@mail.mil

TASS TA Website: <https://www.dmdc.osd.mil/tass>

Reverification Timeout Reminder – Transmitted 160 days after CAC issued/CAC last verified

Dear {TA},

This message has been sent to remind you the prescribed time to reverify contractor ({Contractor Name}) has arrived. Please complete the verification process as prescribed.

Questions may be sent via email to: dodhra.dodc-mb.dmdc.mbx.contractor-verification@mail.mil

TASS TA Website: <https://www.dmdc.osd.mil/tass>

Note this reminder will not be sent if application has been either reverified or revoked.

Reverification Timeout Warning – Transmitted 170 days after CAC issued/CAC last verified

Dear {TA},

This message has been sent to notify you the prescribed time to reverify contractor ({Contractor Name}) has arrived and that that action needs immediate attention. Please complete the verification process as prescribed. The time allotted for you to complete the verification will expire on {Date} at which time the contractor's Defense Enrollment Eligibility Reporting Service record will be terminated.

Questions may be sent via email to: dodhra.dodc-mb.dmdc.mbx.contractor-verification@mail.mil

TASS TA Website: <https://www.dmdc.osd.mil/tass>

Note this reminder will not be sent if application has been either reverified or revoked.

Reverification Expiration – Transmitted 180 days after CAC issued/CAC last verified

Dear {TA},

The time allotted to reverify contractor {Contractor Name} has expired. As a result, that account has been revoked and the Defense Enrollment Eligibility Reporting System has been updated to reflect the change.

Questions may be sent via email to: dodhra.dodc-mb.dmdc.mbx.contractor-verification@mail.mil

TASS Website: <https://www.dmdc.osd.mil/tass>

II. Batch Upload Success Notification

Dear {TA},

The Batch File Upload has Finished OK.

Batch execution details:

File Name....: 201201210001.xml

Batch ID....: 201201210001

Successful Count: 3

Error Count....: 0

Total Processed: 3

Execution Start Date/Time: 01/31/2012 15:42:54 Completion Date/Time....:01/31/2012 15:42:59

Questions may be sent via email to: dodhra.dodc-mb.dmdc.mbx.contractor-verification@mail.mil

TASS Web Site: <https://www.dmdc.osd.mil/tass/>

Appendix F Acronyms, Abbreviations, and Terms

Acronym	Description
C&A	Certification and Accreditation
CA	Certificate Authority
CAC	Common Access Card
ConOps	Concept of Operations
CVS	Contractor Verification System
DISA	Defense Information Systems Agency
DEERS	Defense Enrollment & Eligibility Reporting System
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoDI	Department of Defense Instruction
DSC	DMDC Support Center
DSO	DMDC Support Office
DST	DMDC Security Team
DTM	Directive-Type Memorandum
EBUSOPSOFF	eBusiness Operations Office (Navy)
EDI-PI	Electronic Data Interchange Person Identifier
EEPROM	Electronically Erasable Programmable Read Only Memory
EJB	Enterprise Java Bean
FAQ	Frequently Asked Question
FBI	Federal Bureau of Investigation
FIN	Foreign Identification Number
Government Sponsor	Active Duty member or Civil Servant who approves contractor CAC request
HSPD	Homeland Security Presidential Directive
HVDF	High Volume Data Feed
ICC	Integrated Circuit Chip
ID	Identification
ITIN	Individual Tax Identification Number
J2EE	Java v.2 Enterprise Edition
JSP	Java Server Page
LMS	Learning Management System

Acronym	Description
LOA	Letter of Authorization
MOA	Memorandum of Agreement
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NMCI	Navy Marine Corps Intranet
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POC	Point of Contact
RAPIDS	Real-time Automated Personnel Identification System
RSS	RAPIDS Self Service
S/A	Service/Agency
SOFA	Status-of-Forces Agreement
SPOT	Synchronized Predeployment & Operational Tracker
SSL	Secure Socket Layer
SSM	Site Security Manager (RAPIDS)
SSN	Social Security Number
TA	Trusted Agent
TASM	Trusted Agent Security Manager
TASS	Trusted Associate Sponsorship System
UCMJ	Uniform Code of Military Justice
URL	Universal Resource Locator
USID	Uniformed Services ID
VO	Verifying Official (RAPIDS)
XML	eXtensible Mark-up Language

Appendix G Alphanumeric Character Translations

It is important to communicate Applicant's password information clearly and securely. The following translations follow the military standard for communication of alphanumeric data. They will help you to transmit password characters that may be difficult to understand.

Letters	Translation
a	Lower case Alpha
A	Upper case Alpha
b	Lower case Bravo
B	Upper case Bravo
c	Lower case Charlie
C	Upper case Charlie
d	Lower case Delta
D	Upper case Delta
e	Lower case Echo
E	Upper case Echo
f	Lower case Foxtrot
F	Upper case Foxtrot
g	Lower case Golf
G	Upper case Golf
h	Lower case Hotel
H	Upper case Hotel
i	Lower case India
I	Upper case India
j	Lower case Juliett
J	Upper case Juliett
k	Lower case Kilo
K	Upper case Kilo
l	Lower case Lima
L	Upper case Lima
m	Lower case Mike
M	Upper case Mike
n	Lower case November
N	Upper case November
o	Lower case Oscar
O	Upper case Oscar
p	Lower case Papa
P	Upper case Papa
q	Lower case Quebec
Q	Upper case Quebec
r	Lower case Romeo
R	Upper case Romeo
s	Lower case Sierra
S	Upper case Sierra

t	Lower case Tango
T	Upper case Tango
u	Lower case Uniform
U	Upper case Uniform
v	Lower case Victor
V	Upper case Victor
w	Lower case Whiskey
W	Upper case Whiskey
x	Lower case X-ray
X	Upper case X-ray
y	Lower case Yankee
Y	Upper case Yankee
z	Lower case Zulu
Z	Upper case Zulu

Numbers	Translation
1	Number One
2	Number Two
3	Number Three
4	Number Four
5	Number Five
6	Number Six
7	Number Seven
8	Number Eight
9	Number Nine
0	Number Zero

Special Characters	Translation
(Left parenthesis
)	Right parenthesis
-	Dash
!	Exclamation Point
<	Left carat or Less-than sign
>	Right carat or More-than sign
#	Pound sign or Hash mark
\$	Dollar sign
%	Percent sign
&	Ampersand sign
*	Asterisk or Star
?	Question mark

Appendix H Documentation for DEERS Data Changes

I. DSO Name Correction Request Form

	<u>Today's date</u>
To:	DMDC Support Office (DSO) 800-361-2508 (Office) 831-644-9256 (Fax)
From:	<u>Your name</u> , TASS Trusted Agent <u>Your phone number</u> <u>Your email address</u>
Subj:	Request DEERS Records Correction (Name Change) 1. <u>Applicant's OLD name – first and last</u> has been entered into DEERS under Person Identifier (i.e., SSN, FIN, etc.) <u>Applicant's Person Identifier</u> . 2. The <i>new name</i> is <u>Applicant's NEW name – first and last</u> . 3. I am requesting that the <i>new name</i> , <u>Applicant's NEW name – first and last</u> , be updated in DEERS. Please contact me when this request has been completed.
Thank you,	
V/r	
<u>Your name</u>	<u>Your title</u>
TASS Trusted Agent	
<i>Page 1 of 1</i>	

II. DSO DOB Correction Request Form

<u>Today's date</u>
To: DMDC/DEERS Support Office 800-361-2508 (Office) 831-644-9256 (Fax)
From: <u>Your name</u> , TASS Trusted Agent <u>Your phone number</u> <u>Your email address</u>
Subj: Request DEERS Records Correction (Date of Birth) <ol style="list-style-type: none">1. <u>Applicant's name – first and last</u> has been entered into DEERS under two different Dates of Birth (DOB).2. The <i>correct</i> DOB listed in DEERS is <u>Correct DOB</u>.3. The <i>incorrect</i> DOB listed in DEERS is <u>Incorrect DOB</u>.4. I am requesting that <u>Applicant's name – first and last</u>'s DEERS records be updated accordingly.
Thank you,
V/r <u>Your name</u> , <u>Your title</u> TASS Trusted Agent
<i>Page 1 of 1</i>

III. DSO Person Identifier Correction Request Form

<u>Today's date</u>
To: DMDC Support Office (DSO) 800-361-2508 (Office) 831-644-9256 (Fax)
From: <u>Your name</u> , TASS Trusted Agent <u>Your phone number</u> <u>Your email address</u>
Subj: Request DEERS Records Correction Person Identifier (i.e., SSN, FIN, etc.) <ol style="list-style-type: none">1. <u>Applicant's name – first and last</u> has been entered into DEERS under two Person Identifiers (i.e., SSN, FIN, etc.).2. The <i>correct</i> Person Identifier listed in DEERS is <u>Correct Person Identifier</u>.3. The <i>incorrect</i> Person Identifier listed in DEERS is <u>Incorrect Person Identifier</u>.4. I am requesting that <u>Applicant's name – first and last</u>'s DEERS records be corrected.
Thank you,
V/r <u>Your name</u> , <u>Your title</u> TASS Trusted Agent
<i>Page 1 of 1</i>