Defense Security Service

Office of the Chief Information Officer

National Industrial Security Program (NISP) Central Access Information Security System (NCAISS) Project
NCAISS User Guide

HS0021-13-F-0035

CICN: 0000-DOC-GD-18135-00

October 1, 2014
Version 3.3.2

Table of Contents

1 INTRODUCTION 4

1.1 PURPOSE 4

1.2 GETTING STARTED 4

2 THE DSS NCAISS 5

2.1 ACCESSING DSS NCAISS 5

2.2 NCAISS LOGIN PAGE 5

2.2.1 Frequently Asked Questions 6

2.2.2 Contact DSS 7

2.2.3 Links - DSS Applications 8

2.2.4 Common Log-In Errors 9

3 SELF-ENROLLMENT 12

3.1 REQUEST A DSS NCAISS USER ACCOUNT 12

3.2 NEW ACCOUNTS – EMAIL NOTIFICATIONS 14

4 REGISTER CERTIFICATE 15

4.1 COMMON CERTIFICATE REGISTRATION ERRORS 17

4.1.1 Wrong Account ID or Password 17

4.1.2 Missing Account ID or Password 18

4.1.3 Click "Cancel" or No Certificate Inserted (if Using a CAC) 19

4.1.4 Certificate Already in Use 19

5 LOGIN TO DSS NCAISS 20

6 NAVIGATING THE DSS NCAISS HOME PAGE 22

6.1 DSS LOGIN INFORMATION 23

6.2 QUICK LINKS 23

6.3 SESSION EXPIRATION 24

7 UPDATE PROFILE DATA 25

7.1 ACCOUNT ATTRIBUTES 26

7.2 AUTHENTICATION QUESTIONS 30

8 REQUEST ROLES AND ACCESS 32

8.1 REQUEST AN NCAISS ROLE 32

8.2 REQUEST A PRIVILEGED NCAISS ROLE 35

9 APPROVING/REJECTING ACCOUNT REQUESTS 39

9.1 APPROVING NCAISS ROLE REQUESTS 40

9.2 APPROVING A PRIVILEGED NCAISS ROLE REQUEST 41

9.3 REJECTING A REQUEST 42

10 DELEGATING WORK ITEMS 44

11 LOGGING OUT 47

12 OBMS APPLICATION NCAISS USER GUIDE 49

12.1 ACCESSING OBMS 49

12.1.1 CAC/PKI Authentication from OBMS 49

12.1.2 CAC/PKI Authentication (to OBMS) from NCAISS 52

12.2 REQUESTING ACCESS TO OBMS 53

12.2.1 OBMS Internal User (DSS.mil) Account Request 53

12.2.2 OBMS External Government (non-DSS) Submitter User Access Request 56

12.2.3 OBMS External Contractor (Industry) Submitter User Access Request 58

12.3 REVIEWING AND APPROVING/REJECTING OBMS ACCESS REQUESTS 60

12.3.1 Sponsor Approval for OBMS Internal (DSS.mil) Access Requests 60

12.3.2 Sponsor Approval for OBMS External Government Submitter Access Requests 61

12.3.3 Sponsor Approval for OBMS External Contractor Submitter Access Requests 62

12.4 MANAGING OBMS USER ACCOUNTS 63

12.4.1 Managing OBMS Internal and External Government Submitter User Accounts 63

12.4.2 Managing OBMS External Contractor Submitter User Accounts 65

12.5 PRODUCE OBMS USER REPORT 66

13 STEPP APPLICATION NCAISS USER GUIDE 68

13.1 ACCESSING STEPP 68

13.1.1 CAC/PKI Authentication from the STEPP Homepage 68

13.1.2 CAC/PKI Authentication (to STEPP) from NCAISS 72

13.1.3 Username/Password Authentication (to STEPP) 73

13.2 FIRST TIME ACCESS TO STEPP VIA NCAISS (EXISTING STEPP USERS) 73

13.3 REQUESTING A STEPP USER ACCOUNT (VIA NCAISS) 75

13.4 CORRELATING ADDITIONAL STEPP ACCOUNTS 77

14 GLOSSARY 79

1 Introduction

The Defense Security Service (DSS) National Industrial Security Program (NISP) Central Access Information Security System (NCAISS) Solution is an externally-facing system where users can access their DSS NCAISS account via a single sign-on (SSO) capability. NCAISS Users login using Public Key Infrastructure (PKI) certificates (either a Common Access Card (CAC) or DoD-approved External Certification Authority (ECA) certificate). The system provides a centralized account management interface to create and manage user data across several integrated DSS applications. Through the self-enrollment and self-administration features, user access requests are reviewed and approved by several NCAISS role holders, based on the nature of the request. Once access requests are approved, users are able to access the different applications and resources that have been integrated with the NCAISS Solution using their PKI credentials.

1.1 Purpose

The purpose of this document is to provide step-by-step instructions to enable DSS NCAISS Users to use the system. This guide covers the following capabilities:

- Enrolling (self-registering) for a new NCAISS User account
- Registering a PKI certificate with a user's account
- Accessing the NCAISS using a PKI credential
- Navigating NCAISS
- Requesting additional NCAISS roles and Application Access
- Securing logging out of NCAISS
- Approving and rejecting work items (account/access requests)
- Delegating work items to another user

1.2 Getting Started

The DSS NCAISS is web-based and requires no application to be installed. However, before you begin using NCAISS, verify that Microsoft Internet Explorer (v7.0 or greater) is installed on your computer.

Once the user account is created and the user logs into NCAISS, the user will be able to request access to any integrated applications/resources and access those applications/resources to which they are authorized.

2 The DSS NCAISS

2.1 Accessing DSS NCAISS

Access the DSS NCAISS by copying and pasting this link (https://sso.dss.mil) into a web browser. The DSS NCAISS Disclaimer page is displayed, as shown in Figure 1. The user must accept the DSS Portal Disclaimer in order to access the login page.

Figure 1: NCAISS Disclaimer

2.2 NCAISS Login Page

As depicted in Figure 2, the DSS NCAISS Login page contains the following components:

- Login to DSS Portal
- Register CAC/ECA
- Self-Enrollment
- Threat Advisory
- Links - DSS Applications
- FAQs
- Page footer - Contact DSS link and other DoD links

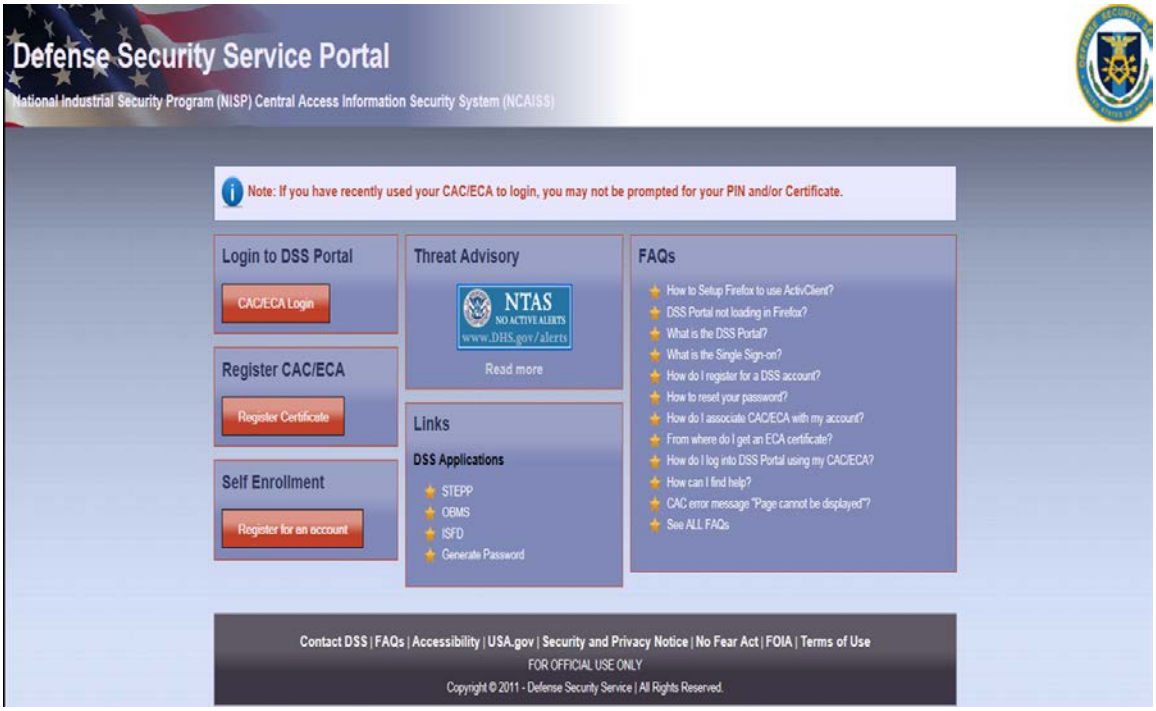


Figure 2: NCAISS Login Page

Use of the Login to DSS Portal, Register CAC/ECA, and Self Enrollment features are addressed in detail in Sections 5, 4, and 3, respectively. The following subsections address the Frequently Asked Questions (FAQs), contacting the Call Center, public information on the applications integrated into the DSS NCAISS Solution, and common errors when logging into the system.

2.2.1 Frequently Asked Questions

To view the Frequently Asked Questions (FAQs) page, click on the "**FAQs"** link at the bottom of the page (part of the page footer) or click on one of the questions in the FAQ box in the right column. Figure 3 illustrates where the FAQ links, on the DSS NCAISS Login Page, are located.

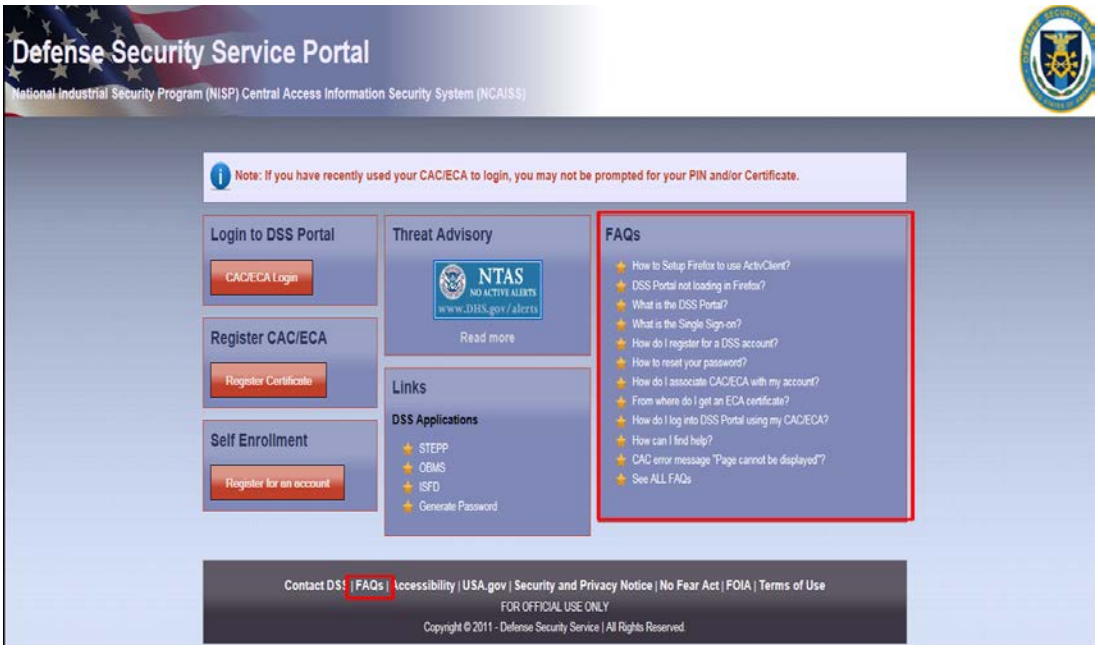


Figure 3: Location of FAQs

If the user clicks on one of the questions on the login page, the user will be redirected to the answer on the FAQ page. On the FAQ page, the user may scroll up and down the page to read the different questions and their corresponding answers, as shown in Figure 4.

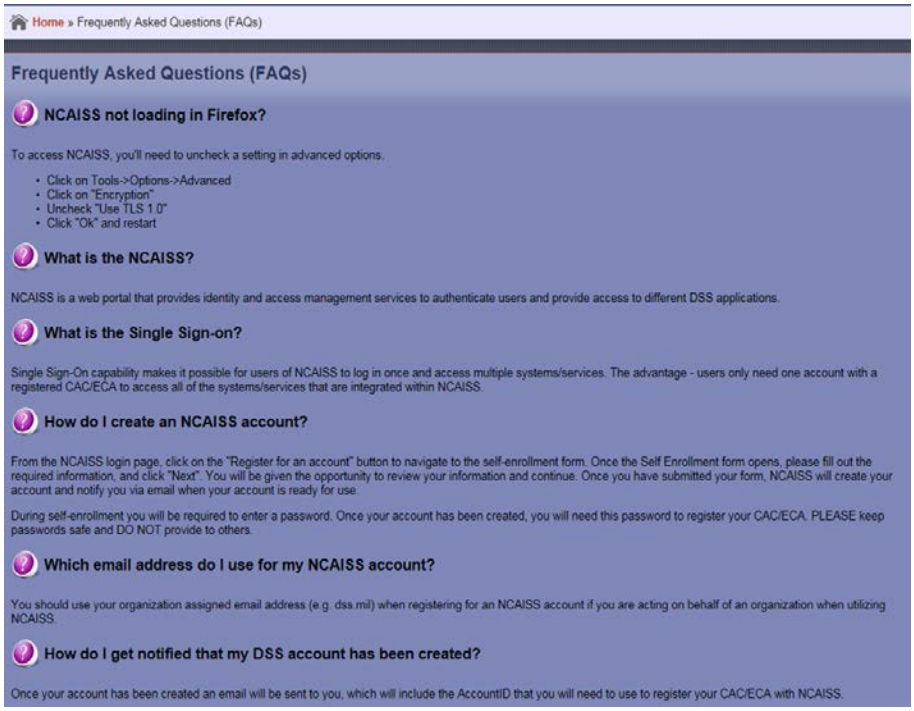


Figure 4: FAQ Responses

2.2.2 Contact DSS

To obtain contact information for the DSS Call Center, click the "Contact DSS" link at the bottom of the page. Figure 5 shows where this link is located.

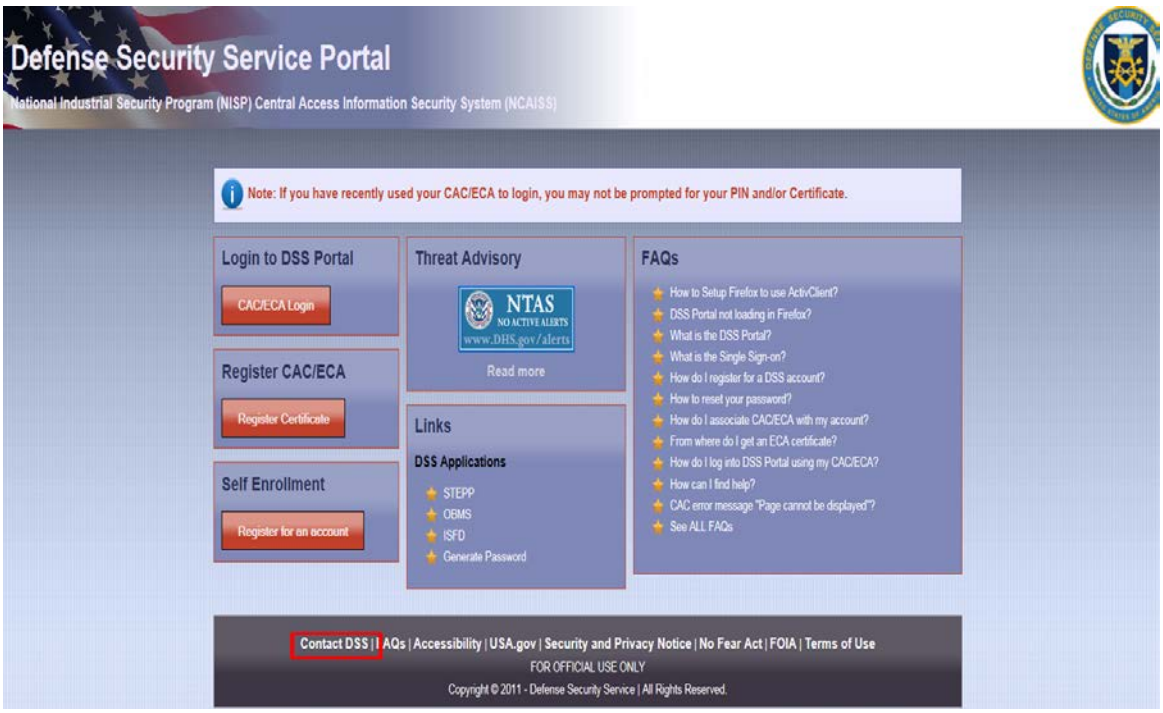


Figure 5: Contact DSS Location

The information required to Contact DSS is displayed, as shown in Figure 6.

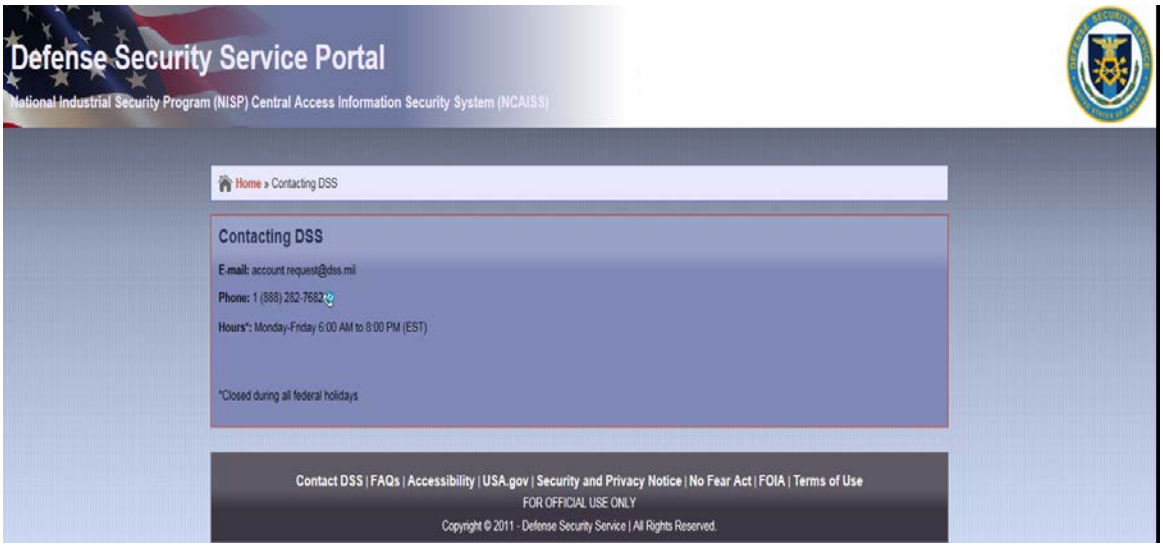


Figure 6: DSS Call Center Contact Information

2.2.3 Links - DSS Applications

The Links section is located in the lower center column of the login page, as depicted in Figure 7**.** This section lists the DSS applications that are integrated into the DSS NCAISS and provides links to relevant sources of information about those applications. When clicking on an application link, a page will be displayed showing public information on the selected application. **Note:** to gain access to an integrated application you must submit an access request, as described in Section 8.

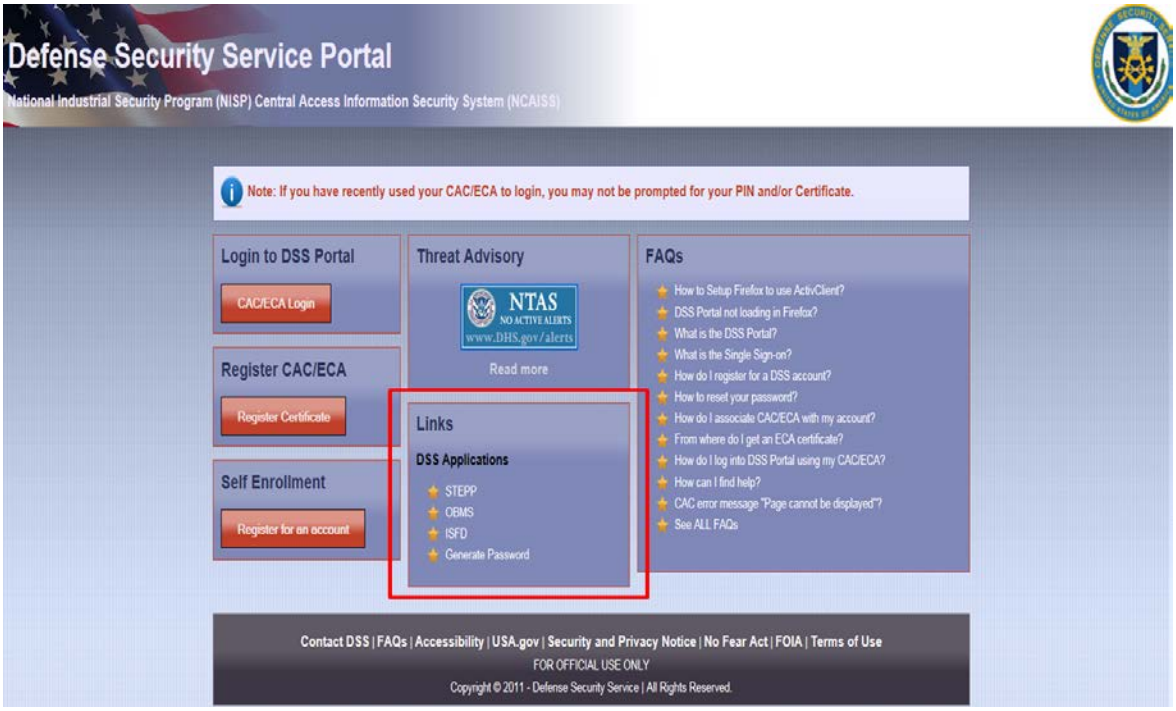


Figure 7: Links Location

2.2.4 Common Log-In Errors

When logging into NCAISS, there are a number of common errors that a user may encounter. This section addresses the following errors that may occur during NCAISS login:

- No Certificate Registered
- Clicking "Cancel" when selecting your certificate
- No account use after 90 days
- Session is idle for 30 minutes

2.2.4.1 No Certificate Registered

The user will see the error shown at the top of the login page (depicted in Figure 8) when he/she tries to login to their NCAISS account before registering their certificate (i.e., CAC or ECA).

Figure 8: Certificate Not Registered Error Message

To resolve this problem:

- If you have not registered your CAC or ECA, then follow the instructions to do so in Section 4
- If you have registered your CAC or ECA, then:
  - Ensure that you selected the correct certificate during the certificate selection process; and/or
  - Re-register your certificate.

2.2.4.2 Clicking "Cancel" When Selecting Your Certificate

Clicking "Cancel" when the certificate selection window is displayed will result in an authentication failed error message, as shown in Figure 9.

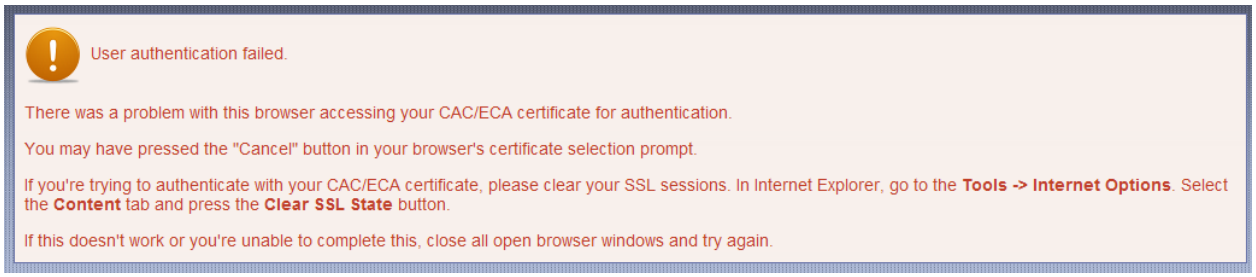


Figure 9: Authentication Failure Error Message

To resolve this problem:

- Select a certificate from the selection window.

2.2.4.3 No Account Use After 90 days

When the user does not access NCAISS within 90 days of their last login, an email is sent to the user notifying him/her that their account will be disabled in 5 days and will have to be reactivated by the Call Center. If the user's account becomes disabled, the "User is not active" message will be displayed, as shown in Figure 10.

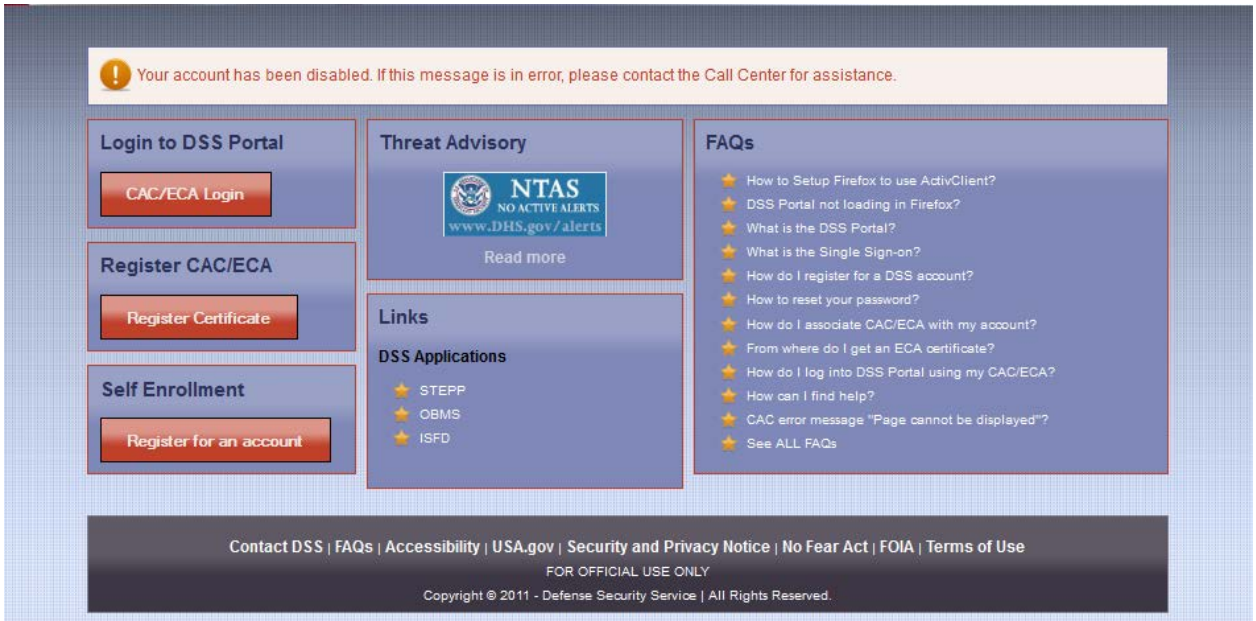


Figure 10: Inactive User Account Error Message

If the user account is disabled due to inactivity, then the user must contact the DSS Call Center by clicking the "Contact DSS" link at the bottom of the NCAISS Login Page.

2.2.4.4 Login Page is Idle for 30 Minutes

When logged into NCAISS, your account will be automatically logged out after 30 minutes of inactivity due to security requirements. When this occurs NCAISS will display a log out message, as shown in Figure 11.

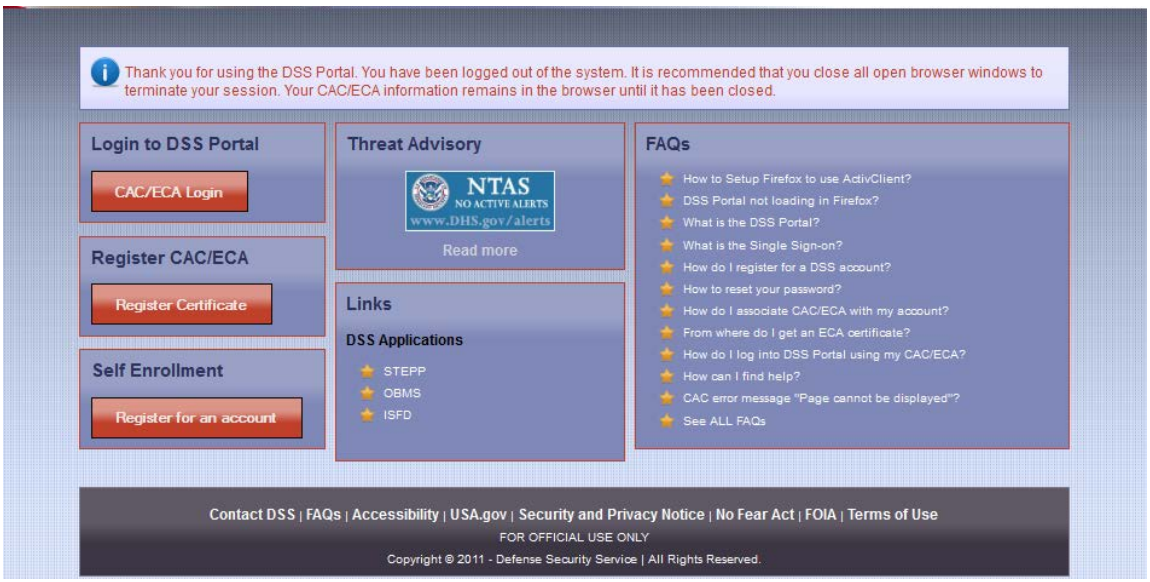


Figure 11: NCAISS Log Out Message

To resolve this problem:

- Reconnect to the DSS NCAISS homepage
- Click “I Accept” on the “DSS Portal Disclaimer”
- Click “CAC/ECA Login” and login using your PKI credential

3 Self-Enrollment

To gain access to the DSS NCAISS, a user must first register for an NCAISS User account (i.e., self-enroll). The self-enrollment module enables the user to complete a registration request and create a new user account. **Note:** If you are acting on behalf of an organization when utilizing NCAISS, you must use your organization assigned email address (e.g. dss.mil) when registering for an NCAISS account.

3.1 Request a DSS NCAISS User Account

The following steps outline the process for self-enrolling for a DSS NCAISS User account:

1. Access the DSS NCAISS by copying and pasting this link (https://sso.dss.mil) into your web browser.
2. Click "I Accept" on the DSS Portal Disclaimer, as shown in Figure 1.
3. On the DSS NCAISS Login page, click "Register for an account" under the "Self Enrollment" section of the bottom left corner, as shown in Figure 12.

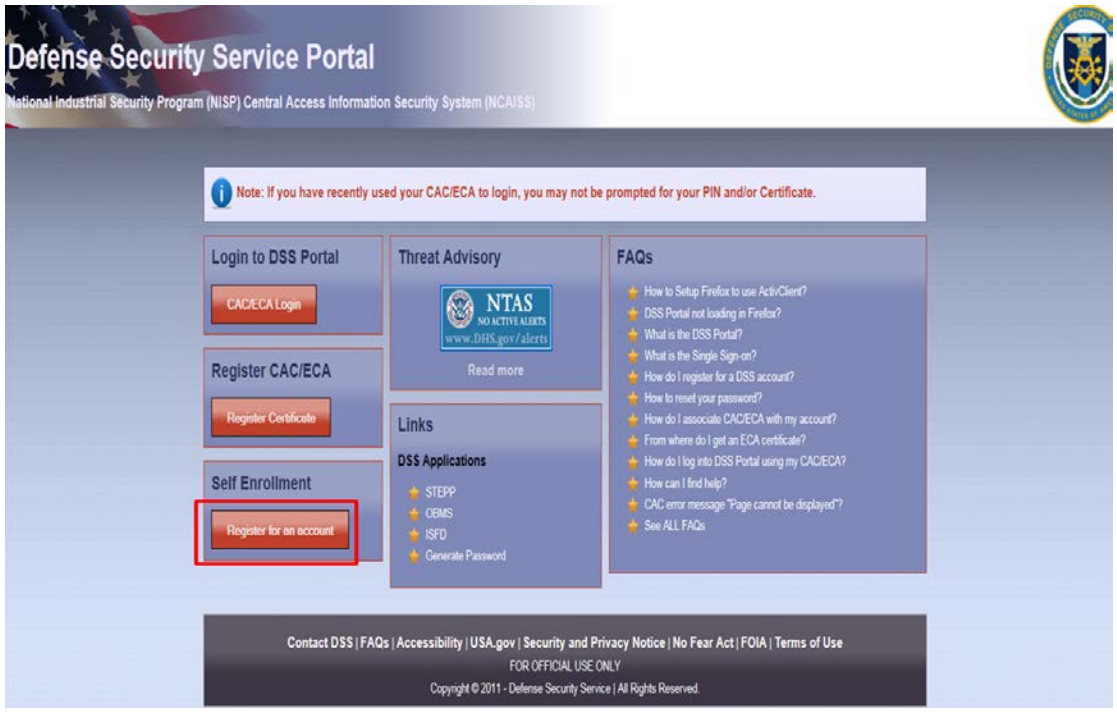


Figure 12: Register for an Account Link

4. Complete the required fields (noted with an "*"), as shown in Figure 13.
5. Answer a minimum of three (3) security questions. **Note:** When contacting the Call Center for support, the Call Center Agent may ask you these questions to verify your identity.
6. Perform one of the following actions:
    a. Click "Cancel" button to cancel the enrollment request. **Note:** Any information that you provided will be deleted.
    b. Click "Next" button to proceed with the self-enrollment process. **Note:** If any required information is not complete, NCAISS will not allow the user to continue with self-enrollment.

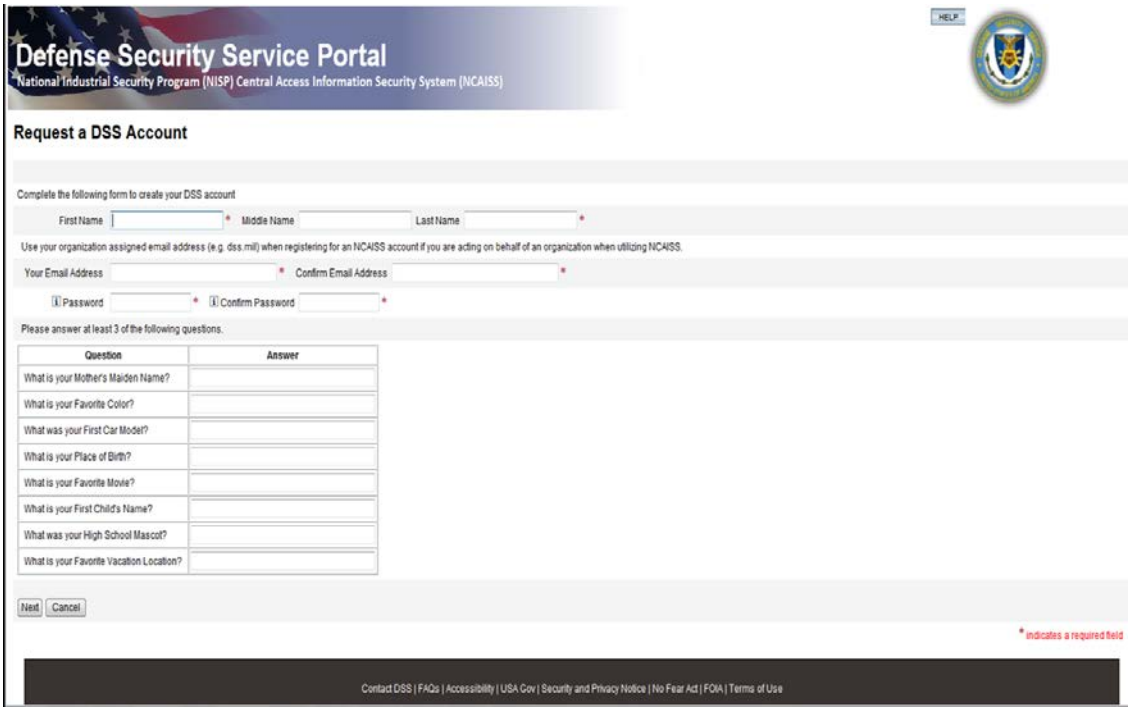


Figure 13: NCAISS Account Request Form

7. Review the information and perform one of the following actions, as shown in Figure 14:
    a. Click "Edit" to modify your information.
    b. Click "Cancel" to cancel the enrollment request. **Note:** Any information that you provided will be deleted.
    c. If the information is complete and accurate, then select the checkbox confirming you have read and agree to the Privacy Act Statement and click "Register" to submit the form.

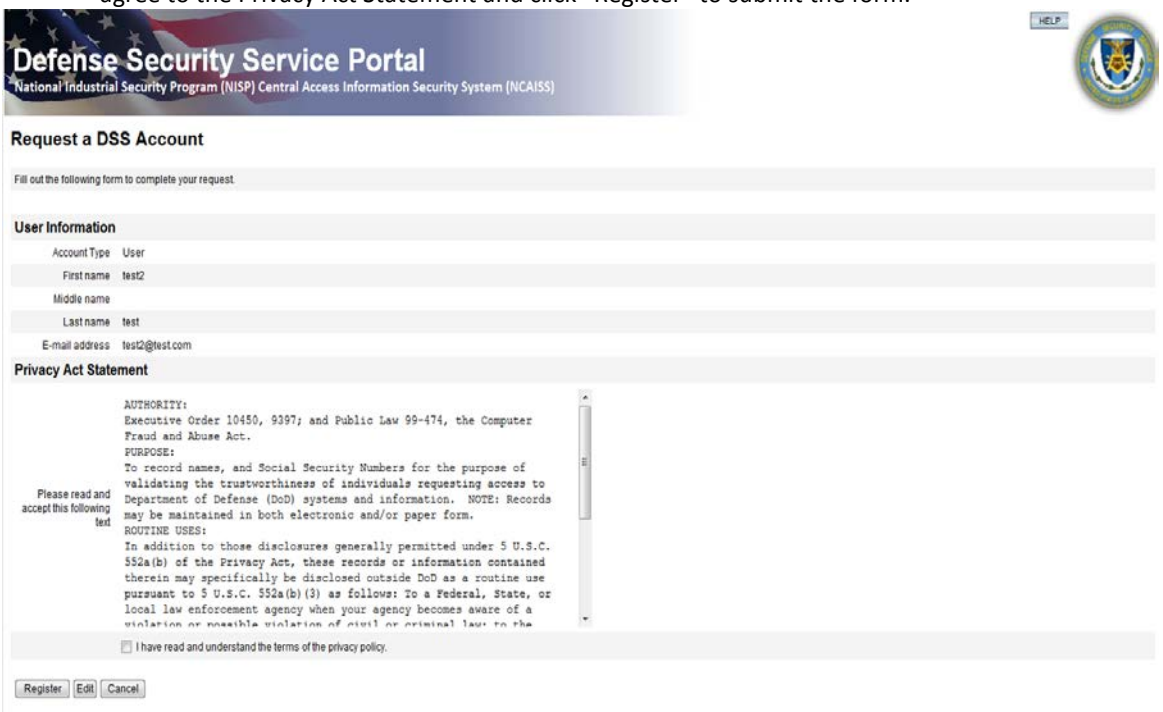


Figure 14: NCAISS Account Request Review

8. Upon clicking “Register” the request will be submitted and NCAISS will display a confirmation page, as shown in Figure 15.
9. Click “OK” to return to the DSS login page. **Note:** Your form is now submitted. Shortly, you will receive an email indicating that your account has been successfully created.

Figure 15: NCAISS Account Request Confirmation

3.2 New Accounts – Email Notifications

After a user submits NCAISS account request form and NCAISS creates the new user account, an email notification is sent to the user indicating successful account creation, as shown in Figure 16. **Note:** Your new account name (Account ID) is provided in this email. You created your password during the self-enrollment process.

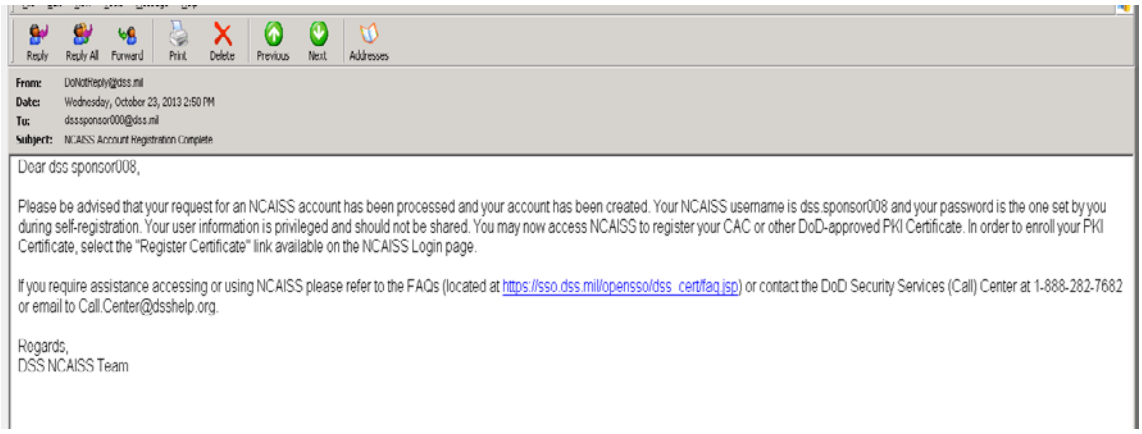


Figure 16: NCAISS Account Created Email

4 Register Certificate

The DSS NCAISS is a CAC/PKI-enforced system. To log into the system, users must use their CAC/ECA certificate and enter their Personal Identification Number (PIN). Prior to accessing the DSS NCAISS, all new users must register their certificate (i.e., associate their certificate to their NCAISS Account ID). This process takes place after a user's request for an account is approved and a user Account ID is created.

Note: Your new Account ID is provided in the "account created" notification email, shown in Figure 16.

Note: You already created your password when completing the "self-enrollment" form.

1. Access the DSS NCAISS by copy and pasting this link (https://sso.dss.mil) into your web browser.
2. Accept the DSS Portal Disclaimer, as shown in Figure 1.
3. On the DSS NCAISS Login page, click "Register Certificate" under the Register CAC/ECA section located in the middle of the left column. Refer to Figure 17.

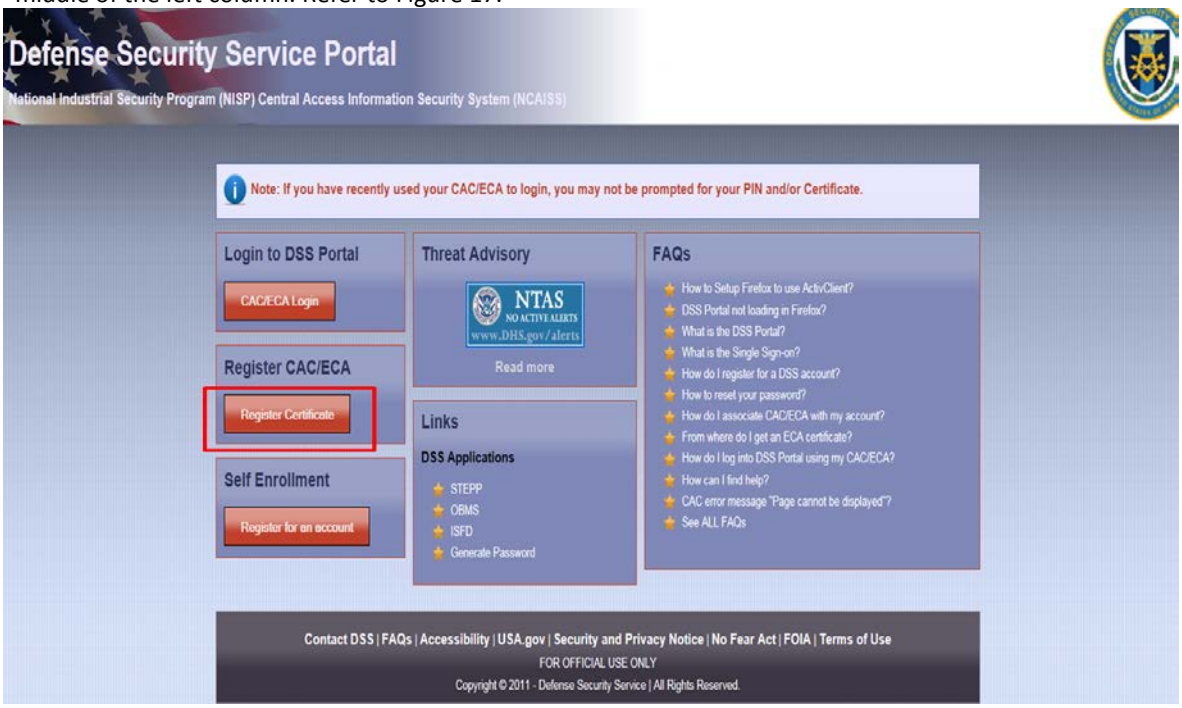


Figure 17: Register Certificate Location

4. Enter your Account ID (provided in your account creation notification email).
5. Enter the password that you set during the self-enrollment process.
6. Click "Submit,"

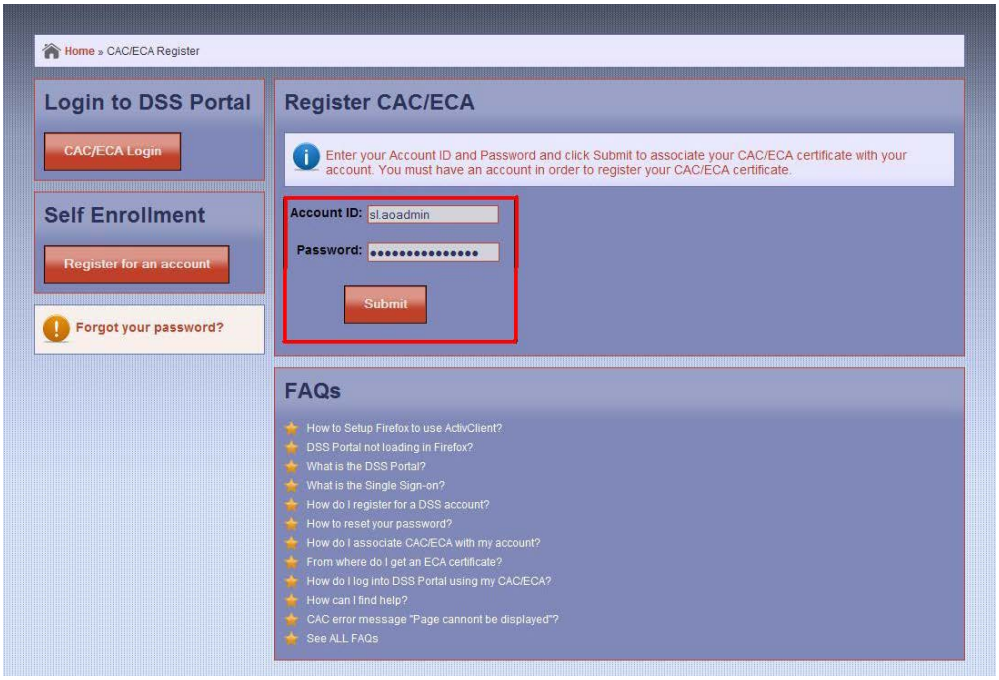


Figure 18: Register Certificate Screen

7. Upon clicking submit, a pop-up box containing a list of digital certificates will appear. Select your certificate, as shown in Figure 19. **Note:** If the window displays more than one certificate, scroll through the list and select the appropriate one.

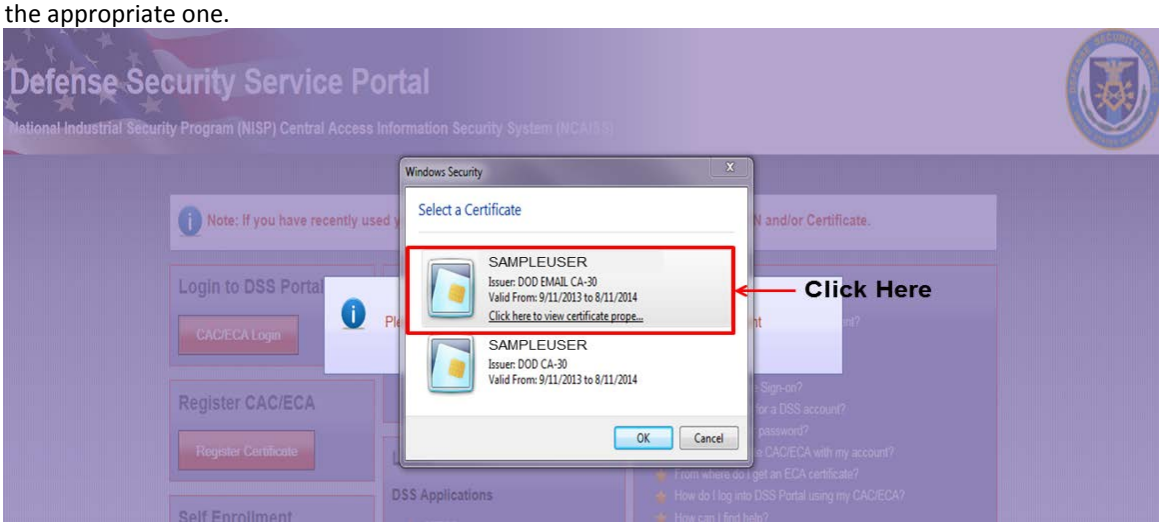


Figure 19: Certificate Selection

8. Enter your PIN, as shown in Figure 20.

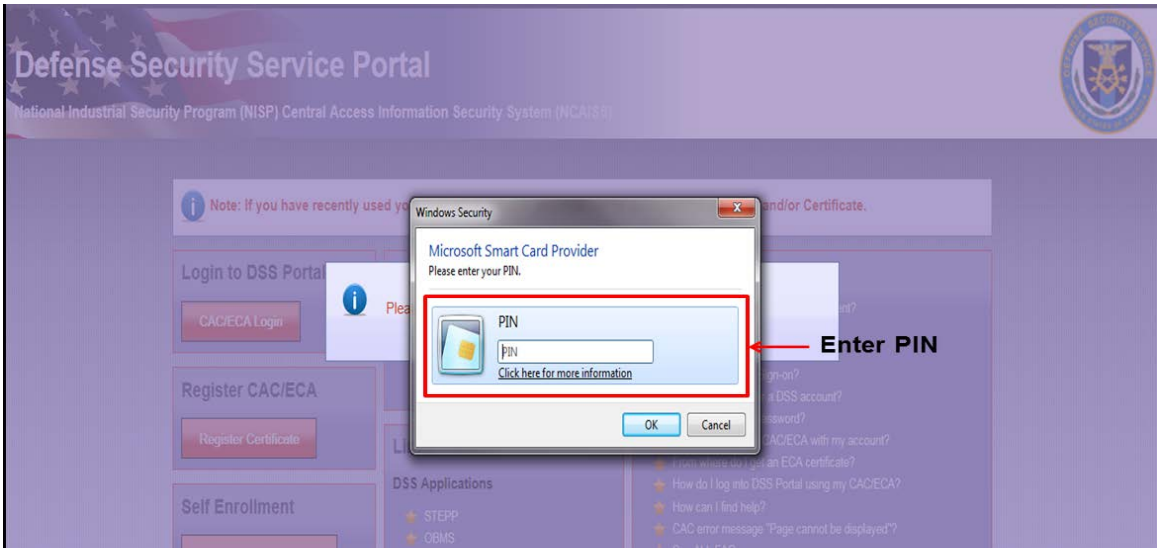


Figure 20: Certificate PIN Entry

9. If successful, a confirmation message will be displayed informing you that your certificate was registered successfully, as shown in Figure 21. You may now login to NCAISS.

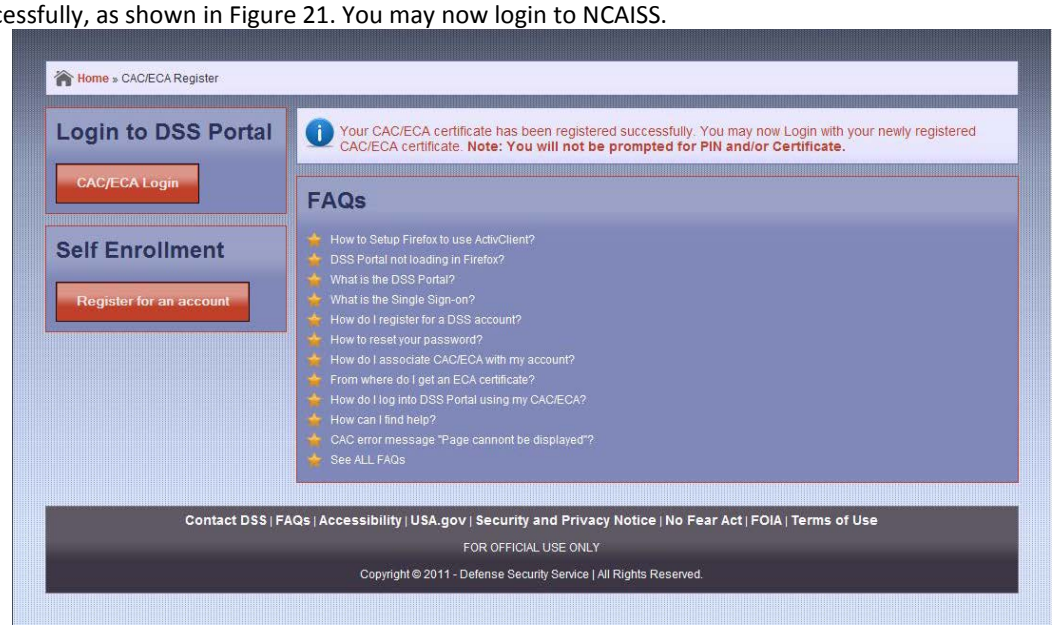


Figure 21: Successful Certificate Registration

4.1 Common Certificate Registration Errors

This section addresses the following errors that may occur during the PKI certificate registration process:

- Wrong Account ID or password
- Submitting without entering an Account ID or password
- Clicking "Cancel" button or no certificate is inserted (if using a CAC)
- Certificate already in use

4.1.1 Wrong Account ID or Password

An error message, as shown in Figure 22, is displayed when the user enters the wrong Account ID or Password when attempting to register a certificate.

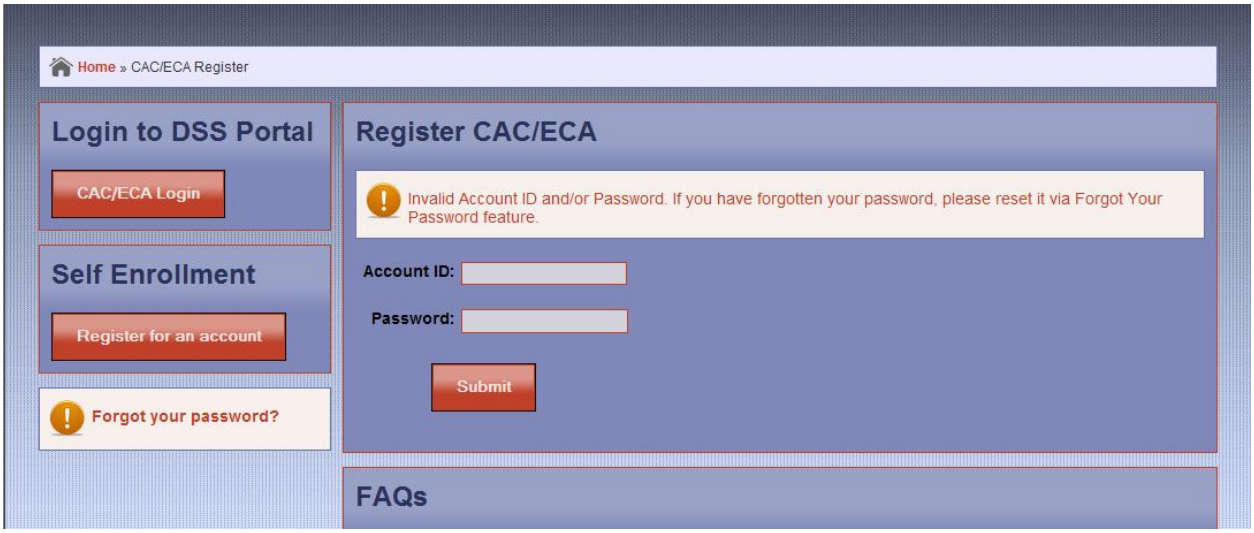


Figure 22: Invalid Account ID or Password During Certificate Registration

To resolve this problem:

- Make sure your Account ID and Password are correct:
  - To reset your password, contact the DSS Call Center
  - Click on the "Contact DSS" link at the bottom of the page

4.1.2 Missing Account ID or Password

One of the following two messages, as shown in Figure 23 and Figure 24, will be displayed when a user clicks "Submit" without entering an Account ID or password.

Figure 23: Missing Account ID

Figure 24: Missing Password

To resolve this problem:

- Enter the Account ID that was provided in the account creation notification email and the password that you created during self-enrollment.

4.1.3 Click "Cancel" or No Certificate Inserted (if Using a CAC)

An error message is displayed when the user selects "Cancel" or when no CAC is inserted into the computer, as shown in Figure 25.

Figure 25: No Certificate Selected Error

To resolve this problem:

- Please select the appropriate certificate; or
- Insert your certificate (CAC) into your computer or smartcard reader

4.1.4 Certificate Already in Use

A certificate may only be registered to a single NCAISS User account. If you have already registered your certificate to your account, then the system will display the following error message:

Figure 26: Certificate Already In-Use Error

To resolve this problem:

- Select CAC/ECA Login and log into the system using your certificate and PIN. Refer to Section 5, for more details on how to login.

5 Login to DSS NCAISS

Once a user's NCAISS User account has been created and a certificate is registered to the account, the user may log into the DSS NCAISS.

1. Access DSS NCAISS by copy and pasting this link (https://sso.dss.mil) into your web browser.
2. Accept the DSS Portal Disclaimer, as shown in Figure 1.
3. On the DSS NCAISS Login page, click "CAC/ECA Login" under the "Login to DSS Portal" section in the top left column. Refer to Figure 27.

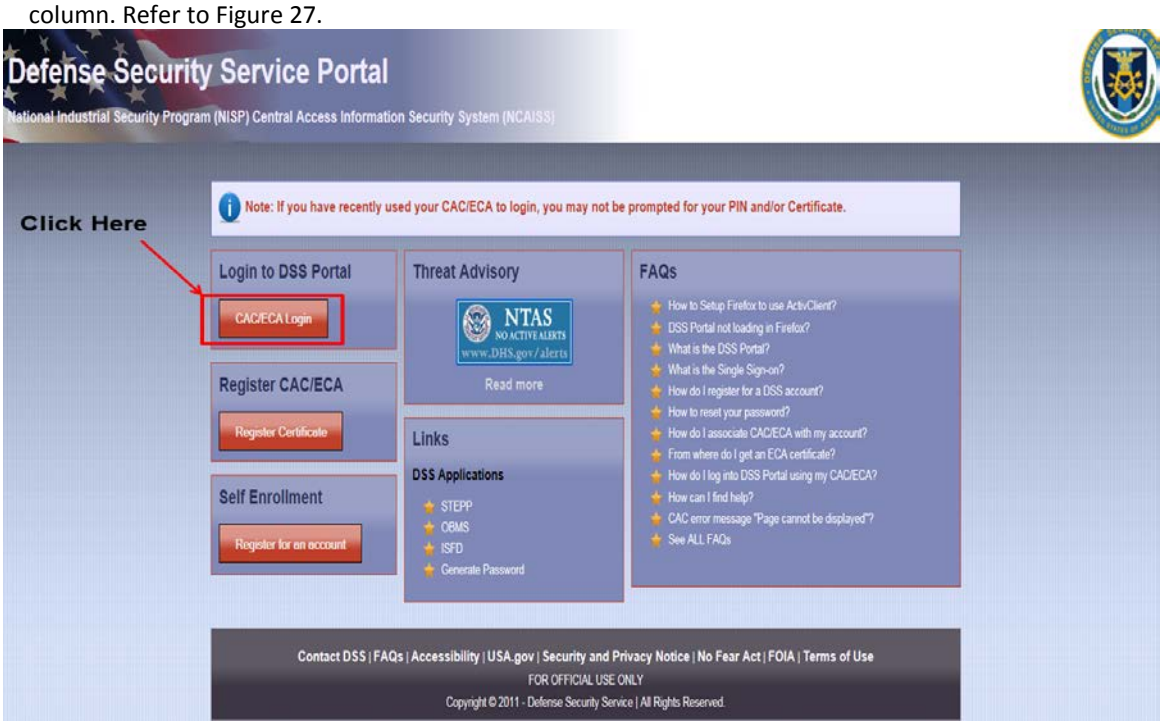


Figure 27: CAC/ECA Login Location

4. A window will pop up displaying one or more certificates on your system. Select your certificate. **Note:** Make sure you select the certificate that you registered to your Account ID.

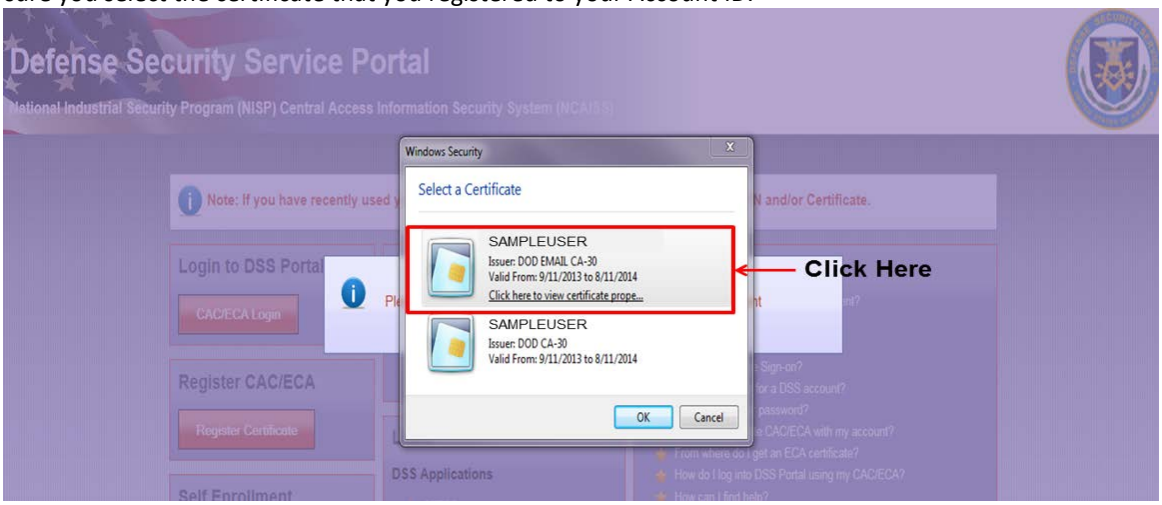


Figure 28: Login to NCAISS - Certificate Selection

5. Enter your PIN.

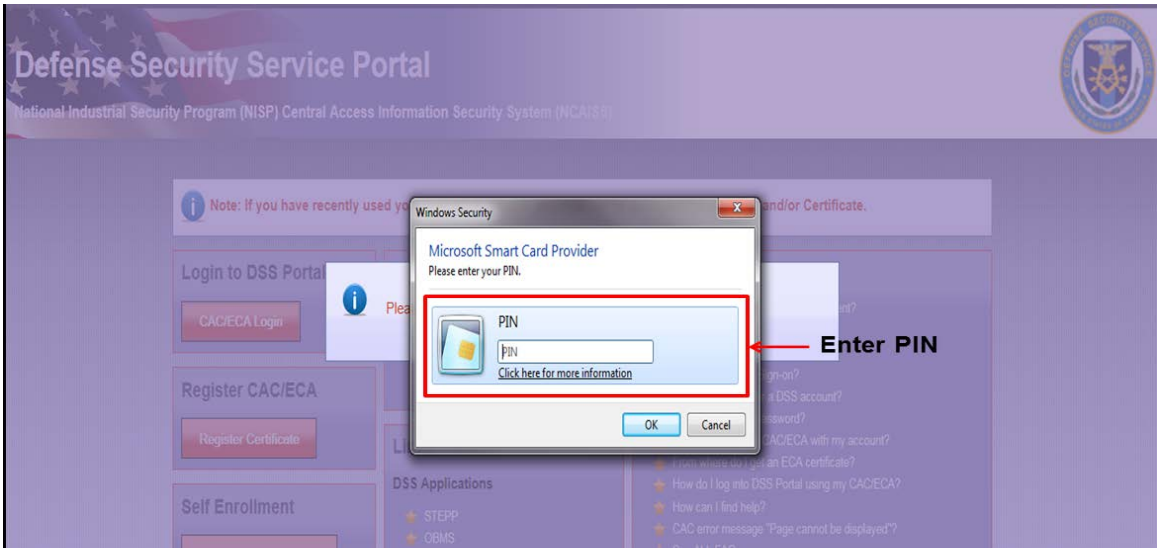


Figure 29: Login to NCAISS - Certificate PIN Entry

6. You have successfully logged in and will be directed to the DSS Portal Home Page, as shown in Figure 30.

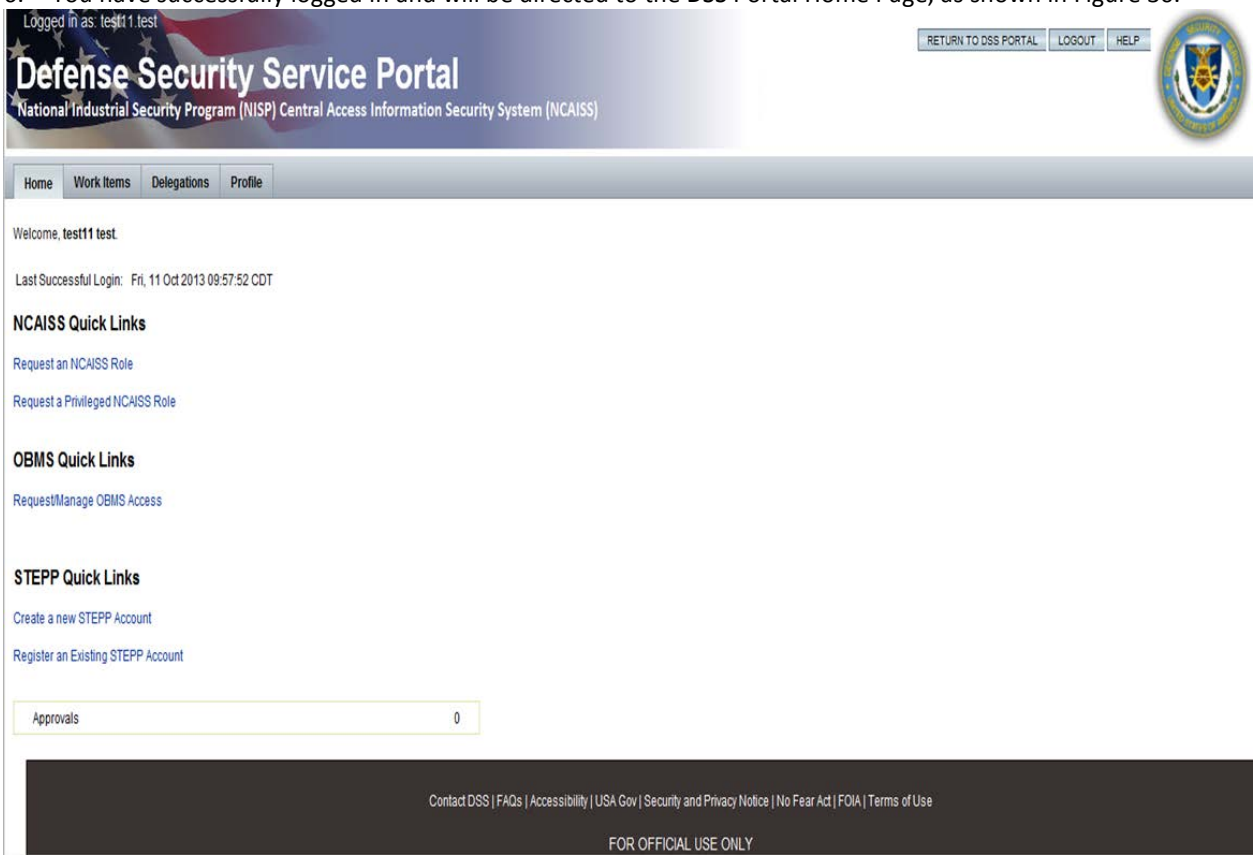


Figure 30: DSS Portal Home Page

6 Navigating the DSS NCAISS Home Page

The DSS NCAISS Home Page enables users to access the systems/applications/resources for which they have been authorized. As depicted in Figure 31**,** the home page tabs (at the top of the page) provide access to various capabilities within NCAISS. All DSS NCAISS users have access to a standard set of tabs that allow them to perform basic functions within the NCAISS Solution, including:

- Home – active by default upon login, clicking this tab returns users to the NCAISS Home Page
- Work Items – allows users to view/manage any access requests for which they serve as a Sponsor or Approver (see Section 9)
- Delegations – enables a user to temporarily delegate work items to another DSS NCAISS user (see Section 10)
- Profile – allows a user to view/manage their user information (see Section 7)

Depending on the user's privileges, additional tabs are displayed at the top of the home page representing additional NCAISS components that the user can access, including:

- IA User – allows a DSS information security official access to various reports and auditing capabilities (see the IA Account User Guide for additional information)
- Call Center – enables a DSS Call Center agent to perform administrative/support services within the NCAISS (see Account Administrator User Guide for additional information)

Every page within the NCAISS Solution has the "Return to DSS Portal" button in the top right corner of the screen. Clicking this button will return the user to his/her NCAISS Home Page. **Note:** Clicking the "Return to DSS Portal" button while on the NCAISS Home Page will refresh the screen.

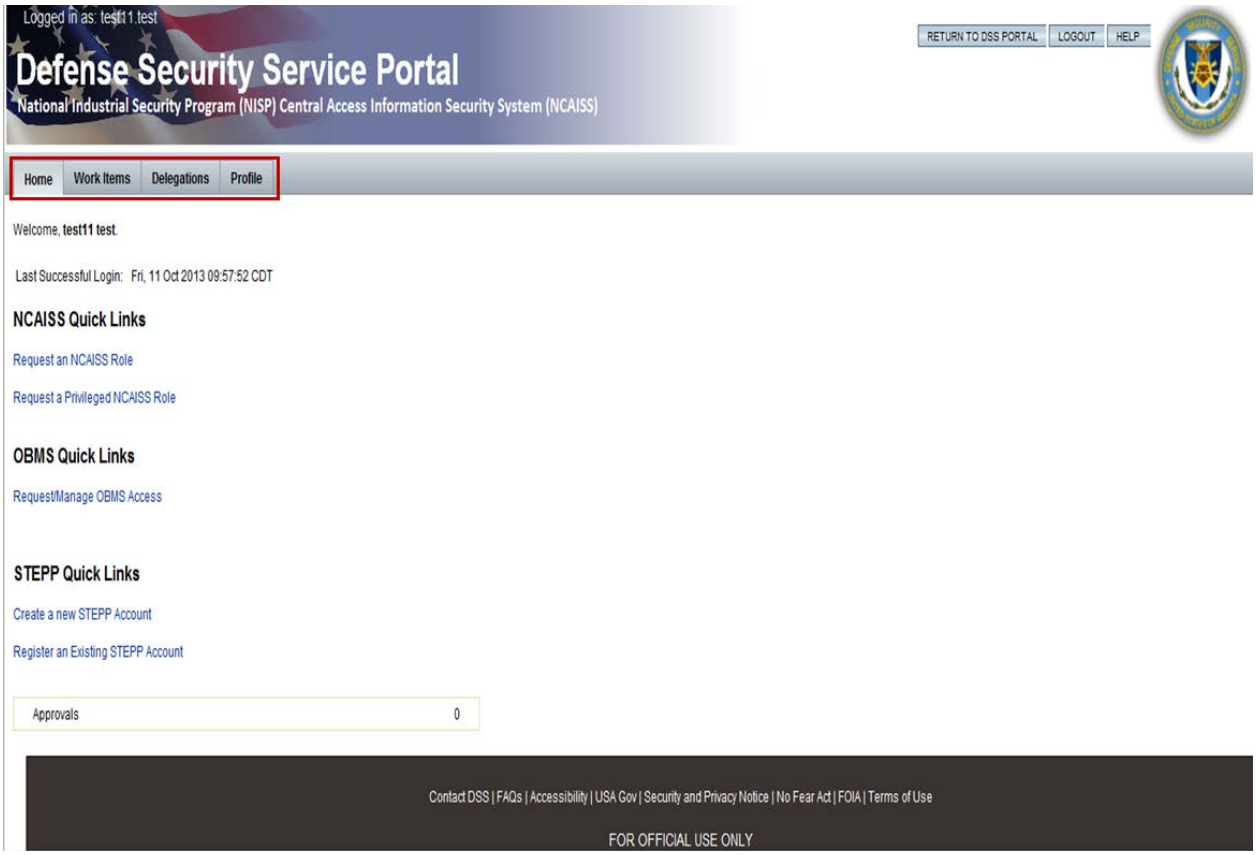


Figure 31: NCAISS Home Page Tabs

The remainder of this section provides overview information for locating and using the different components/applications on the NCAISS Home Page.

6.1 DSS Login Information

The DSS Login Information lists the last time the user was successfully logged into NCAISS. This function is located at the top left corner of the DSS NCAISS Home Page. Figure 32 highlights the "DSS Login Information" on the home page.

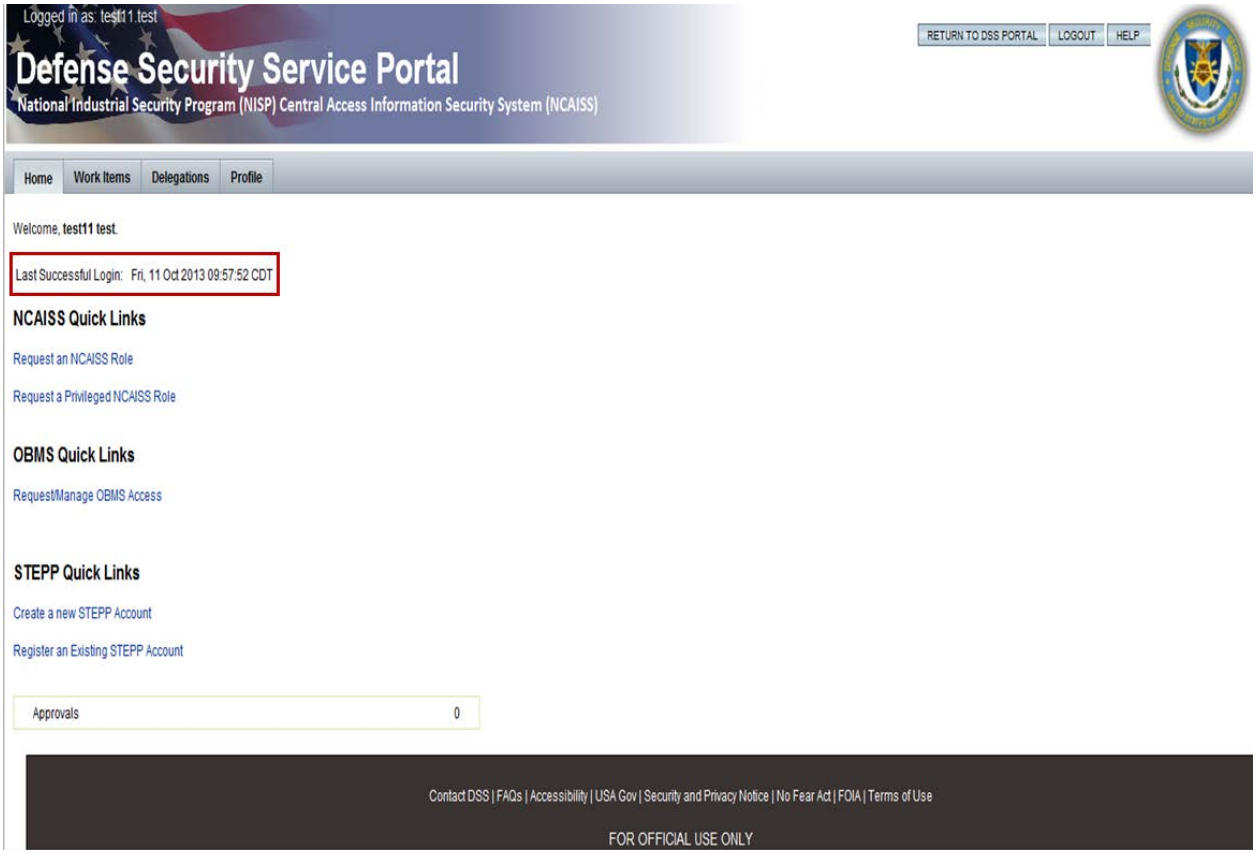


Figure 32: NCAISS Home Page Login Information

6.2 Quick Links

The main component of the DSS NCAISS Home Page is the "Quick Links" section, which provides users with hyperlinks to request additional NCAISS roles, request access to integrated applications, and access application-specific functionality, where it exists. The "Quick Links" section is located below the "DSS Login Information," as depicted in Figure 33. In order to support ease of navigation, the "Quick Links" are broken down into topic-specific sub-groups, as follows:

- NCAISS Quick Links
- Application-specific (e.g., OBMS) Quick Links

Note: Quick links are dynamic and displayed to users based on their particular permissions for the system (e.g., NCAISS Quick Links are only available for DSS users); additional application-specific sub-groups of "Quick Links" will appear on the DSS NCAISS Home Page as new applications are integrated with the NCAISS Solution. Step-by-step instructions for using the "Quick Links" are provided in subsequent sections of this document.

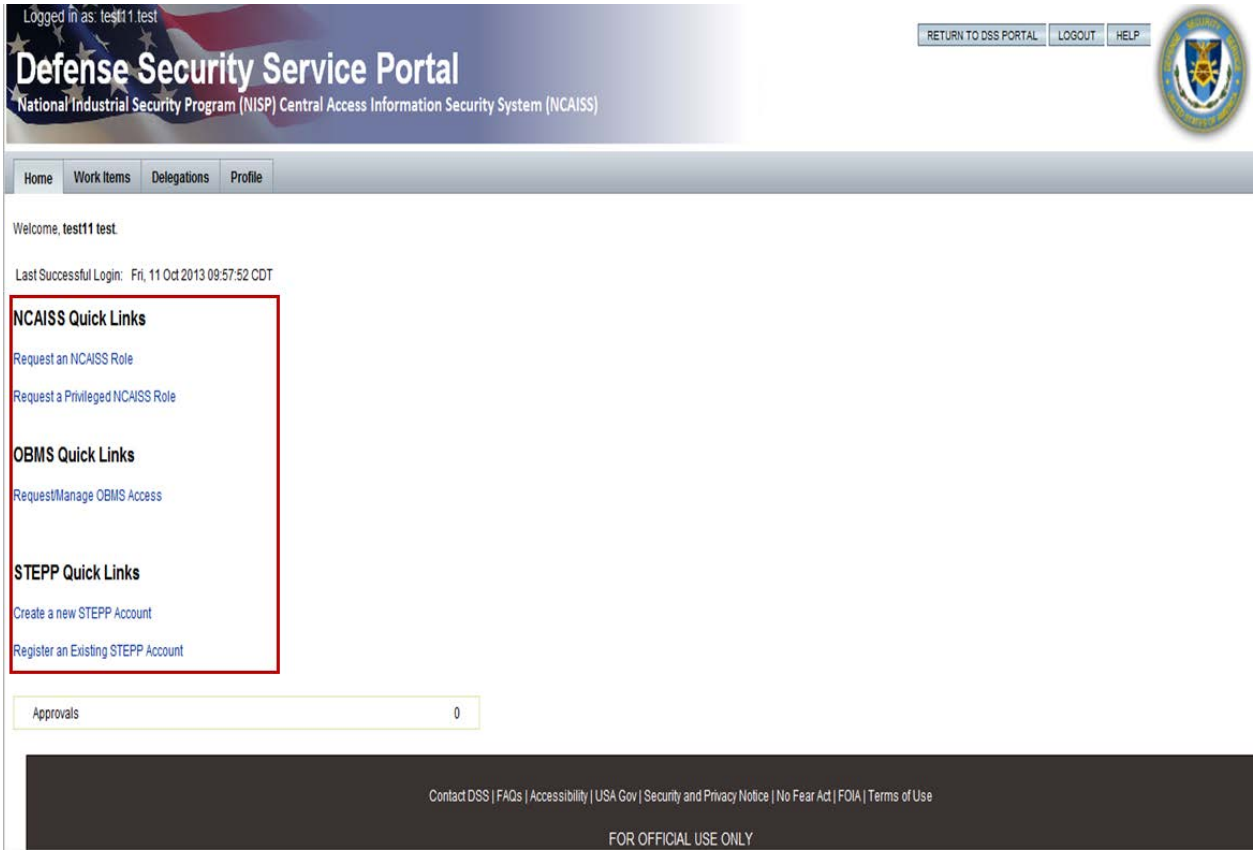


Figure 33: NCAISS Home Page Resource Links

6.3 Session Expiration

A user's NCAISS session will timeout when it sits idle for more than 30 minutes. If you wish to terminate your session, you may do so by:

- Clicking on the "Logout" button in the top right corner of the NCAISS Home Page;
- Allowing the session timeout to expire; or
- Exiting (closing) the web browser.

7 Update Profile Data

The "Profile" tab on the NCAISS Home Page allows users to view and update their profile information. The user profile information is accessed via the "Profile" tab at the top of the NCAISS Home Page, as depicted in Figure 34.

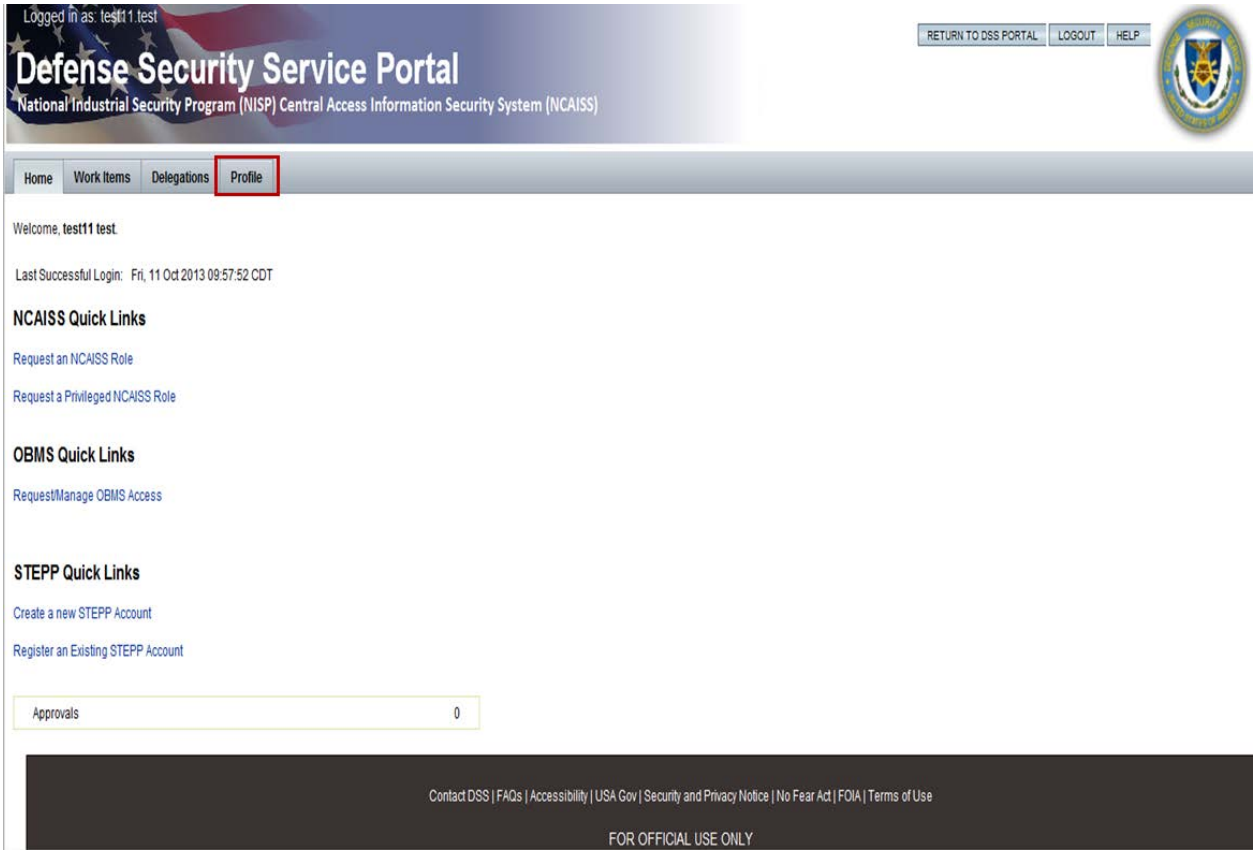


Figure 34: NCAISS Home Page My Profile Data Tab

The "Profile" tab includes two tabs, as shown in Figure 35.

- Account Attributes
- Authentication Questions

Each of these tabs is covered in greater detail in the sub-sections that follow.

1. Click the "Return to DSS Portal" button (at the top right side of the page) or the "Home" tab to leave the "Profile" page and return to the DSS NCAISS Home Page.
2. Click "Logout" (at the top right side of the page) to log out of the DSS NCAISS.

Note: Refer to Section 11, "Logging Out," of this document, for more information on the different ways to log out of the DSS NCAISS.

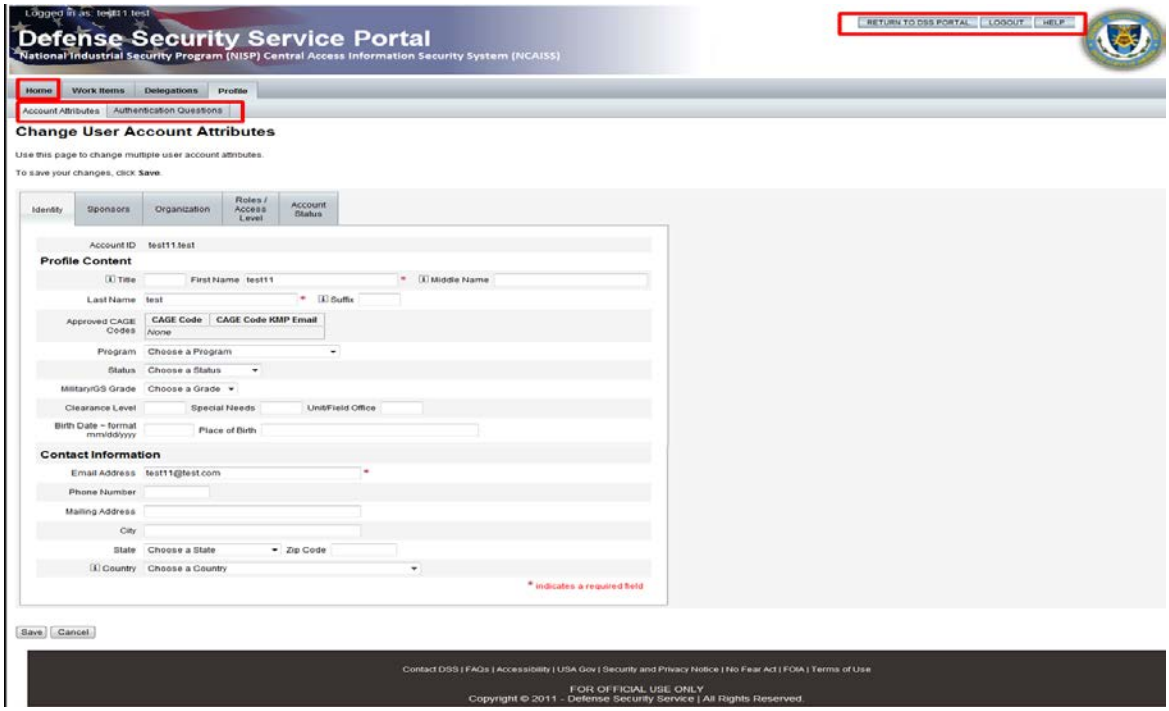


Figure 35: My Profile

7.1 Account Attributes

Within the "Account Attributes" tab, user data is organized in five (5) sub-tabs as follows:

- Identity
- Sponsor
- Organization
- Roles/Access Level
- Account Status

To update profile data, enter the necessary changes in the appropriate fields on the specified tab, as described below:

1. Click the appropriate "Account Attributes" sub-tab to view/update data; click "Save" to store any changes or "Cancel" to discard any changes.

Note: Users cannot change their email address. If you need to change your email address, contact the DSS Call Center.

Note: Required fields are marked with a "*" to the right of the field.

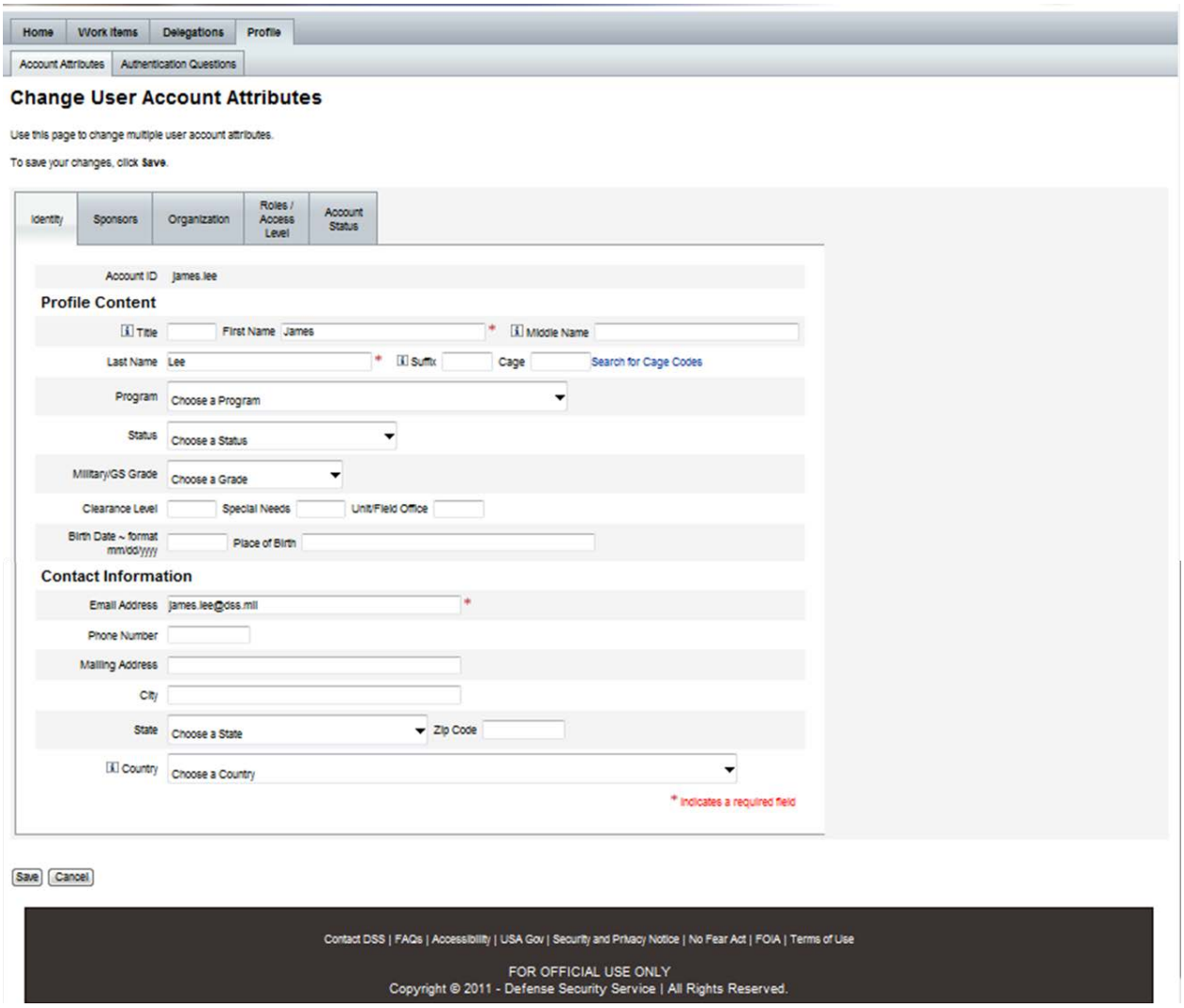


Figure 36: My Profile - Identity Tab

Note: Users cannot change their Sponsor name and email address on the Sponsor tab, however; Sponsors may be changed when requesting a new DSS NCAISS role or access to an integrated application.

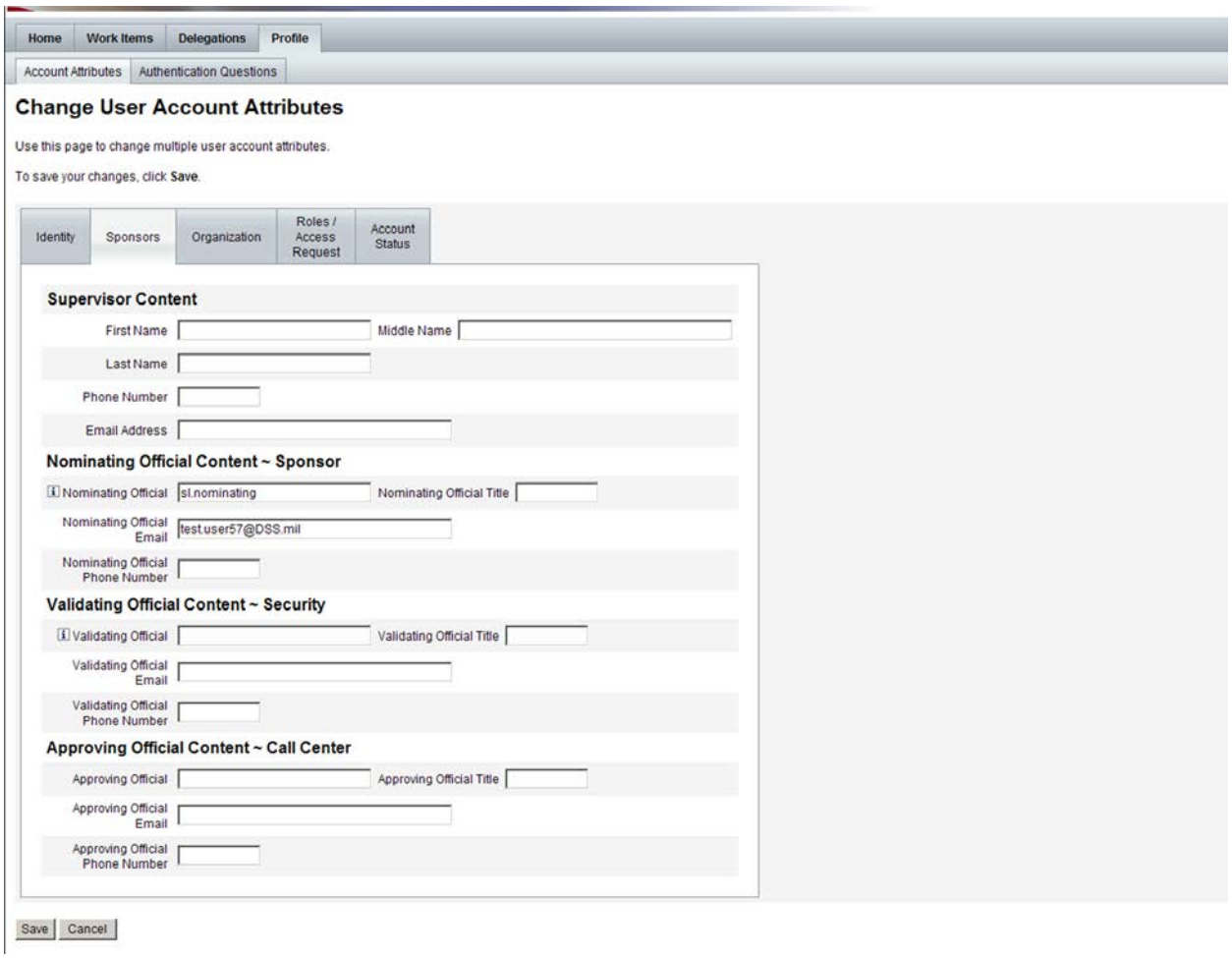


Figure 37: My Profile - Sponsor Tab

As depicted in Figure 38 the Organization Name field is free-form and allows the user to enter the appropriate information. Company contact information is for commercial and private organizations.

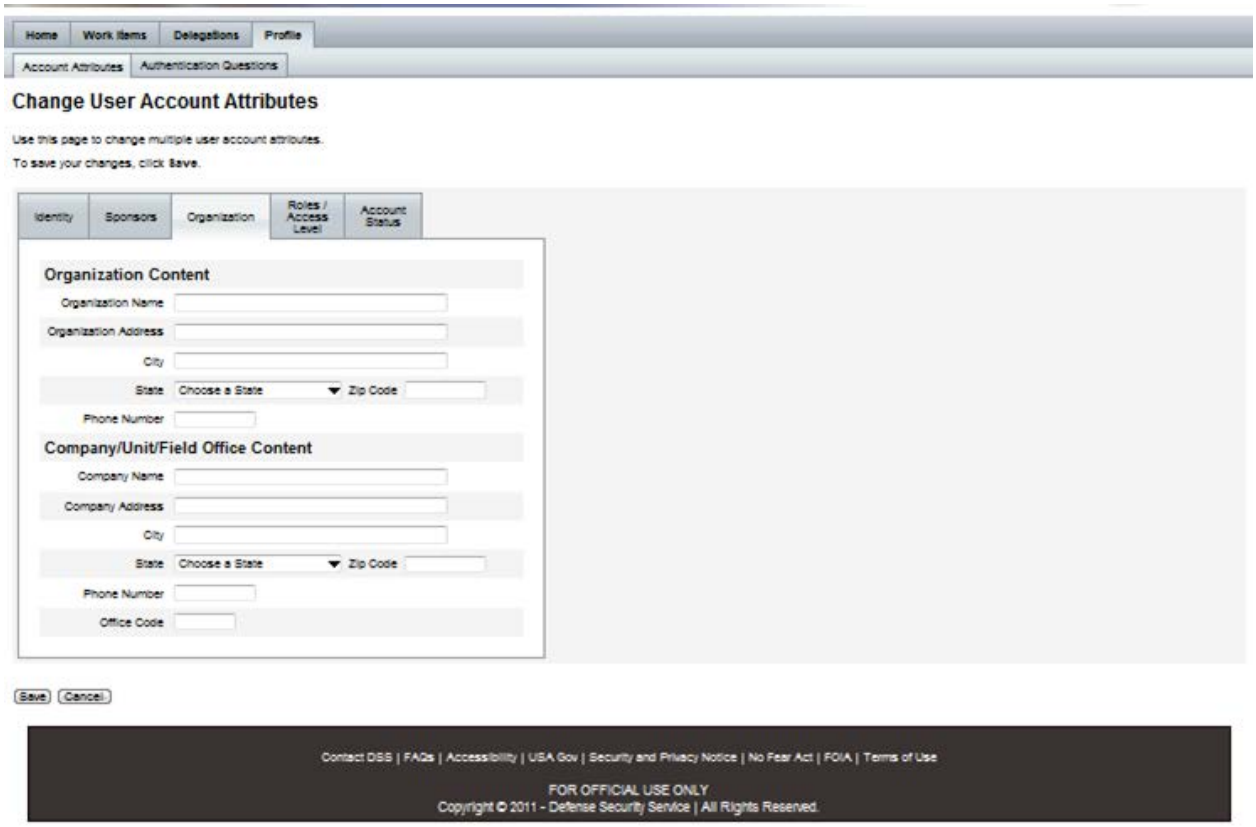


Figure 38: My Profile - Organization Tab

The Roles/Access Request tab shows users what role they currently have. As depicted in Figure 39, users can view their current access level for NCAISS Roles and Privileged NCAISS Roles. They can request additional access by clicking on the "Home" tab then on the appropriate quick link(s).

Note: Reference subsequent sections of this document for step-by-step instructions for requesting roles and access.

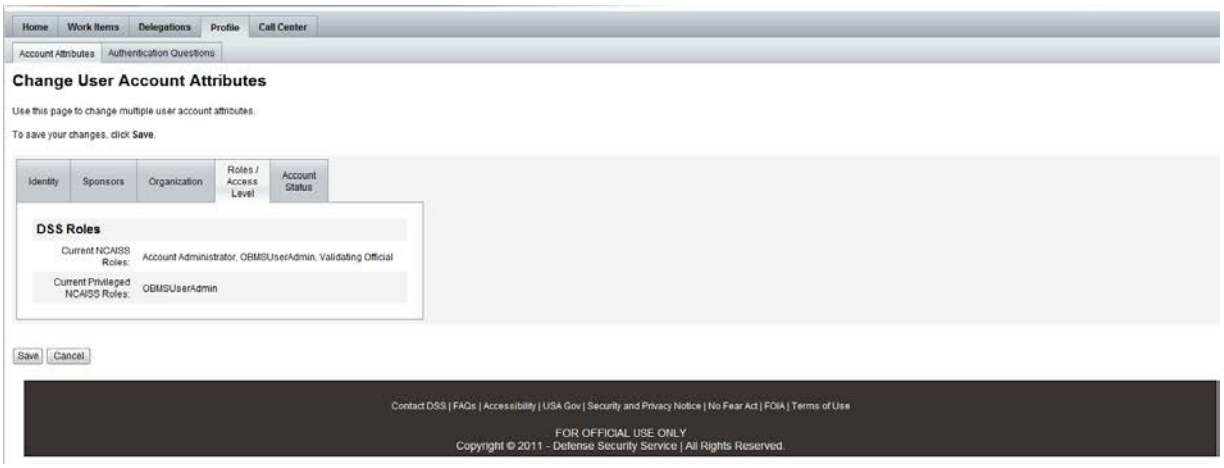


Figure 39: My Profile - Roles/Access Level Tab

The "Account Status" tab provides the user's relevant account status information, as shown in Figure 40.

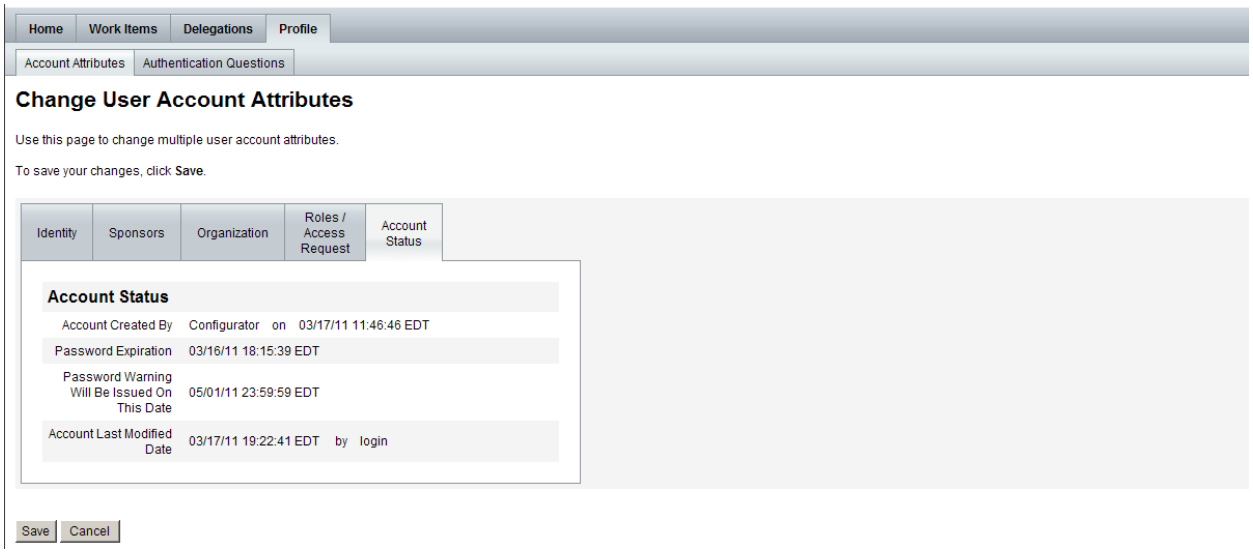


Figure 40: My Profile - Account Status Tab

2. When clicking "Save," the "Operation Successful" message is displayed, as shown in Figure 41.

Figure 41: My Profile - Save Changes Successful

3. Select "Ok" to return to the NCAISS Home Page.
4. Click "Logout" (at the top right side of the page) to log out of the DSS NCAISS.

Note: Refer to Section 11 for more information on the different ways to log out of the DSS NCAISS.

7.2 Authentication Questions

Use the following steps to update the answers to the authentication security questions that were set during the self-enrollment process. The Call Center uses these answers to identify the user, when needed.

1. Click on "Authentication Questions" sub-tab on the Profile tab, as shown in Figure 42. **Note:** Users must answer at least three (3) authentication questions.
2. Update the answers, as necessary.

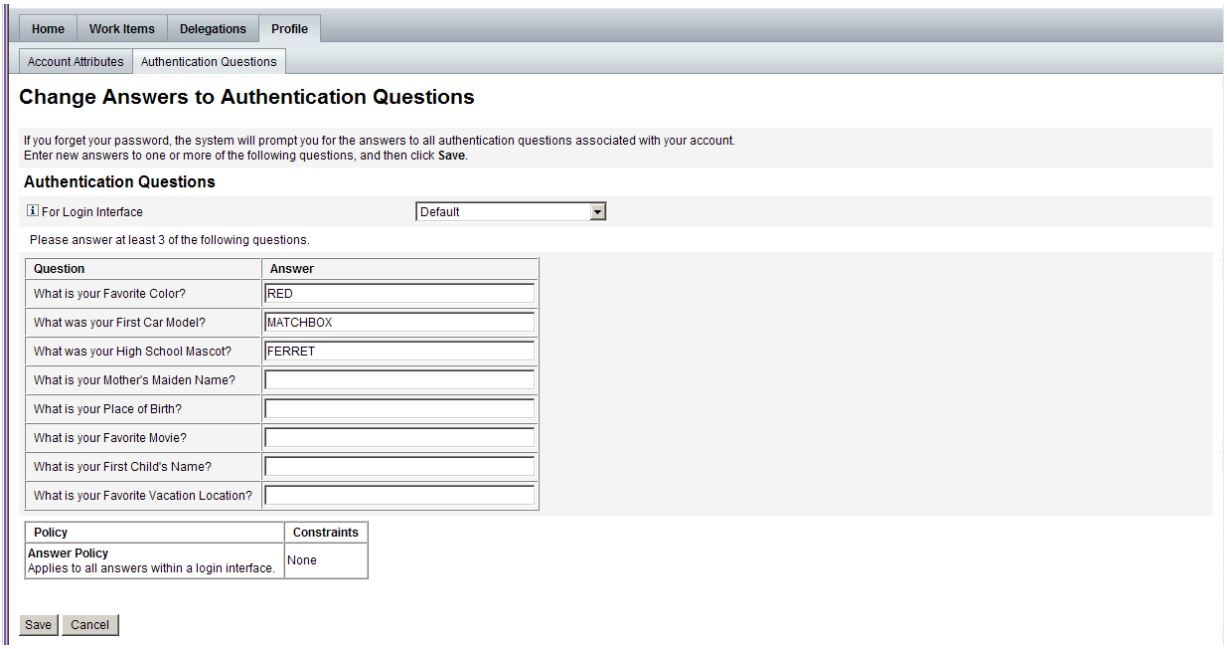


Figure 42: My Profile - Authentication Questions

3. When clicking “Save,” the “Operation Successful” message will be displayed, as shown in Figure 41.
4. Click “OK” to return to the NCAISS Home Page.
5. Click “Logout” (at the top right side of the page) to log out of the DSS NCAISS.

Note: Refer to Section 11 for more information on the different ways to log out of the DSS NCAISS.

8 Request Roles and Access

DSS NCAISS users may request additional roles and access to applications/resources that have been integrated with the DSS NCAISS Solution from the various "Quick Links" sections of the NCAISS Home Page, as shown in Figure 43. Additional NCAISS roles may be requested by selecting the appropriate link under the "NCAISS Quick Links." Sections 8.1 and 8.2 provide step-by-step instructions for requesting NCAISS roles. **Note:** Available quick links are dynamic and displayed to users based on their particular permissions for the system.

Each application that is integrated with the NCAISS Solution (e.g., OBMS) will have a group of related "Quick Links," as depicted in Figure 43. To request access to an integrated application, users begin by clicking on the "Request/Manage <Application> Access" link from within the desired application's "Quick Links." Application-specific user instructions are provided in later sections of this document. **Note:** Additional "Quick Links" will appear on the NCAISS Home Page as new applications/resources are integrated with the NCAISS Solution.

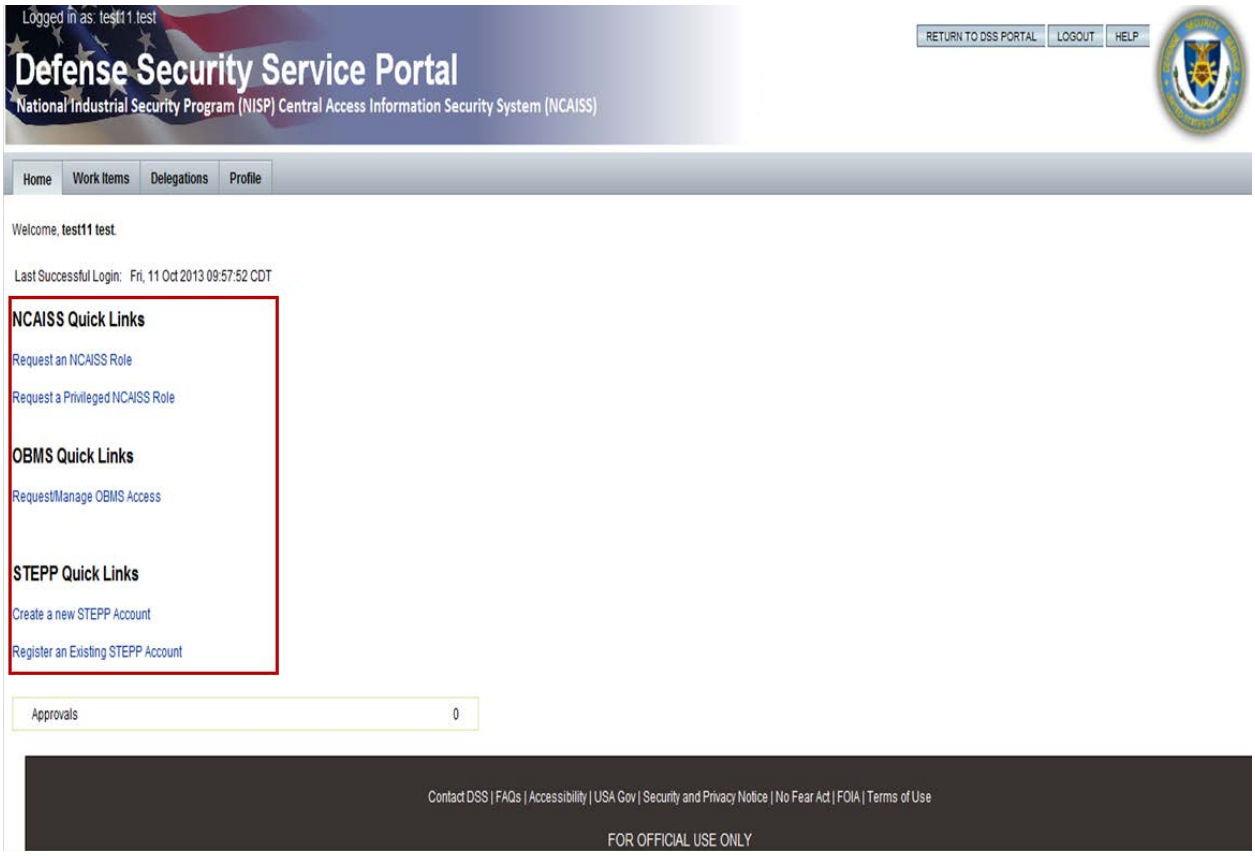


Figure 43: Requesting Roles/Access from the NCAISS Home Page

8.1 Request an NCAISS Role

A user may request an additional DSS Portal Role from the NCAISS Home Page by taking the following steps:

Note: NCAISS roles are only available to DSS users.

1. Click "Request an NCAISS Role" link under the "NCAISS Quick Links."

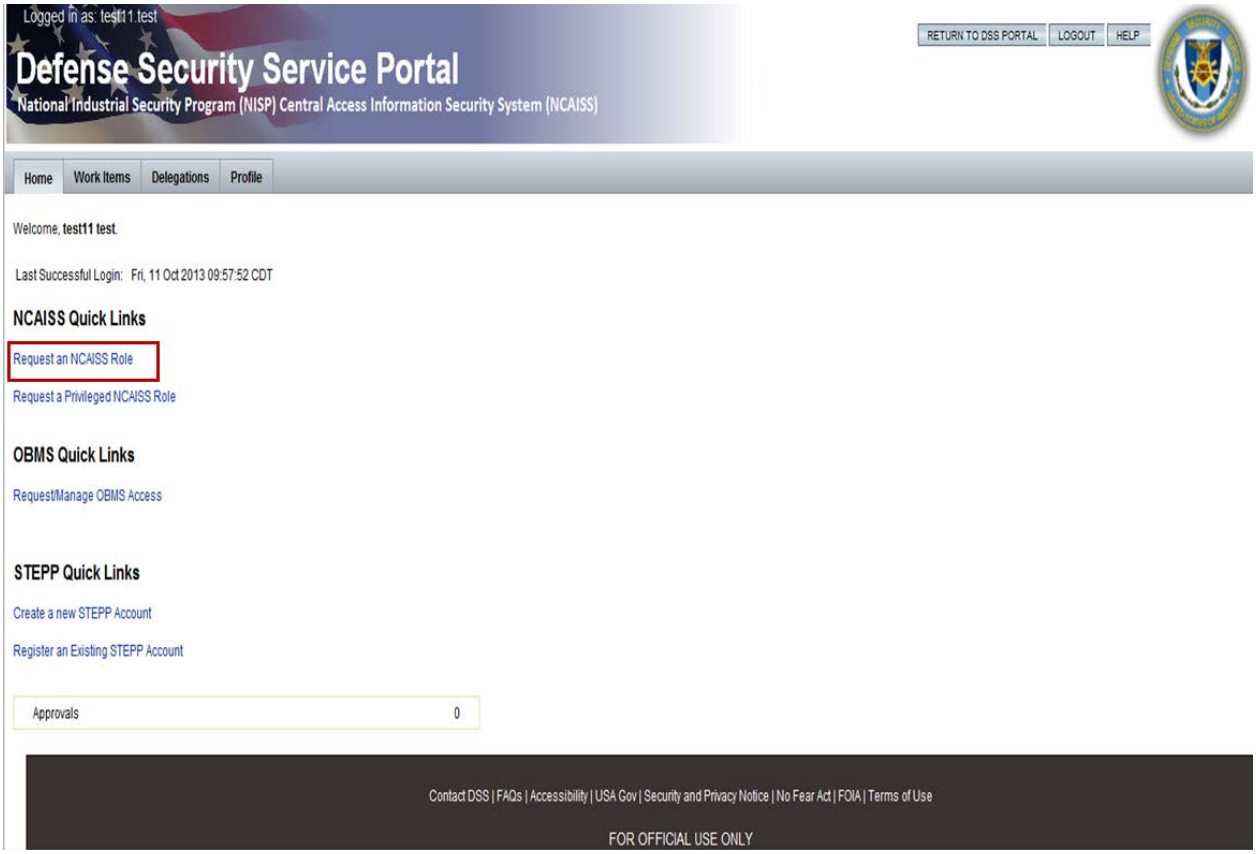


Figure 44: Request an NCAISS Role

2. The Request NCAISS Role form is displayed, as shown in Figure 45. **Note:** Your current NCAISS roles (if any) are displayed in the "Current Roles" field.
3. Select the appropriate role by checking the Account Administrator or Validating Official radio button, depending on the needed access.
4. Complete the NCAISS Role request form by providing your Sponsor's email address and entering your Social Security Number (SSN). **Note:** When requesting an NCAISS Role, your Sponsor must have a dss.mil email address.

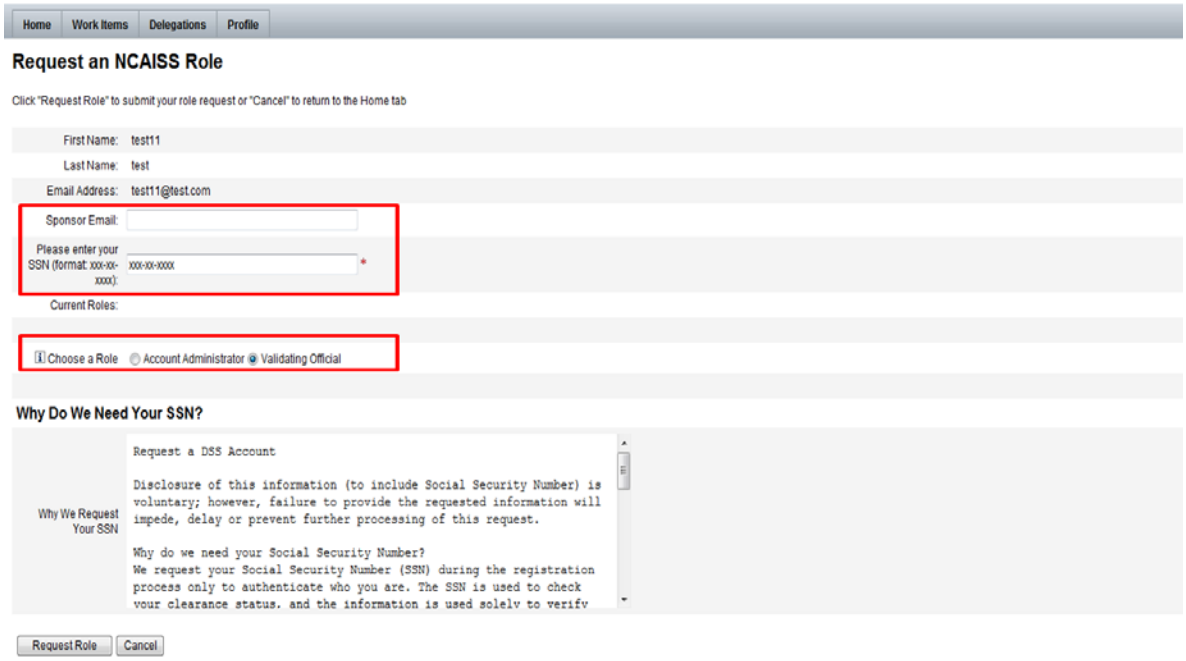


Figure 45: NCAISS Role Request Form

5. Click "Cancel" to cancel the request. **Note:** Any data entered will be cleared once you hit "Cancel."
6. Click "Request Role" to submit your request.

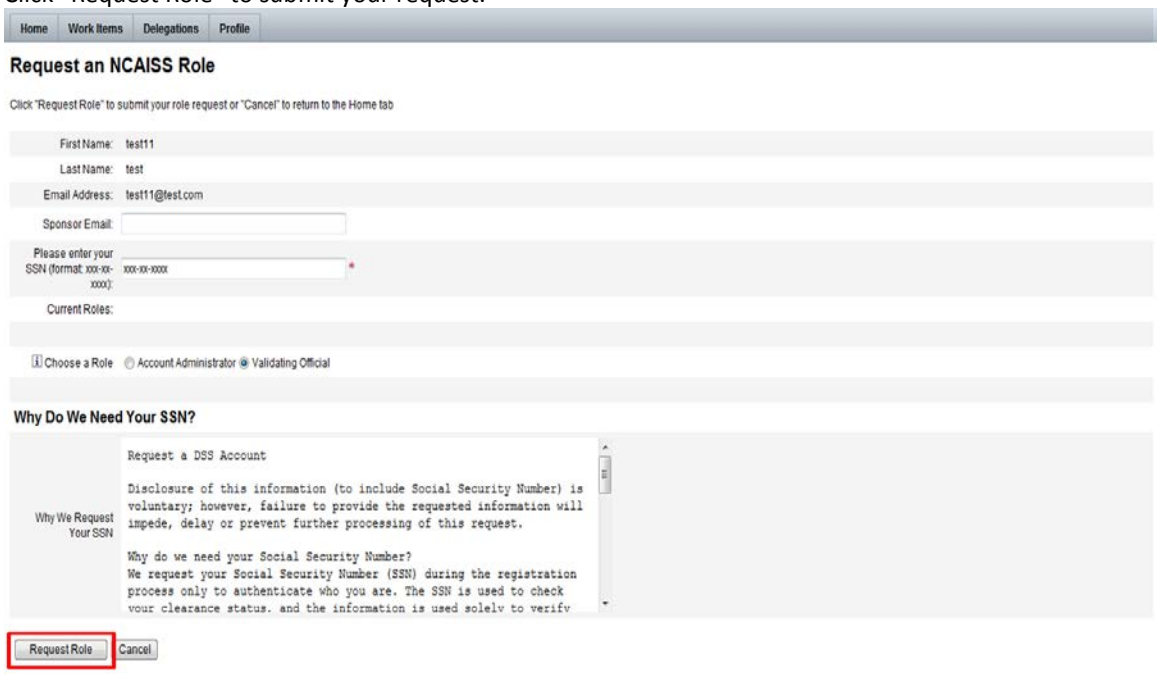


Figure 46: NCAISS Role Request Form Submission

7. A confirmation page will be displayed, as shown in Figure 47. Review the accuracy of the information presented, and click the check box to indicate that you have read and agree to the terms of the privacy policy.
8. Click "Cancel" to cancel the request. **Note:** Any data entered will be cleared once you hit "Cancel."
9. Click "Submit" to submit your role request for review.

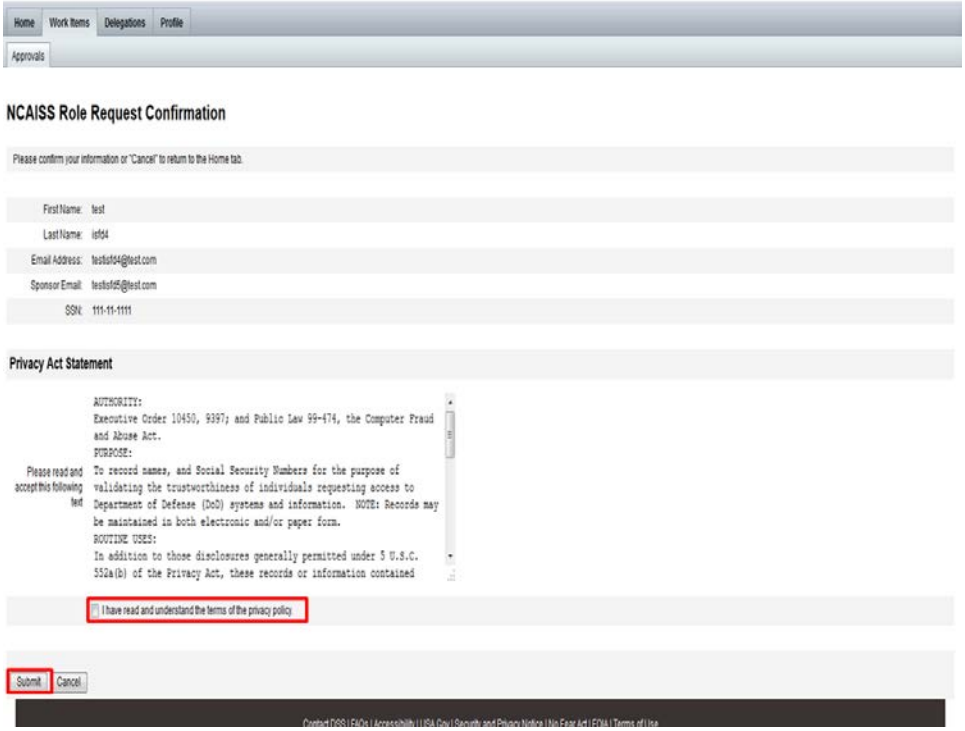


Figure 47: NCAISS Role Request Confirmation

10. Upon form submission, you are returned to the NCAISS Home Page.
11. Click “Logout” (at the top right side of the page) to log out of the DSS NCAISS.

Note: Your submitted request will be sent to your Sponsor’s inbox for approval and they will be notified via email.

8.2 Request a Privileged NCAISS Role

A user may request a Privileged NCAISS Role from the NCAISS Home Page by completing the steps below.

Note: Privileged NCAISS roles are only available to DSS users.

1. Click “Request a Privileged NCAISS Role” link.

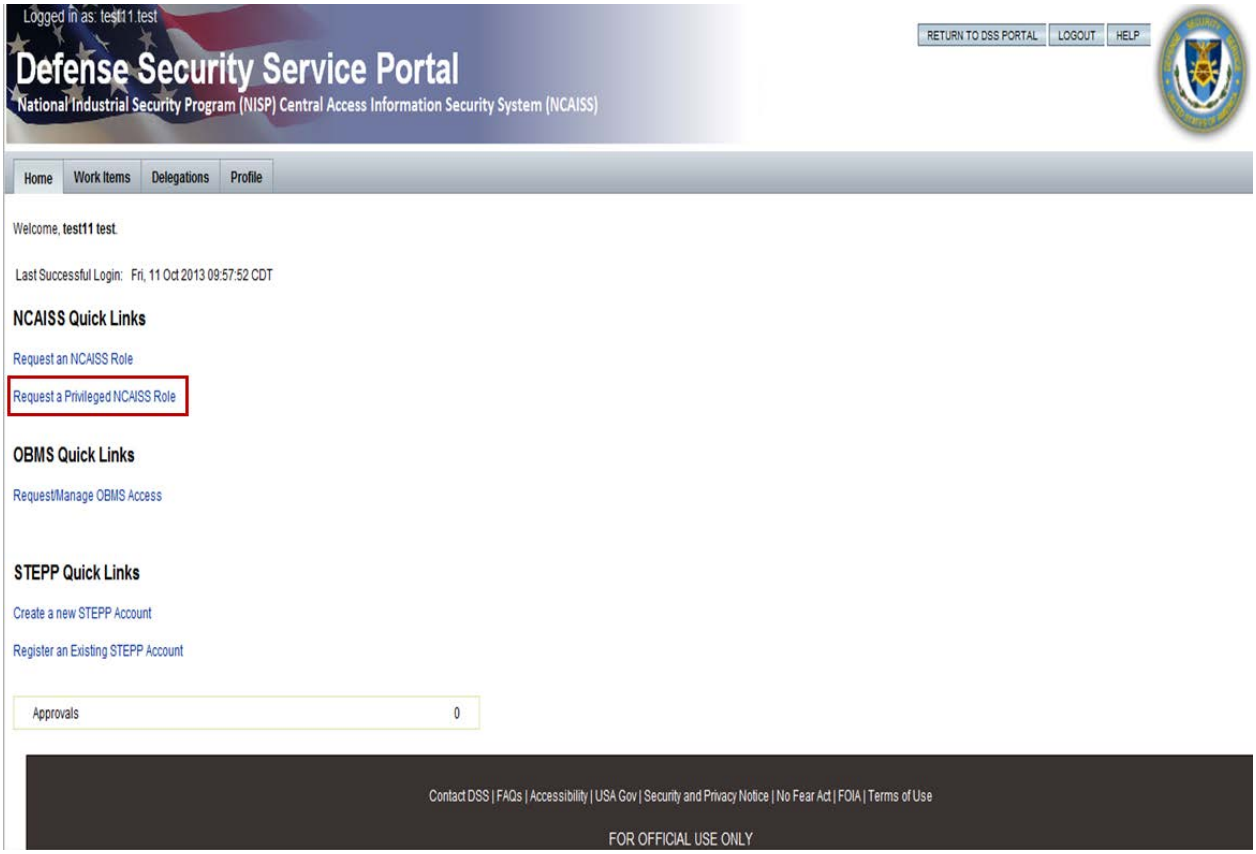


Figure 48: Request Privileged NCAISS Role

2. Complete the Privileged NCAISS Role Request Form by specifying your Sponsor's email address and entering your SSN. **Note:** When requesting a Privileged NCAISS Role, your Sponsor must have a dss.mil email address.

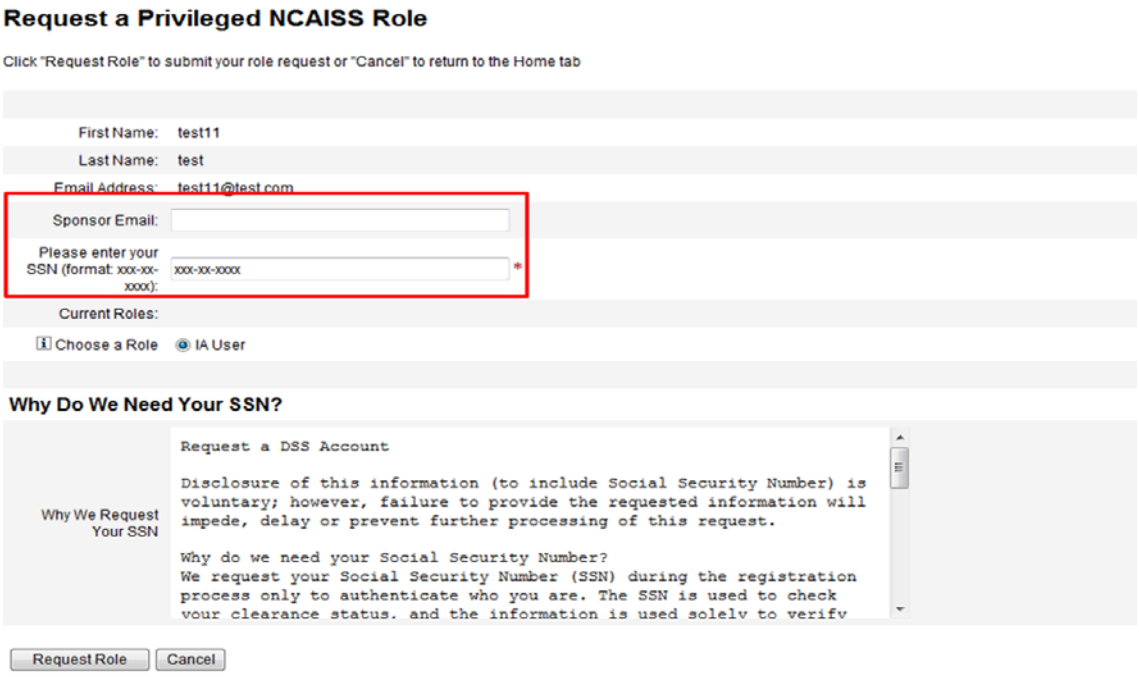


Figure 49: Privileged NCAISS Role Request Form

3. Click “Cancel” to cancel the request. **Note:** Any data entered will be cleared once you hit “Cancel.”
4. Click “Request Role” to submit your request.

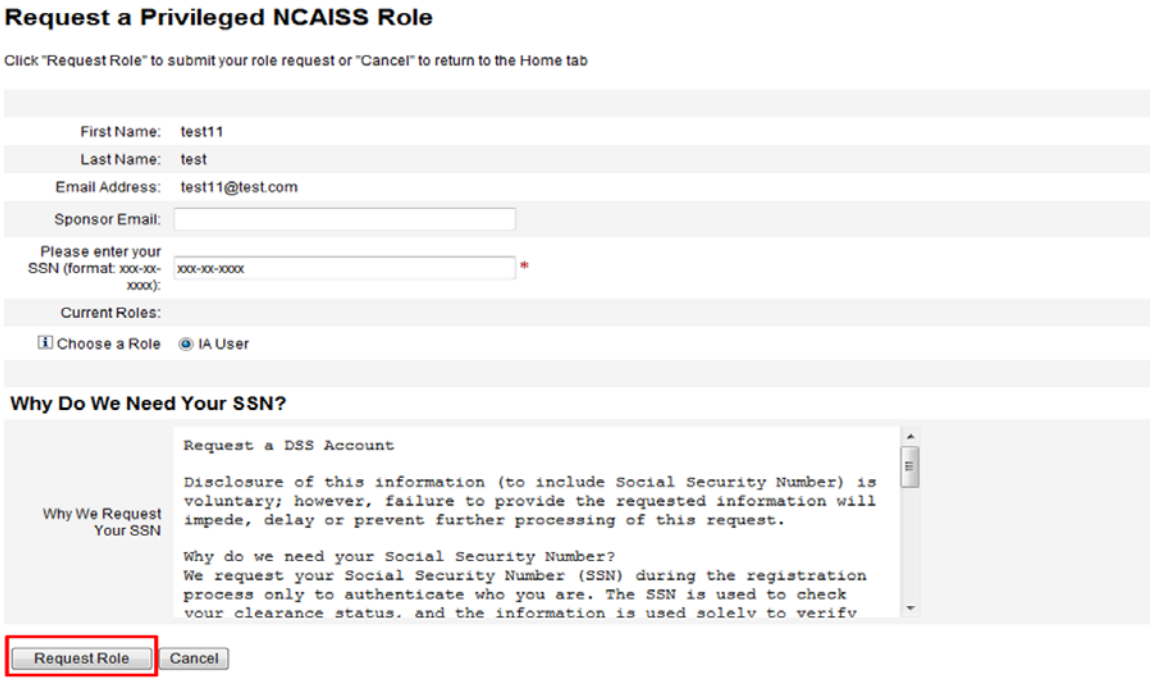


Figure 50: Privileged NCAISS Role Request Form Submission

5. A confirmation page will be displayed, as shown in Figure 51. Review the accuracy of the information presented and click the check box to indicate that you have read and agree to the terms of the privacy policy.
6. Click “Cancel” to cancel the request. **Note:** Any data entered will be cleared once you hit “Cancel.”
7. Click “Submit” to submit your request.

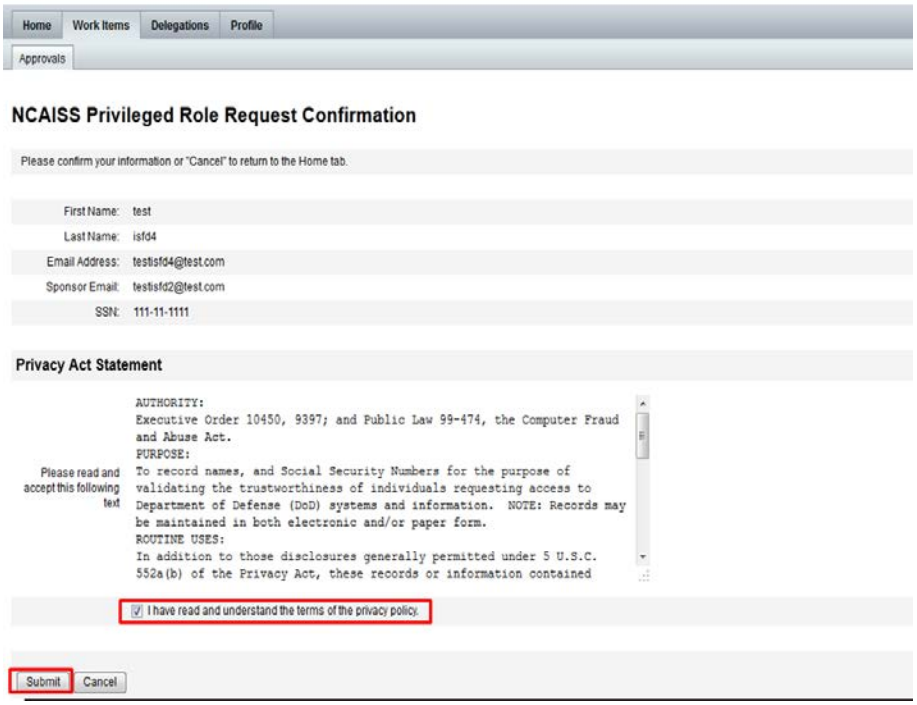


Figure 51: Privileged NCAISS Role Request Confirmation

8. Upon form submission, you are returned to the NCAISS Home Page.

9. Click “Logout” (at the top right side of the page) to log out of the DSS NCAISS.

Note: Your submitted request will be sent to your Sponsor’s inbox for approval and they will be notified via email.

9 Approving/Rejecting Account Requests

When DSS NCAISS users submit requests for additional roles and/or access to integrated applications, these requests are posted in the Sponsors'/Approvers' inboxes. As depicted in Figure 52, new requests that require review and approval can be viewed by clicking either the "Approvals" bar at the bottom of the NCAISS Home Page or the "Work Items" tab at the top of the page.

Note: the number of approval steps and the approvers involved are determined based on the type of role or application access that is requested; however, the basic approval process remains unchanged from the process documented below.

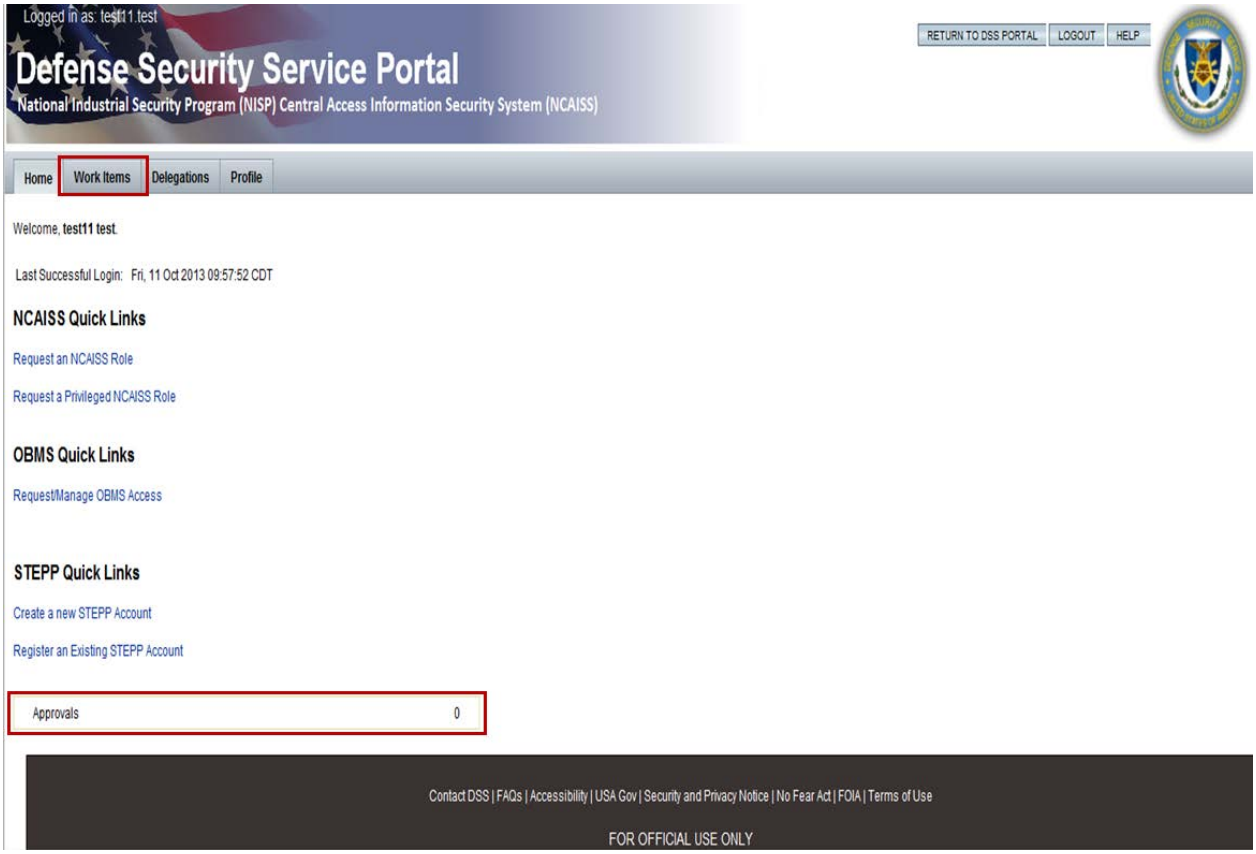


Figure 52: NCAISS Home Page – Accessing Approval Items

Clicking either the "Approvals" bar or the "Work Items" tab allows a user to see a list of requests awaiting their review and approval, as depicted in Figure 53.

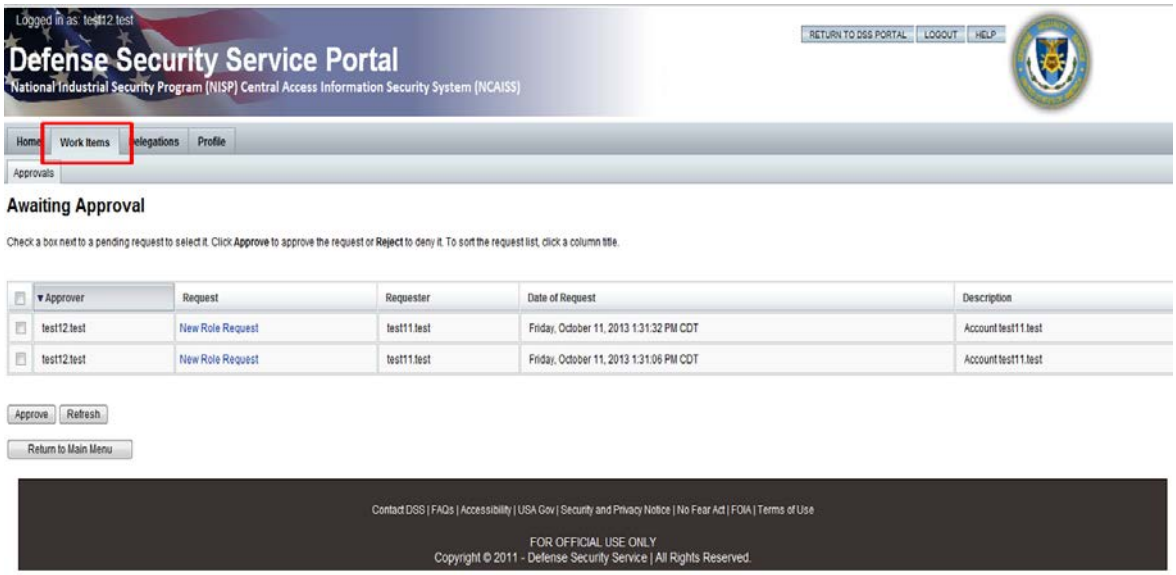


Figure 53: Work Items Tab

9.1 Approving NCAISS Role Requests

Once a user's DSS NCAISS account is established, he/she may request additional roles on the DSS NCAISS, to include Account Administrator and Validating Official. The submitted requests are posted in the appropriate Sponsor's Work Items list. If the a User requests the role of Validating Official, then a "Validating Official" must review the request once it has been approved by the user's Sponsor. Once the Validating Official verifies the security level for the requester, they may approve or reject the request. If the requestor has selected an "Account Administrator" account type, the workflow includes an Account Administrator review of the request, following approval by both the Sponsor and Validating Official. **Note:** Request rejections are addressed in Section 9.3.

1. Log into the DSS NCAISS.
2. The DSS NCAISS Home Page is displayed, as shown in Figure 30.
3. Click on the "Approvals" bar or "Work Items" tab.
4. The "Work Items" tab is displayed with a list of requests awaiting approval, as shown in Figure 54.

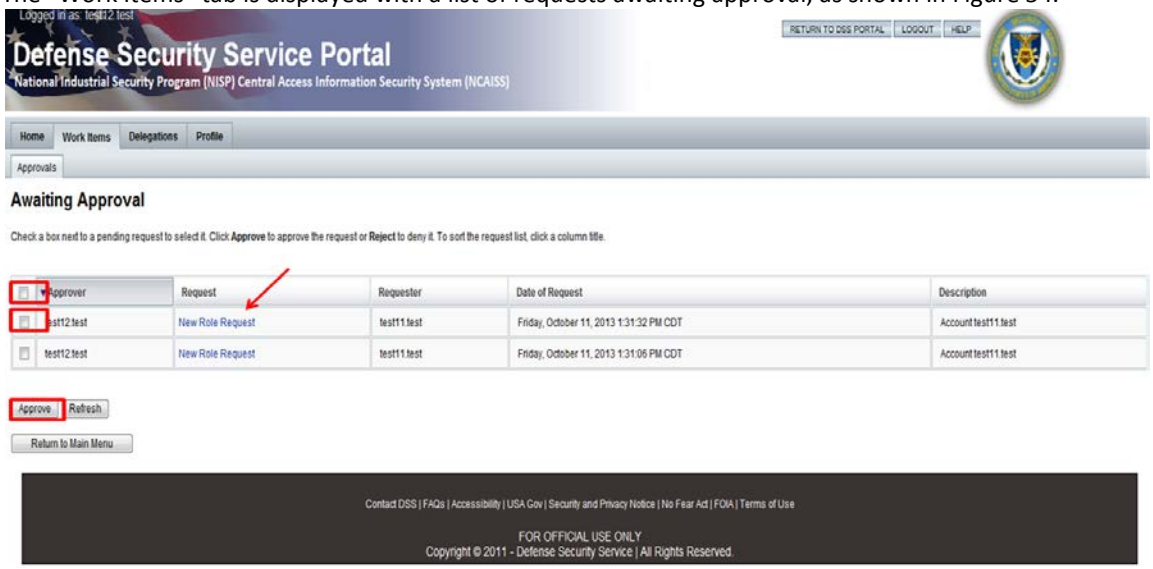


Figure 54: NCAISS Role Requests Awaiting Approval

5. There are two ways to approve a request:

a. You can check the checkbox next to the request and click "Approve." **Note:** To approve multiple requests, check the top checkbox to select all requests in the list and click "Approve."
b. Click on "New Account Request" link in the Request box.

6. The Account Request Approval detail view is displayed, as shown in Figure 55. Here you can view the account details and the account type the user is requesting.
7. Review the request, enter a comment (optional), and click "Approve." **Note:** After the Sponsor approves the request, the request is forwarded to other NCAISS role holders for subsequent approvals (i.e., Validating Official for Validating Official access requests and Validating Official and Account Administrator for Account Administrator access requests).

Figure 55: NCAISS Role Request Review

8. After approving, the system redirects you to the "Home" tab to display the remaining number of approvals on the list.

9.2 Approving a Privileged NCAISS Role Request

Established NCAISS users may request privileged roles on the DSS NCAISS such as, an IA User. The submitted requests are posted in the Sponsor's Work Items list. If the Sponsor approves a request, the approval workflow moves the request to the "Validating Official" (Security representative) Work Items list. Once the Validating Official verifies the security level for the requester, they may approve or reject the request appropriately. **Note:** Request rejections are addressed in Section 9.3.

Note: Currently the only Privileged NCAISS Role is "IA User."

1. Log into the DSS NCAISS.
2. The DSS NCAISS Home Page is displayed, as shown in Figure 30.
3. Click on either the "Approvals" bar or "Work Items" tab.
4. The "Work Items" tab is displayed with a list of requests awaiting approval, as shown in Figure 56.

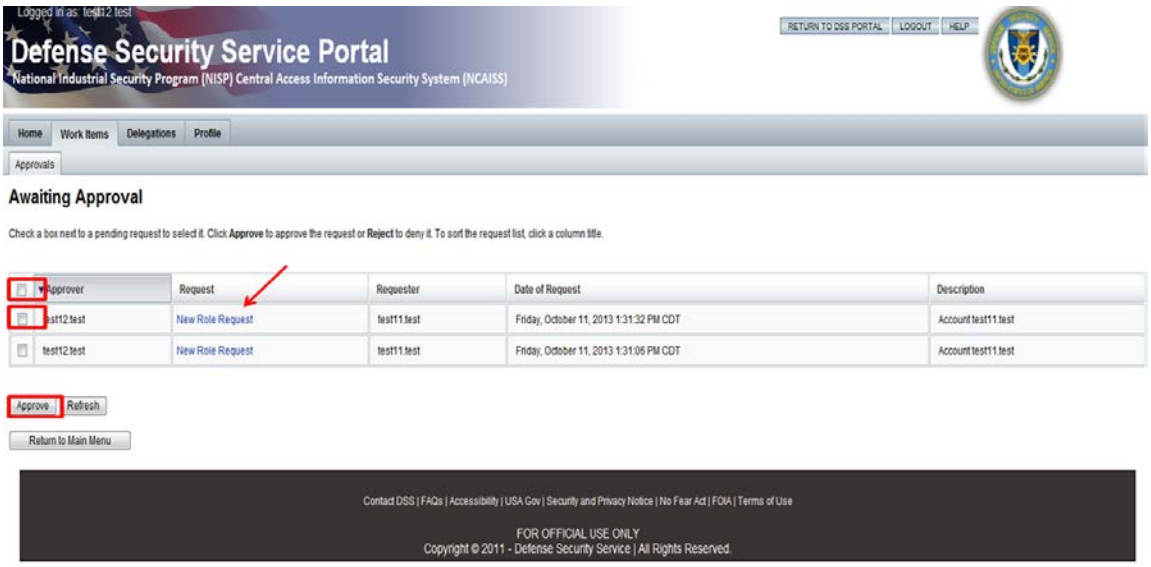


Figure 56: Privileged NCAISS Role Requests Awaiting Approval

5. There are two ways to approve a request:
    a. You can check the checkbox next to the request and click "Approve." **Note:** To approve multiple requests, check the top checkbox to select all requests in the list and click "Approve."
    b. Click on "New Account Request" link in the Request box.
6. The Account Request Approval detail view is displayed, as shown in Figure 57. Here you can view the account details and the account type the user is requesting.
7. Review the request, enter a comment (optional), and click "Approve." Note: After the Sponsor approves the request, the request is forwarded to the Validating Official for a subsequent approval.

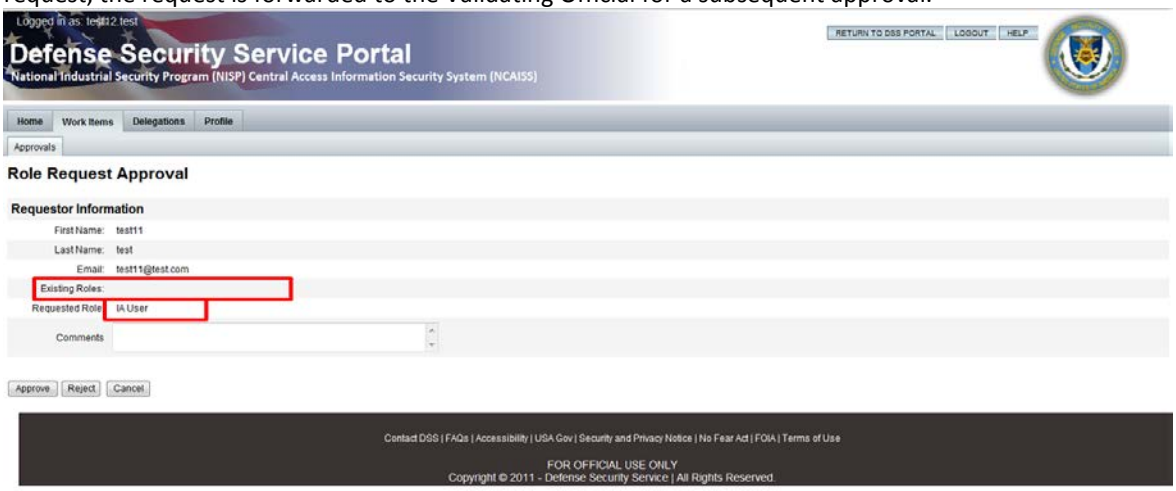


Figure 57: Privileged NCAISS Role Request Detail View

8. After approving, the system redirects you to the "Home" tab to display the remaining number of approvals on the list.

9.3 Rejecting a Request

Any NCAISS User that receives an access request Work Item has capability to review the request and either approve or reject it. All NCAISS users follow the same process to reject a request. **Note:** Any Work Item that is rejected requires the user to enter a custom comment to indicate the justification for rejection.

1. Click on a link in the "Request" column, as shown in Figure 58.

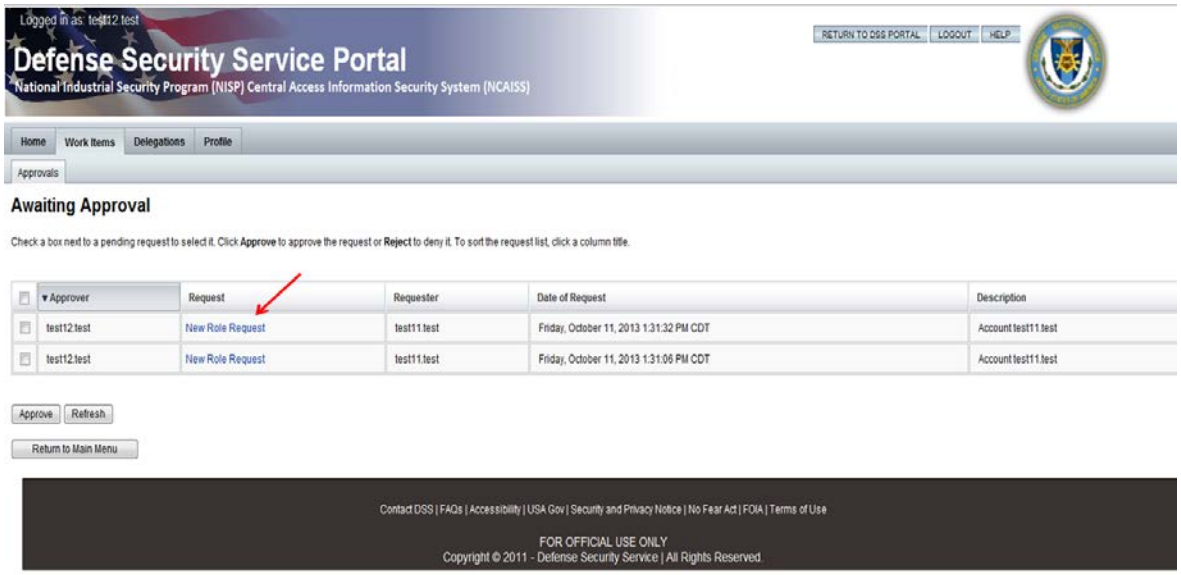


Figure 58: Work Item Request Section

2. The Account Request detail view is displayed, as shown in Figure 59. Here you can view the account details and the account type the user is requesting.
3. Review the request, enter a reason for rejection in the comments box, and click "Reject." **Note:** Comments are required in order to reject a request using this process; if no comments are entered, then an error message will be displayed.

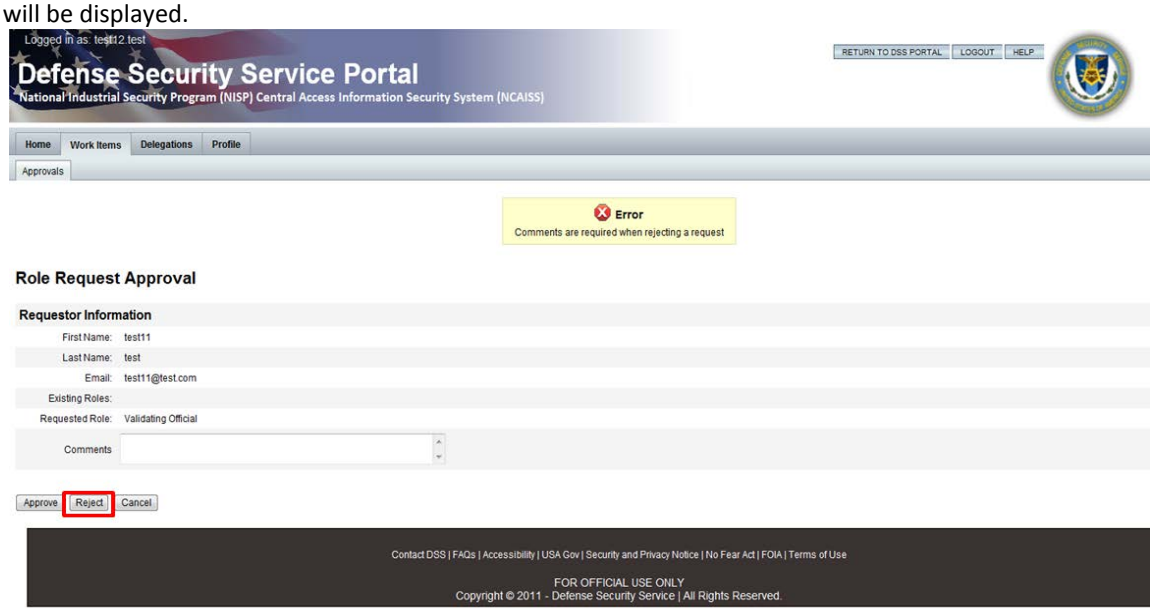


Figure 59: Access Request Detailed Rejection

4. The request is rejected and an email is sent to the user with the reason it was rejected.

10 Delegating Work Items

Any NCAISS user that receives Work Items (e.g., access approval requests) may delegate his/her Work Items to another user for a specified period of time. Work Item delegation can help ensure that access requests are processed quickly and efficiently during prolonged absences. When delegating Work Items, it is the responsibility of the Delegator to ensure that the Delegate is fully capable of completing the assigned work tasks. The process for delegating Work Items is the same for all NCAISS users and follows the process outlined below. **Note:** Only one delegation may be active at any given time, including delegations set for a future time period; creating a second delegation will supersede any previously created delegation.

1. From the NCAISS Home Page, click the "Delegations" tab, as shown in Figure 60.

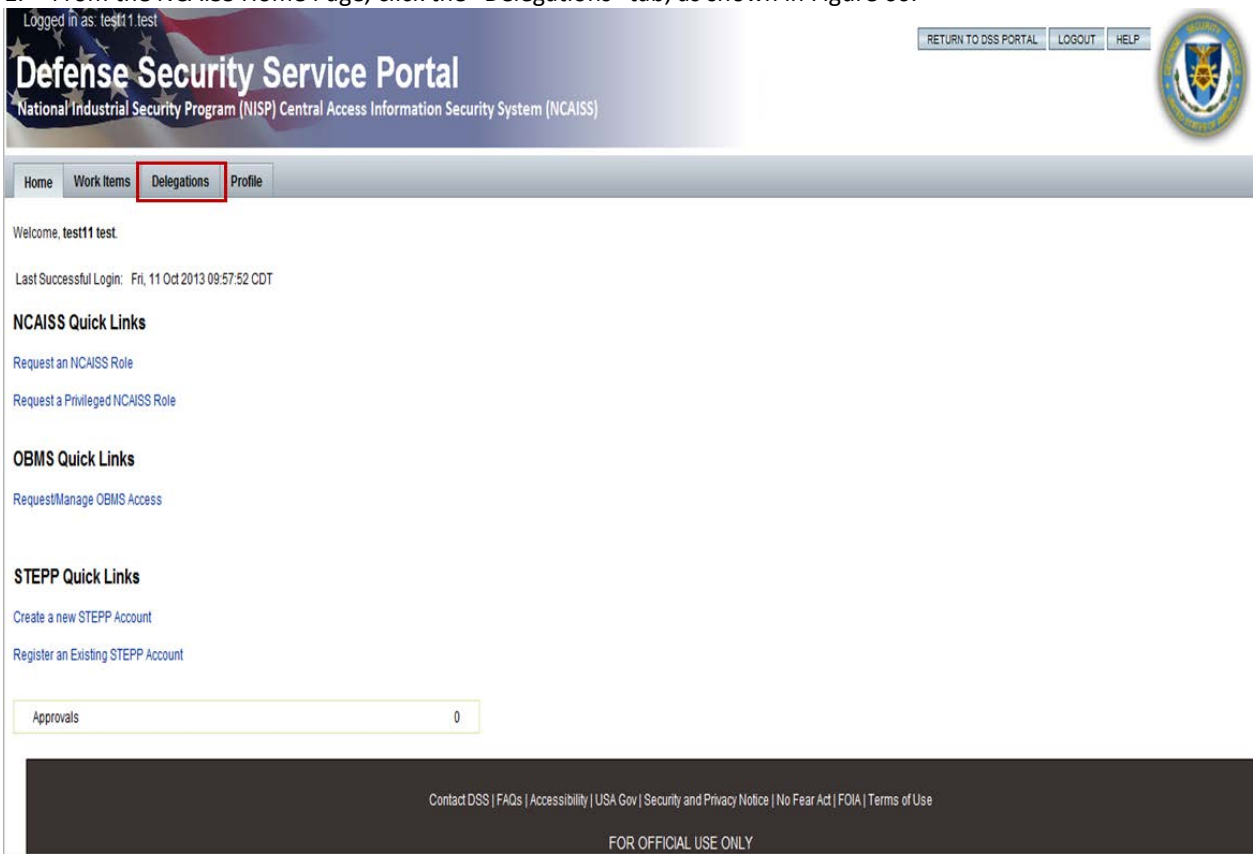


Figure 60: Delegating Work Items from the NCAISS Home Page

2. The Delegations tab displays any active or ended delegations and allows the user to begin a new Delegation.
3. Click "New" to initiate a new Delegation.

Figure 61: Begin New Delegation

4. Enter a Start Date and End Date for the period in which you would like to delegate your Work Items.
5. Locate the desired user by selecting and entering search criteria.

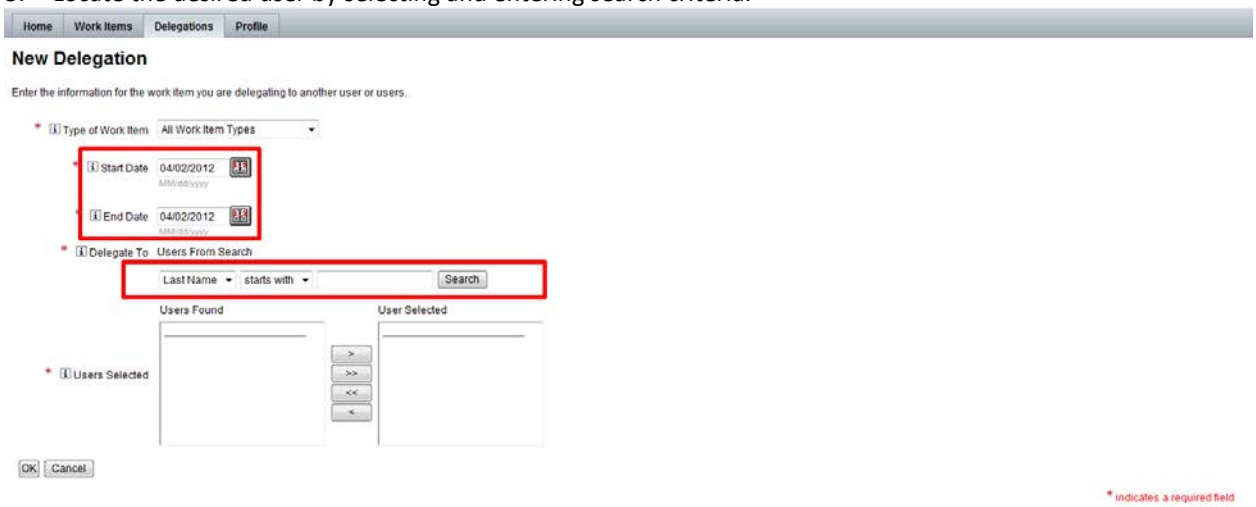


Figure 62: Set Delegation Parameters

6. Once you've found the appropriate user, select his/her name in the Users Found box and click the right single arrow button. This will move the user's name into the User Selected box.
7. Click "OK."

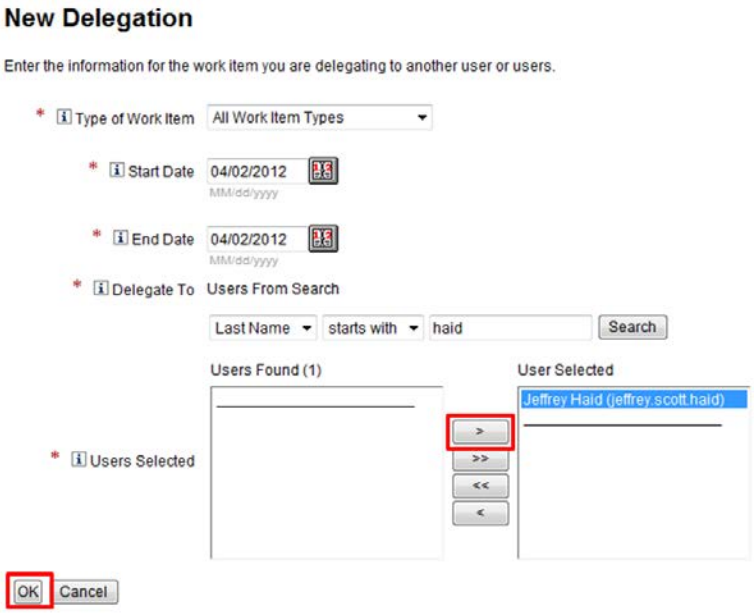


Figure 63: Select User for Delegation

8. The delegation task will be created and you will be returned to the Delegations tab. Here you will see the new delegation task in the delegation summary box.

Figure 64: Completed Delegation Summary

11 Logging Out

Users may log out of the DSS NCAISS using the “Logout” button or by closing their web browser. The process and screen shots below demonstrate logging out of NCAISS using the “Logout” button.

1. From any screen within NCAISS, click on the “Logout” button in the top right corner, as shown in Figure 65.
2. Once logged out, NCAISS Login Page is displayed. **Note:** You must close your web browser to fully terminate the session.

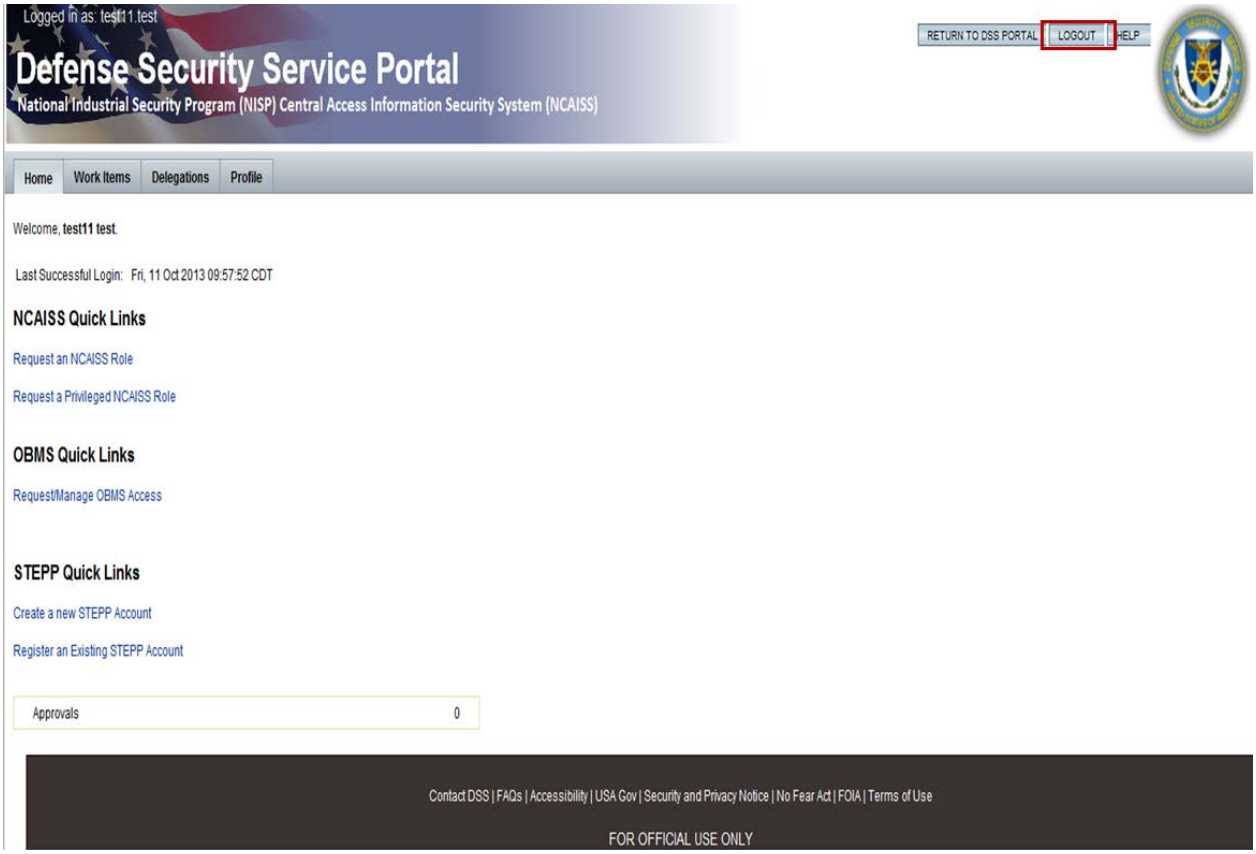


Figure 65: NCAISS Home Page Log Out

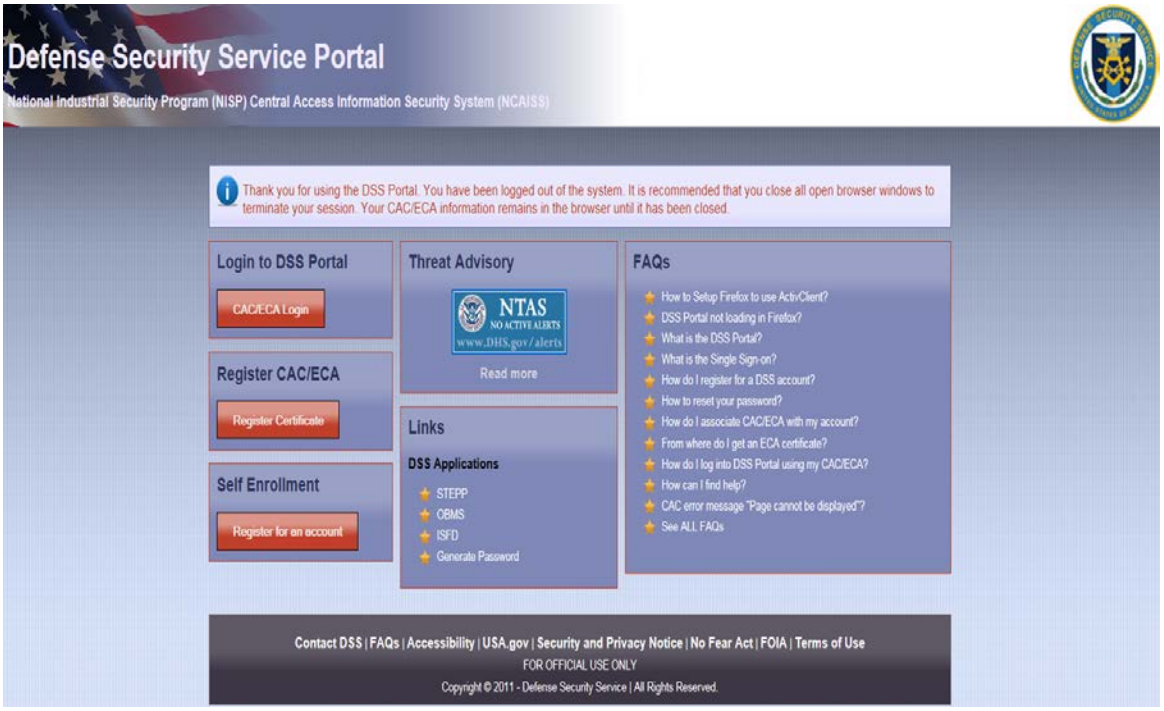


Figure 66: Successful Logout

12 OBMS Application NCAISS User Guide

This section describes the step-by-step processes for requesting access to, accessing, and managing users for the OBMS application using the NCAISS Solution. **Note:** this portion of the User Guide focuses exclusively on use of the NCAISS Solution as it relates to the OBMS application. Actions that a user may take within the OBMS application, following successful authentication, are out of scope for this User Guide. This section assumes that an OBMS access requestor already has a valid NCAISS user account. If a valid NCAISS user account does not exist, refer to Section 3 for step-by-step instructions for NCAISS self-enrollment.

12.1 Accessing OBMS

CAC/PKI authentication is the process through which all OBMS users, regardless of role, will access the OBMS application using the CAC or a DoD-approved ECA certificate. For convenience, there are two ways in which a user may authenticate to OBMS, including:

- Navigate to the public-facing OBMS home page and click "Login" (CAC/PKI Authentication from OBMS)
- Access OBMS from the NCAISS (CAC/PKI Authentication from NCAISS)

The following sections provide step-by-step instructions for accessing OBMS using the two methods described above. **Note:** This section assumes that the User already possesses valid NCAISS and OBMS application accounts.

12.1.1 CAC/PKI Authentication from OBMS

The steps below describe the process for accessing OBMS via NCAISS from the OBMS homepage through the use of a CAC or DoD-approved ECA certificate.

1. Navigate to the OBMS unauthenticated homepage (www.obms.dss.mil).
2. Check the box to indicate that you consent to the terms of the User agreement and select "Login."

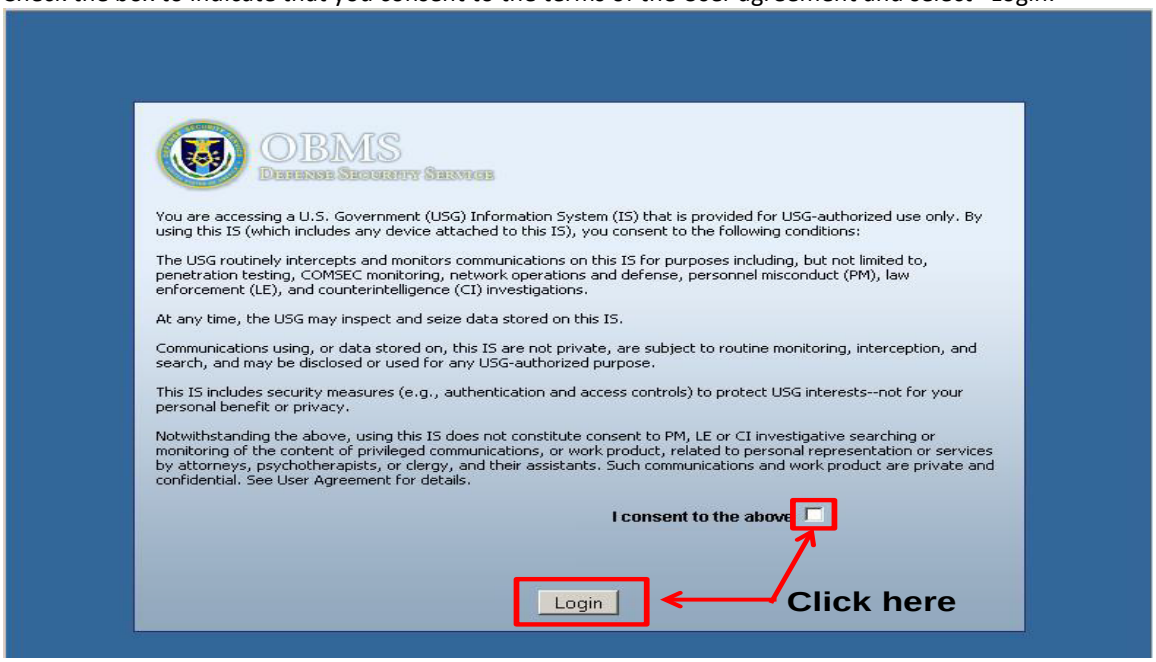


Figure 67: Unauthenticated OBMS Home Page

3. You are redirected to the NCAISS Disclaimer page, as shown in Figure 68. Select "I Accept" to proceed.

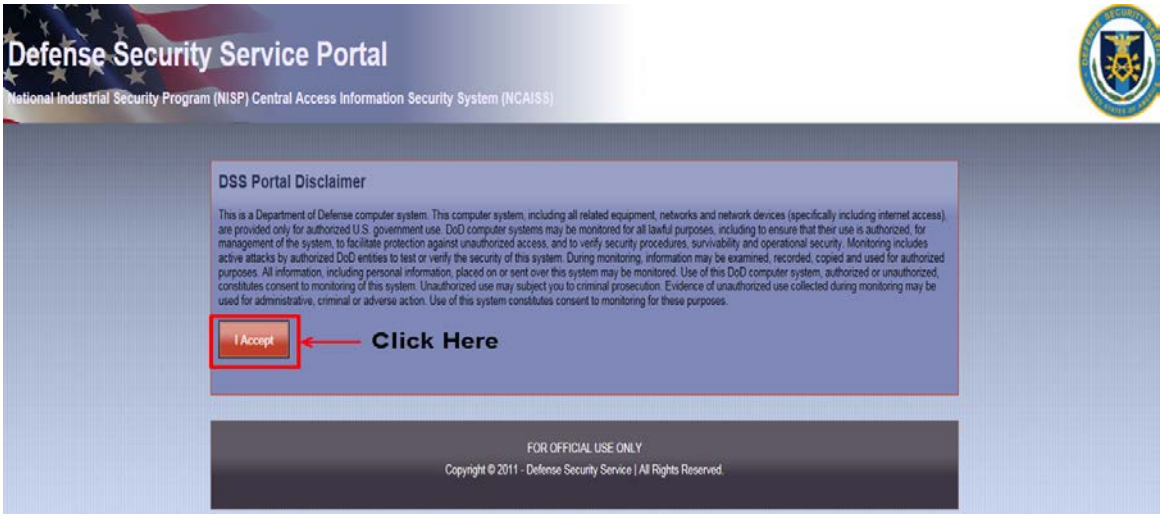


Figure 68: NCAISS Disclaimer

4. The unauthenticated NCAISS page is displayed, as shown in Figure 69. Select "CAC/ECA Login" to proceed.

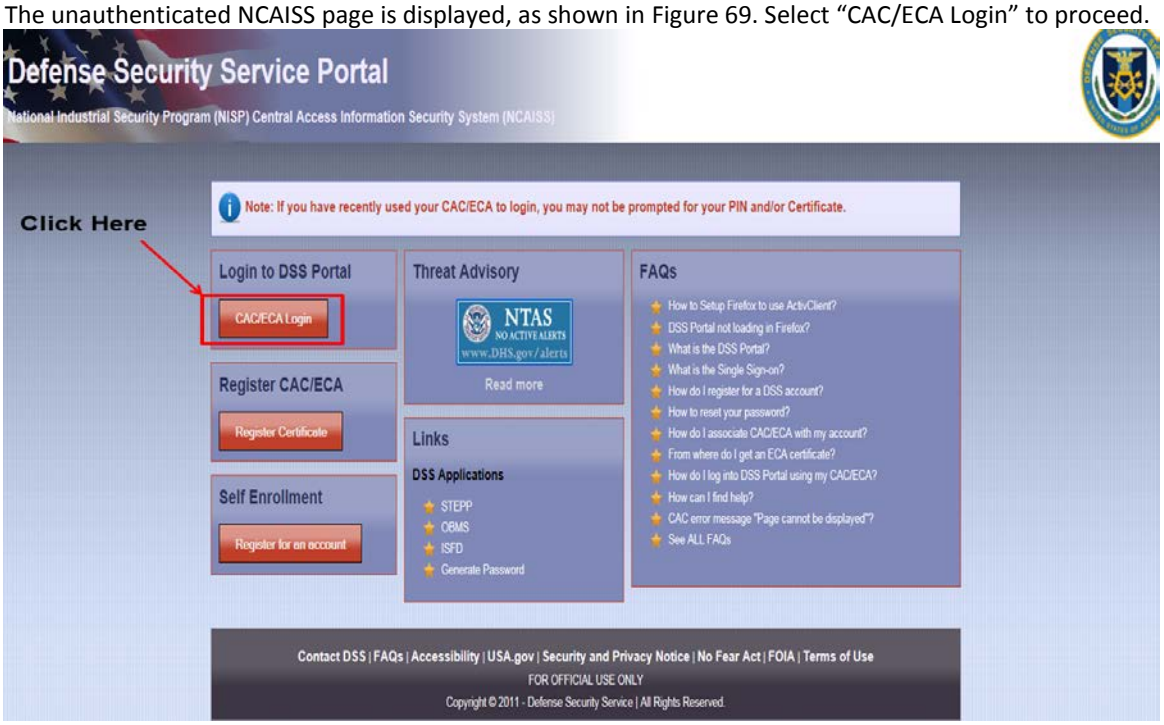


Figure 69: Unauthenticated NCAISS Home Page

5. Select the certificate that you would like to use. **Note:** You must use the certificate that has been associated to your NCAISS account.

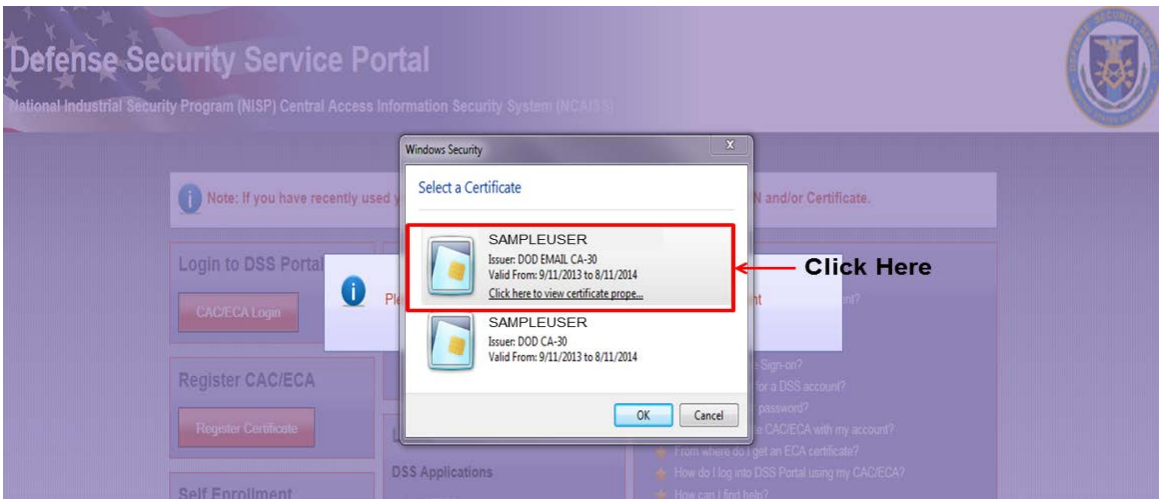


Figure 70: Certificate Selection

6. Enter your PIN.

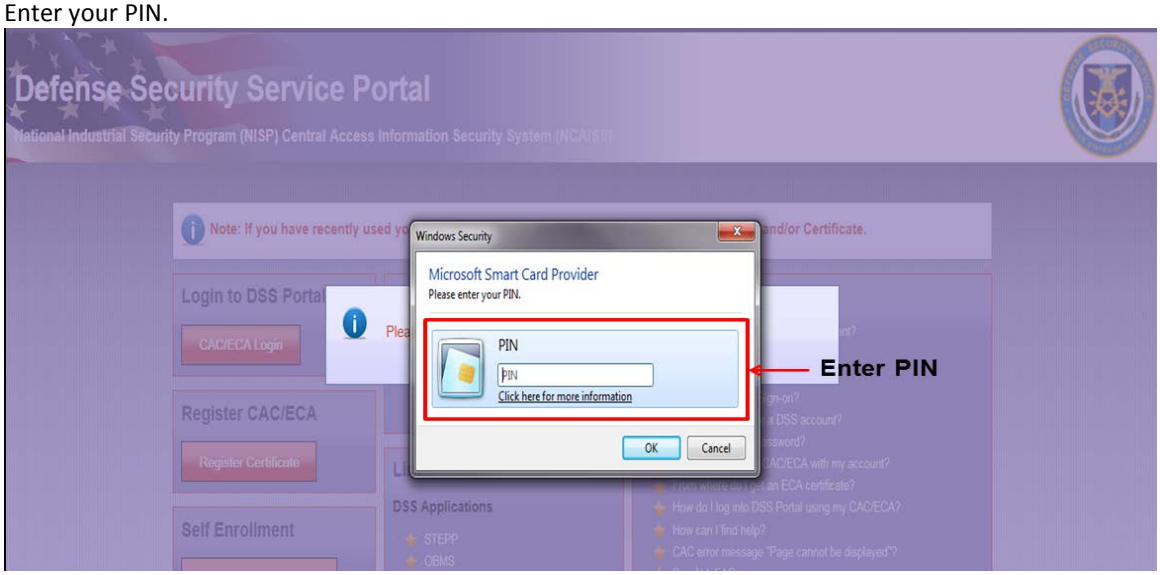


Figure 71: PIN Entry

7. The NCAISS Solution authenticates you and, if successful, directs you to OBMS. The OBMS user's homepage is displayed, as shown in Figure 72.

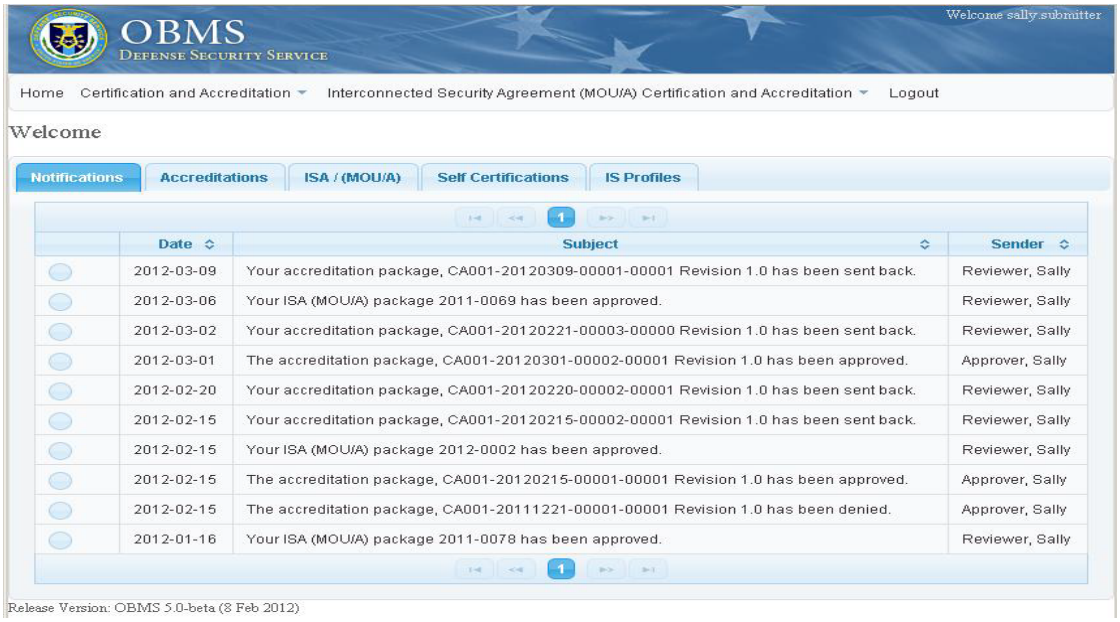


Figure 72: OBMS User Home Page

Note: OBMS users with multiple OBMS roles will be prompted by OBMS to select the role that they would like to use during a given session, as shown in Figure 73. If applicable, select the desired role from the drop down menu and click "Submit."

Figure 73: Multiple OBMS Role Selection

12.1.2 CAC/PKI Authentication (to OBMS) from NCAISS

The steps below describe the process for accessing OBMS via NCAISS from NCAISS through the use of a CAC or DoD-approved ECA certificate.

1. Navigate to the NCAISS (https://sso.dss.mil) in your web browser.
2. Authenticate to NCAISS, as described in Section 5.
3. Upon successful authentication, the NCAISS Home Page is displayed.
4. Click the "Access OBMS" link within the "OBMS Quick Links," as shown in Figure 74.

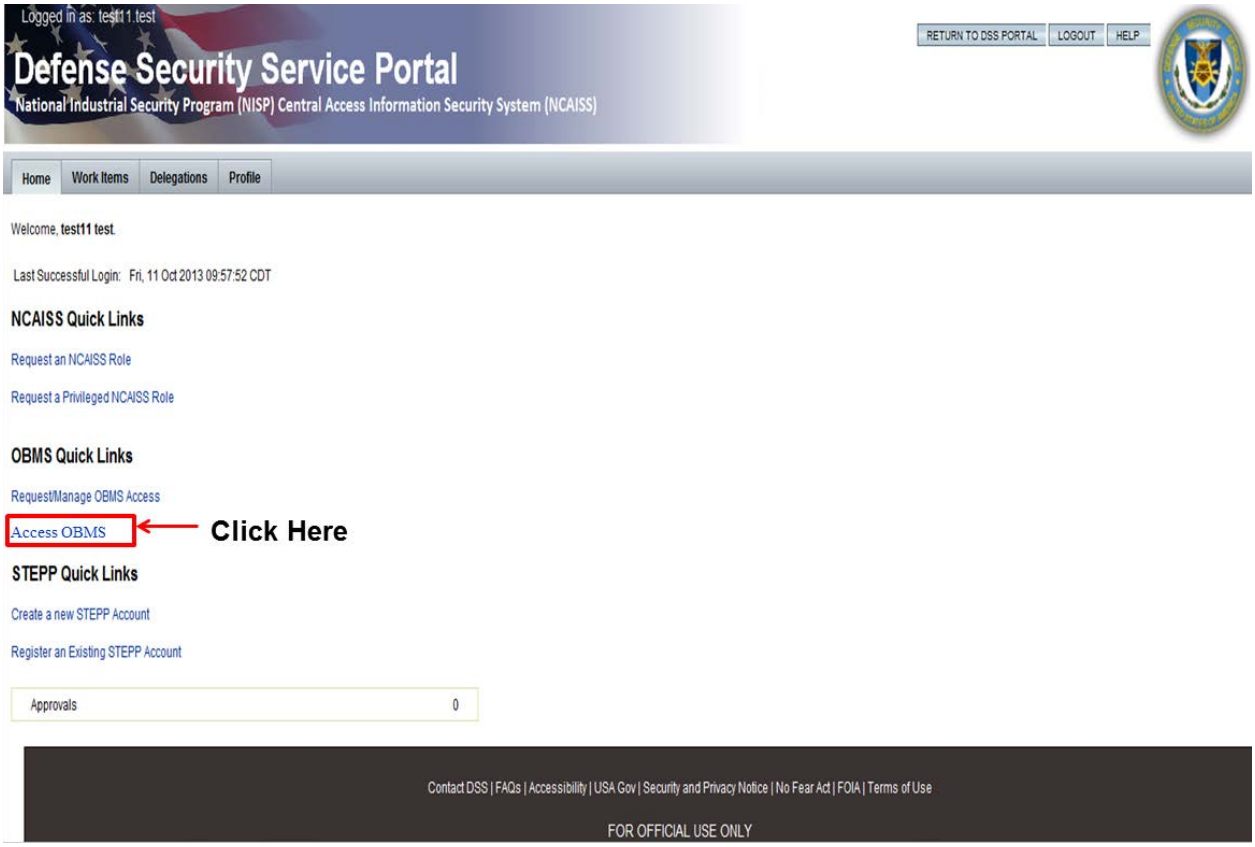


Figure 74: Accessing OBMS from the NCAISS Home Page

5. NCAISS will direct you to OBMS and the OBMS user home page is displayed, as shown in Figure 72.

Note: OBMS users with multiple OBMS roles will be prompted by OBMS to select the role that they would like to use during a given session, as shown in Figure 73. If applicable, select the desired role from the drop down menu and click "Submit."

12.2 Requesting Access to OBMS

In order to gain access to OBMS, an NCAISS user must request access using the OBMS access request form from within the NCAISS. Based upon the user's affiliation with DSS (using their email address on record), NCAISS will display the appropriate OBMS access request form. OBMS Internal Users, either DSS employees or contractors with a dss.mil email address will complete the Internal OBMS access request form, as described in Section 12.2.1. OBMS External Government Users, individuals from the industrial security community, representing a Federal Government organization, that have a .mil or .gov (non-DSS) email address will complete the External Government Submitter OBMS access request form, as described in Section 12.2.2. OBMS External Contractor Submitter Users, industry users with an email address other than .gov or .mil (e.g., .com, .org, etc.); will complete the External OBMS Contractor Submitter access request form, as described in Section 12.2.3. The following sections provide step-by-step instructions for requesting access to OBMS, based upon your affiliation with DSS.

12.2.1 OBMS Internal User (DSS.mil) Account Request

This process allows an Internal OBMS Access Requestor with a dss.mil email address to request access to the OBMS application. **Note:** This process assumes that the Access Requestor has a valid NCAISS account and has already logged into NCAISS, as described in Section 5.

1. Once logged into NCAISS, click the "Request/Manage OBMS Access" link in the "OBMS Quick Links," as shown in Figure 75.

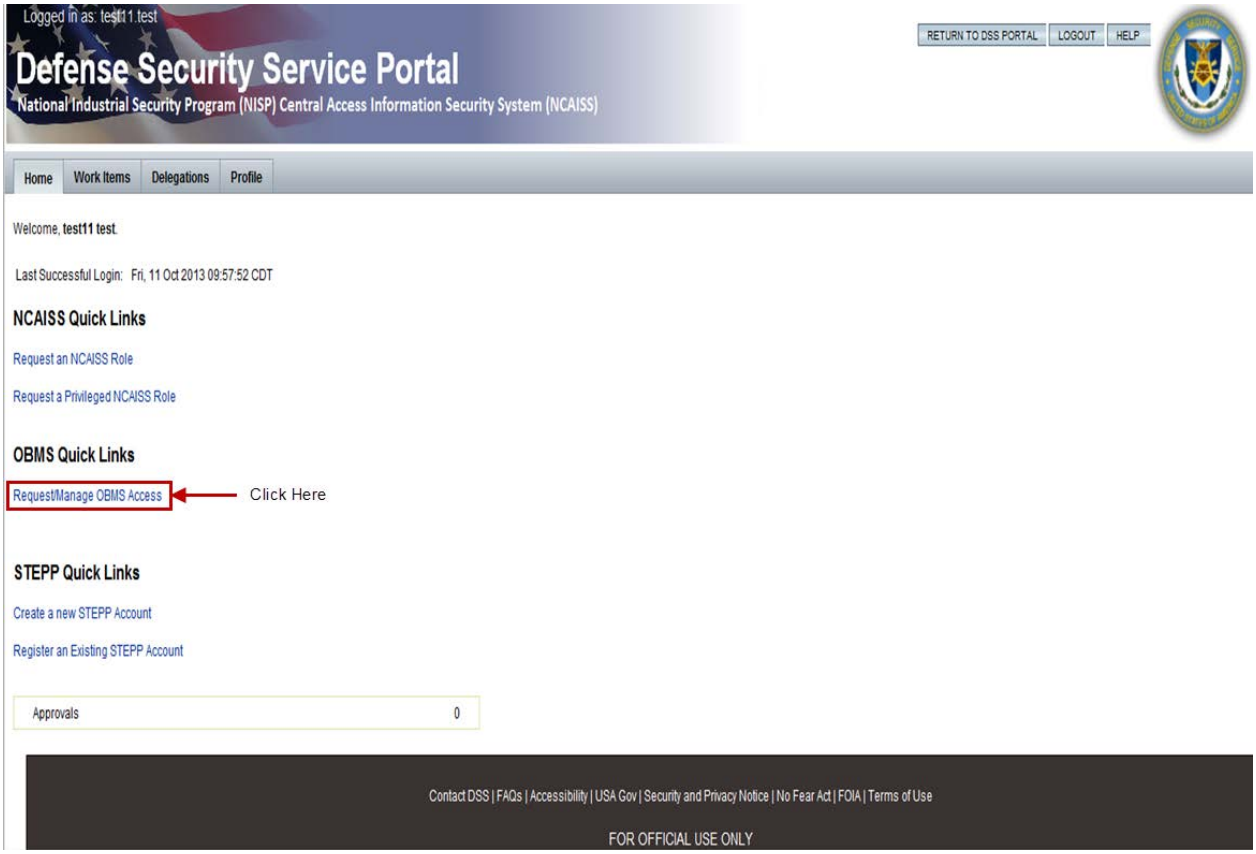


Figure 75: Requesting Access to OBMS from the NCAISS Home Page

2. NCAISS will determine that you are an Internal Requestor because a dss.mil email address is affiliated with your NCAISS account, and will display the Internal OBMS Access Request Form.
3. Complete the form, selecting "User OBMS Title" and "User OBMS Region" from the drop-down lists, adding "Role" assignment(s), and providing your Sponsor's (current DSS Supervisor) email address, as shown in Figure 76. **Note:** As an Internal OBMS User, your Sponsor must have a dss.mil email address.
   Note: If you have previously completed the User Information data fields (e.g., Name, Address, Organization, Phone Number, etc.) the data will be pre-populated and locked for editing; should you need to revise your previously entered information you may do so on the Profile tab (see Section 7 for additional guidance on editing the user profile).
4. Click "Submit."

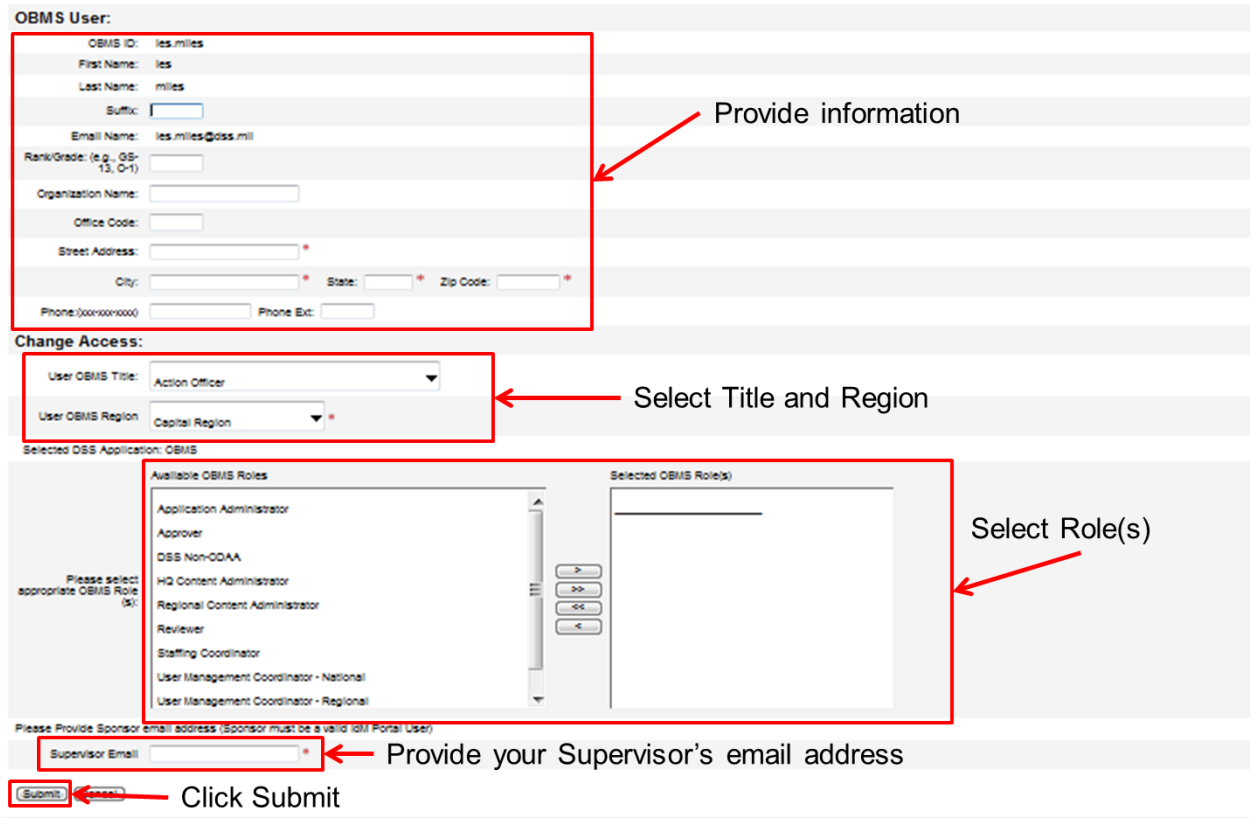


Figure 76: Internal OBMS Access Request Form

5. A confirmation screen will be displayed, as shown in Figure 77. Confirm the accuracy of the information.
6. Click "Cancel" to cancel the request if changes are needed.
7. Click "Confirm" to submit the request for review.

OBMS User:

OBMS ID:	les.miles
First Name:	les
Last Name:	miles
Suffix:	
Email Name:	les.miles@dss.mil
Rank/Grade: (e.g., GS-13, O-1)	
Organization Name:	
Office Code:	
Street Address:	10430 Furnance Road
City:	Lorton State: VA Zip Code: 22079
Phone:(xxx-xxx-xxxx)	Phone Ext:
Sponsor:	marques.colston
Sponsor Email:	marques.colston@dss.mil
Title:	Action Officer
Region:	Capital Region

Current Access:

User Type	System Role(s)

New Access:

User Type	System Role(s)
OBMS	Application Administrator

Please confirm the new access

Confirm Cancel

Figure 77: OBMS Internal Access Request Confirmation

8. Upon clicking “Confirm” your access request is submitted and you are returned to the NCAISS Home Page.

12.2.2 OBMS External Government (non-DSS) Submitter User Access Request

This process allows an External OBMS Government Submitter Access Requestor with a non-dss.mil email address to request access to the OBMS application. **Note:** This process assumes that the Access Requestor has a valid NCAISS account and has already logged into NCAISS, as described in Section 5.

1. Once logged into NCAISS, click the “Request/Manage OBMS Access” link, as shown in Figure 75.
2. NCAISS will determine that you are an External Government Submitter Requestor because a .gov or .mil (non-dss.mil) email address is affiliated with your NCAISS account, and will display the External OBMS Access Request Form for Government Submitter users.
3. Complete the form, selecting “OBMS User Title” from the drop-down list, adding the “Role” assignment, providing your Sponsor’s (your current supervisor within your government organization) email address, as shown in Figure 78.
   Note: Your Sponsor must have an NCAISS account in order to approve your access to OBMS – you will not be able to submit your OBMS access request until your Sponsor creates an NCAISS account.
   Note: If you have previously completed the User Information data fields (e.g., Name, Address, Organization, Phone Number, etc.) the data will be pre-populated and locked for editing; should you need to revise your previously entered information you may do so on the Profile tab (see Section 7 for additional guidance on editing the user profile).
4. Click “Submit.”

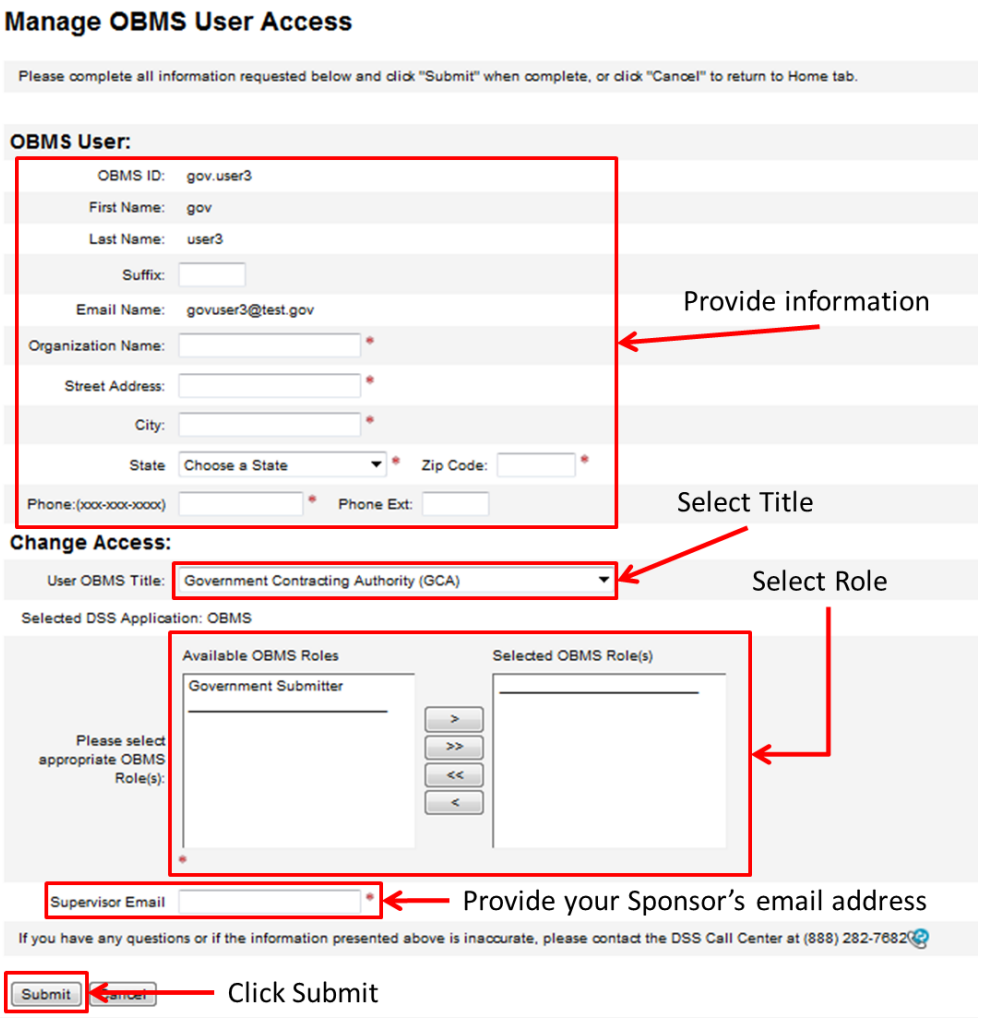


Figure 78: OBMS Government Submitter Access Request Form

5. A confirmation screen will be displayed, as shown in Figure 79. Confirm the accuracy of the information.
6. Click "Cancel" to cancel the request if changes are needed.
7. Click "Confirm" to submit the request for review.

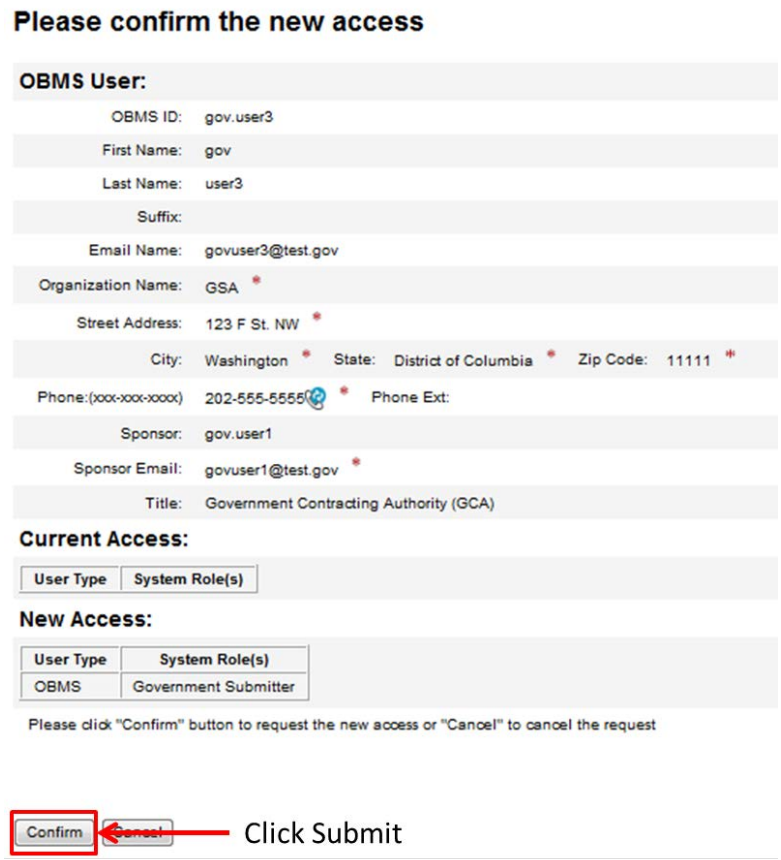


Figure 79: OBMS Government Submitter Access Request Confirmation

8. Upon clicking “Confirm” your access request is submitted and you are returned to the NCAISS Home Page.

12.2.3 OBMS External Contractor (Industry) Submitter User Access Request

This process allows an External OBMS Contractor Submitter Access Requestor with a (non-.gov or .mil) email address to request access to the OBMS application. **Note:** This process assumes that the Access Requestor has a valid NCAISS account and has already logged into the NCAISS, as described in Section 5.

1. Once logged into the NCAISS, click the “Request/Manage OBMS Access” link, as shown in Figure 75.
2. NCAISS will determine that you are an External Requestor because a non-dss.mil email address is affiliated with your NCAISS account, and will display the External OBMS Access Request Form.
3. Complete the form, selecting “OBMS User Title” from the drop-down list, adding the “Role” assignment, and providing CAGE Code and KMP email address, as shown in Figure 80.
   Note: You may add additional CAGE Codes by clicking the “Add Another CAGE Code” button. You must provide a KMP email address for each CAGE Code that you’re requesting. Each KMP must have a valid NCAISS account in order to approve access to the respective CAGE Code.
   Note: If you are requesting CAGE Code changes to your existing OBMS account, then you must use the “Add Another CAGE Code” button, input the necessary information, and then remove the un-needed CAGE Code(s).
   Note: A KMP requesting OBMS access for a CAGE Code that he/she manages or maintains may self-sponsor their request by using the email address associated with their NCAISS account for the corresponding CAGE Codes; the KMP will be required to approve each CAGE Code request that he/she self-sponsors upon submitting the request form.
   Note: You may search for the appropriate CAGE Code using the link provided; once found copy and paste the appropriate code into the “Cage Code” box.
   Note: If you have previously completed the User Information data fields (e.g., Name, Address, Organization, Phone Number, etc.) the data will be pre-populated and locked for editing; should you need to revise your

previously entered information you may do so on the Profile tab (see Section 7 for additional guidance on editing the user profile).

4. Click "Submit."

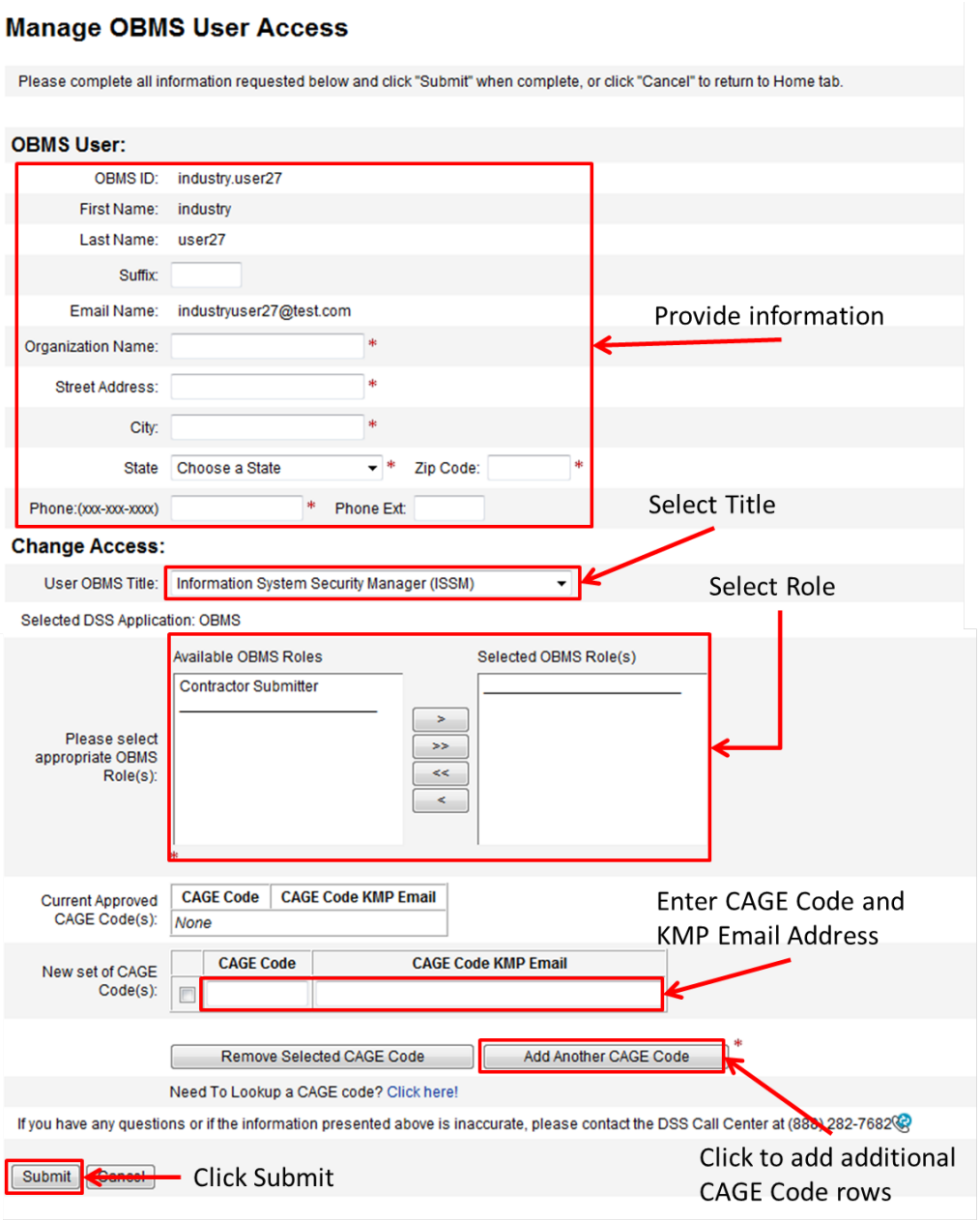


Figure 80: External OBMS Access Request Form

5. A confirmation screen will be displayed, as shown in Figure 81. Confirm the accuracy of the information.
6. Click "Cancel" to cancel the request if changes are needed.
7. Click "Confirm" to submit the request for review.

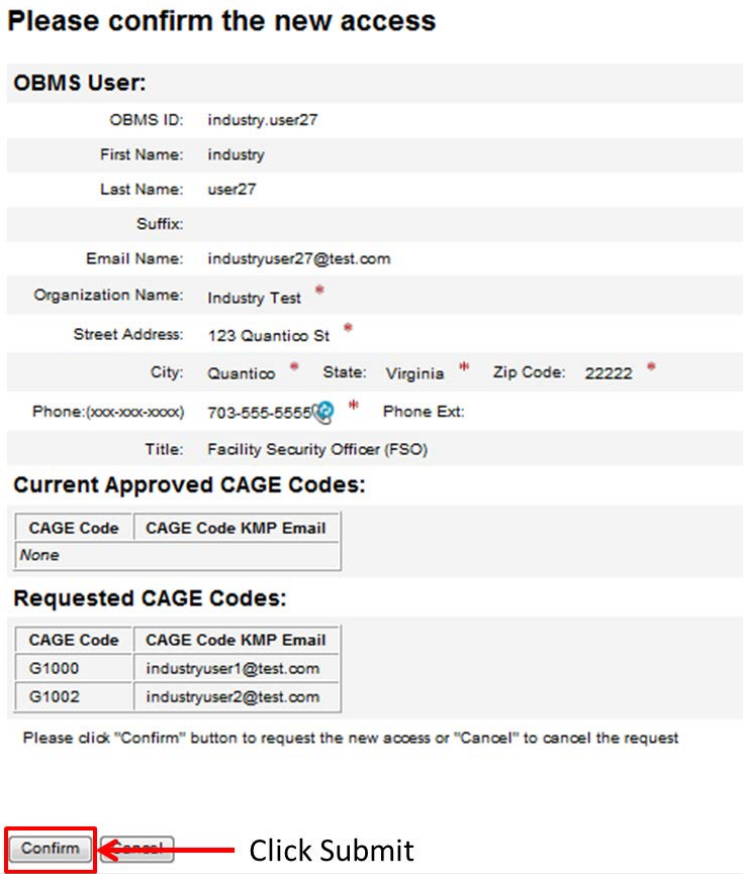


Figure 81: External OBMS Account Request Confirmation

8. Upon clicking “Confirm” your access request is submitted and you are returned to the NCAISS Home Page.

12.3 Reviewing and Approving/Rejecting OBMS Access Requests

When an OBMS Access Requestor submits a request to access the OBMS application, a Work Item is added in the appropriate Sponsor’s queue. **Note:** Internal OBMS Access Requestors specify their current DSS Supervisor as their Sponsor, External Government Submitter Access Requestors specify their current government organization supervisor as their Sponsor, and External Contractor (Industry) Submitter Access Requestors specify the KMP for each requested CAGE Code as their Sponsor(s). Once approved by the Sponsor, accounts for Internal and External Government Submitter OBMS Access Requests are created by NCAISS and the user is notified. External Contractor Submitter OBMS Account Requests must be reviewed approved by the DSS Call Center, in addition to the Requestor’s Sponsor(s), prior to account creation. This subsections that follow outline the process for reviewing and approving or rejecting OBMS access requests at the Sponsor-level. **Note:** Refer to the Account Administrator User Guide for guidance on DSS Call Center processing of OBMS External Contractor Submitter Access Requests.

12.3.1 Sponsor Approval for OBMS Internal (DSS.mil) Access Requests

The following steps outline the process for reviewing and approving access to OBMS Internal users as the Sponsor (DSS Supervisor).

1. Log into NCAISS, as described in Section 5.
2. Click on either the “Approvals” bar or the “Work Items” tab.
3. The “Work Items” tab is displayed with a list of requests awaiting approval, as shown in Figure 82.
4. There are two ways to approve a request:
    a. You can check the checkbox next to the request and click “Approve.” **Note:** To approve multiple requests, check the top checkbox to select all requests in the list and click “Approve.”

b. Click on “New Account Request” link in the Request box.

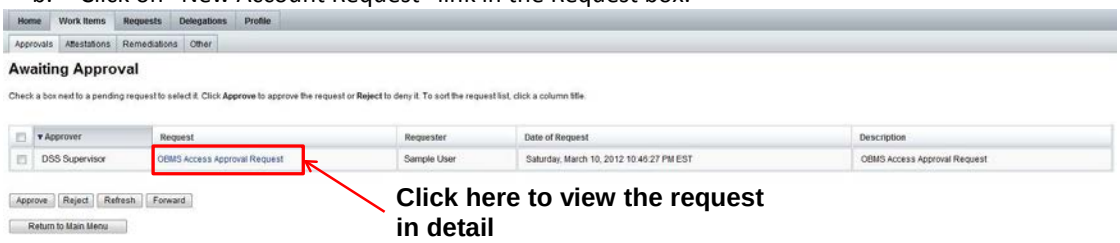


Figure 82: OBMS Access Request Work Item

5. The OBMS Access Request Approval detail view is displayed, as shown in Figure 83. Here you can view the account details and the account type the user is requesting.
6. Review the request and click either “Approve” or “Reject” to grant or deny the request.
   Note: The Sponsor may change a requestor’s role selection, if needed.
   Note: If you are rejecting the OBMS access request, then you must enter a comment into the comment box.

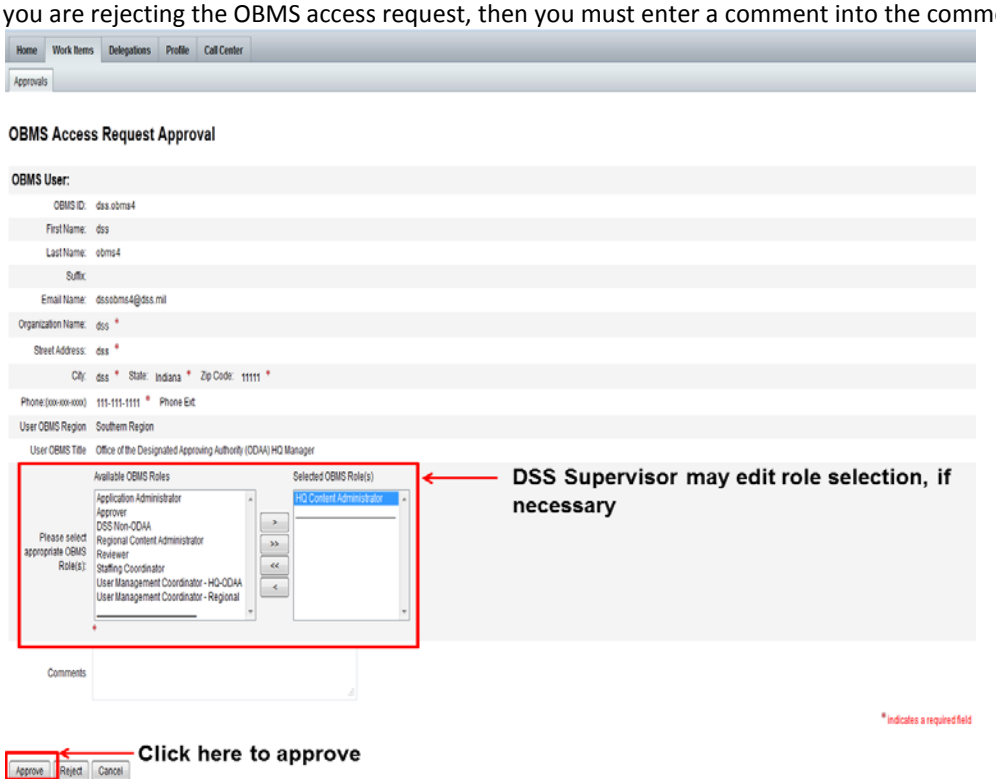


Figure 83: OBMS Access Request Review - Detailed View

7. Upon clicking “Approve,” the system redirects you to the NCAISS Home Page. **Note:** If you have additional items to approve, click on either the “Approvals” bar or the “Works Items” tab to continue.

12.3.2 Sponsor Approval for OBMS External Government Submitter Access Requests

The following steps outline the process for reviewing and approving access to OBMS External Government Submitter users as the Sponsor (Government Organization Supervisor).

1. Log into NCAISS, as described in Section 5.
2. Click on either the “Approvals” bar or the “Work Items” tab.
3. The “Work Items” tab is displayed with a list of requests awaiting approval, as shown in Figure 82.
4. There are two ways to approve a request:
   a. You can check the checkbox next to the request and click “Approve.” **Note:** To approve multiple requests, check the top checkbox to select all requests in the list and click “Approve.”

b. Click on “New Account Request” link in the Request box.

5. The OBMS Access Request Approval detail view is displayed, as shown in Figure 84. Here you can view the account details and the account type the user is requesting.
6. Review the request and click either “Approve” or “Reject” to grant or deny the request.
   Note: If you are rejecting the OBMS access request, then you must enter a comment into the comment box.

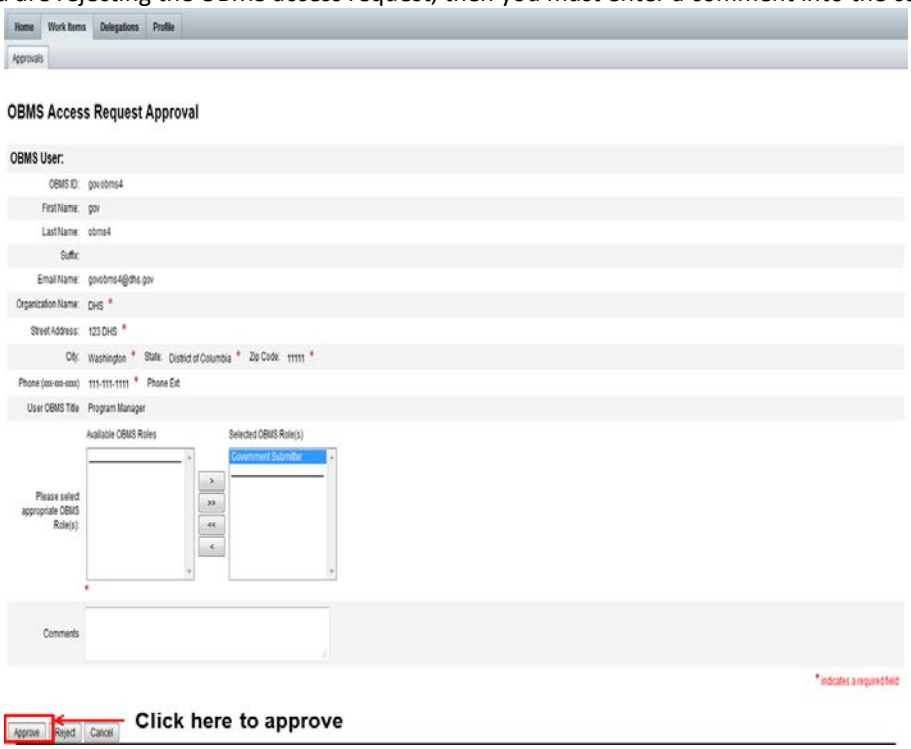


Figure 84: OBMS Government Submitter Approval Form

7. Upon clicking “Approve,” the system redirects you to the NCAISS Home Page. **Note:** If you have additional items to approve, click on either the “Approvals” bar or the “Works Items” tab to continue.

12.3.3 Sponsor Approval for OBMS External Contractor Submitter Access Requests

The following steps outline the process for reviewing and approving access to OBMS External Contractor Submitter users as the Sponsor (KMP for specified CAGE Code). **Note:** OBMS Contractor Submitters may request access to multiple CAGE Codes; a KMP must be specified for each CAGE Code requested. Accordingly, there may be multiple Sponsor-level approves required for a single OBMS Contractor Submitter access request; access to each CAGE Code must be approved or rejected by the specified KMP before the access request can be processed by the DSS Call Center. Failure to approve or reject an OBMS Contractor Submitter access request as the Sponsor within seven (7) days will result in automatic rejection of access to the specified CAGE Code(s).

1. Log into NCAISS, as described in Section 5.
2. Click on either the “Approvals” bar or the “Work Items” tab.
3. The “Work Items” tab is displayed with a list of requests awaiting approval, as shown in Figure 82.
4. There are two ways to approve a request:
   a. You can check the checkbox next to the request and click “Approve.” **Note:** To approve multiple requests, check the top checkbox to select all requests in the list and click “Approve.”
   b. Click on “New Account Request” link in the Request box.
5. The OBMS Access Request Approval detail view is displayed, as shown in Figure 85. Here you can view the account details and the account type the user is requesting.
6. Review the request and click either “Approve” or “Reject” to grant or deny the request.
   Note: If you are rejecting the OBMS access request, then you must enter a comment into the comment box.

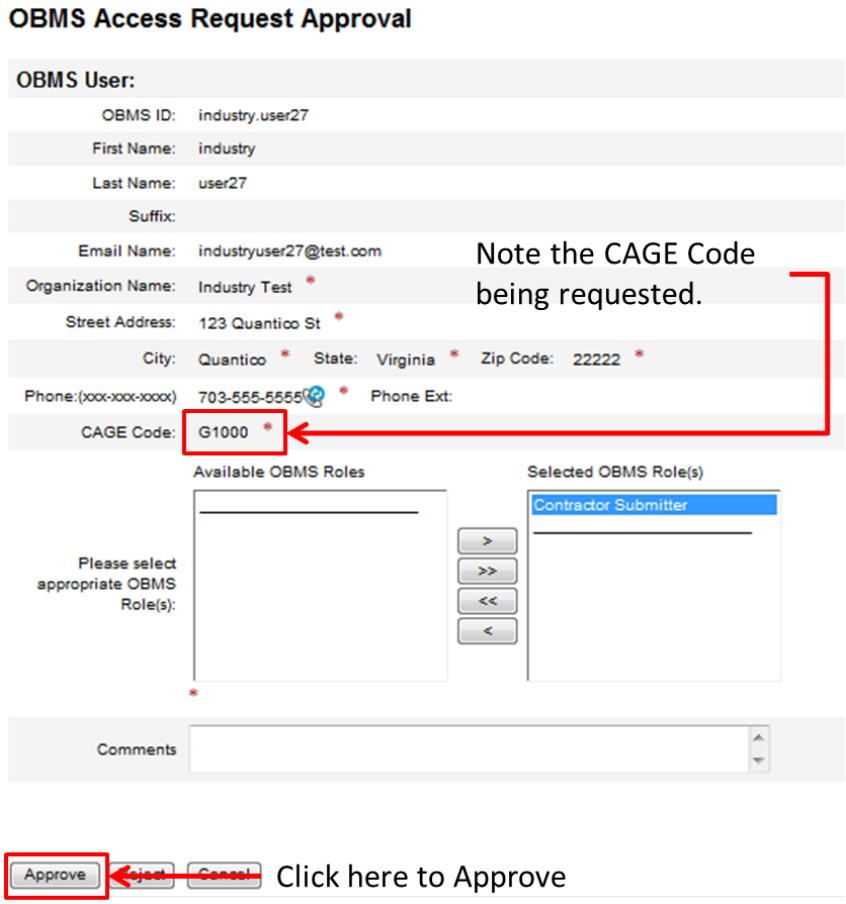


Figure 85: OBMS Contractor Submitter Approval Form

7. Upon clicking "Approve," the system redirects you to the NCAISS Home Page. **Note:** If you have additional items to approve, click on either the "Approvals" bar or the "Works Items" tab to continue.

OBMS External Contractor Submitter account requests must be reviewed and approved by a DSS Call Center Agent, in addition to the Access Requestor's Sponsor(s) (Organization KMP) for the requested CAGE Code(s). **Note:** Refer to the Account Administrator User Guide for guidance on DSS Call Center processing of OBMS External Contractor Submitter Access Requests.

12.4 Managing OBMS User Accounts

This section provides step-by-step instructions related to the process that allows an OBMS User Management Coordinator to modify an OBMS user's assigned OBMS role(s) (i.e., add or remove roles) and modify a user's OBMS profile (i.e., change region code or CAGE code) within the NCAISS Solution.

12.4.1 Managing OBMS Internal and External Government Submitter User Accounts

1. Log into OBMS, as described in Section 12.1.
2. Click the "Edit Role" or "Edit Title," as appropriate, from the "User Management" tab within the OBMS User Management Coordinator interface, as shown in Figure 86.

Figure 86: OBMS User Management Coordinator Interface

3. OBMS re-directs you to NCAISS and the NCAISS Solution starts the User Management workflow. Search for the desired OBMS user by inputting search parameters and clicking "Search."
    a. You may search for a user by entering any combination of: OBMS user ID, First Name, Last Name, or Email Address
    b. Entering no search criteria will display a list of all available OBMS users

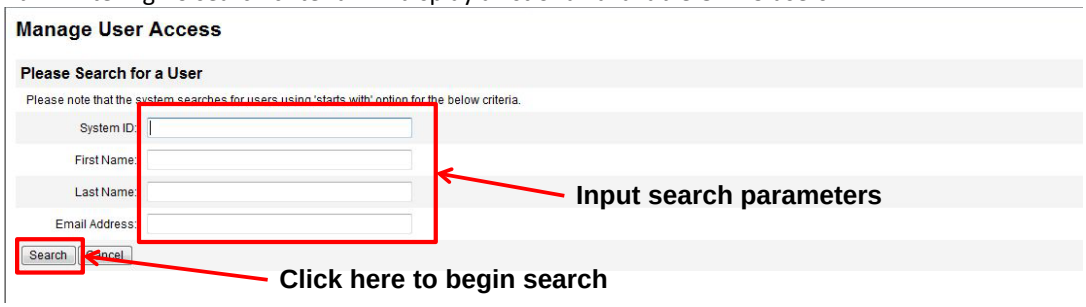


Figure 87: Search for an OBMS User

4. NCAISS will display the results of the OBMS user search. Click the "Manage Access" button, as shown in Figure 88.

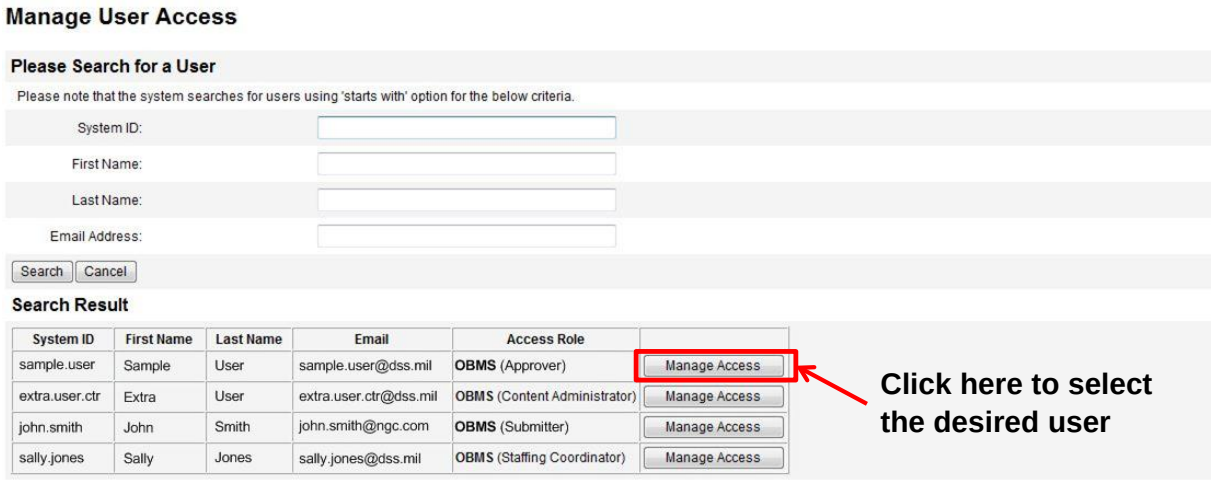


Figure 88: OBMS User Search Results

5. NCAISS displays the desired user's record, as shown in Figure 89. Modify the user's account, as necessary.
   Note: To disable a user's access to OBMS, remove all OBMS roles from the user's account.
   Note: To reinstate a disabled user's access to OBMS, add a role to the user's account.
6. Click "Save" to store the changes that you have made to the user's account. **Note:** Clicking "Cancel" will discard any changes that have been made to the user's account.

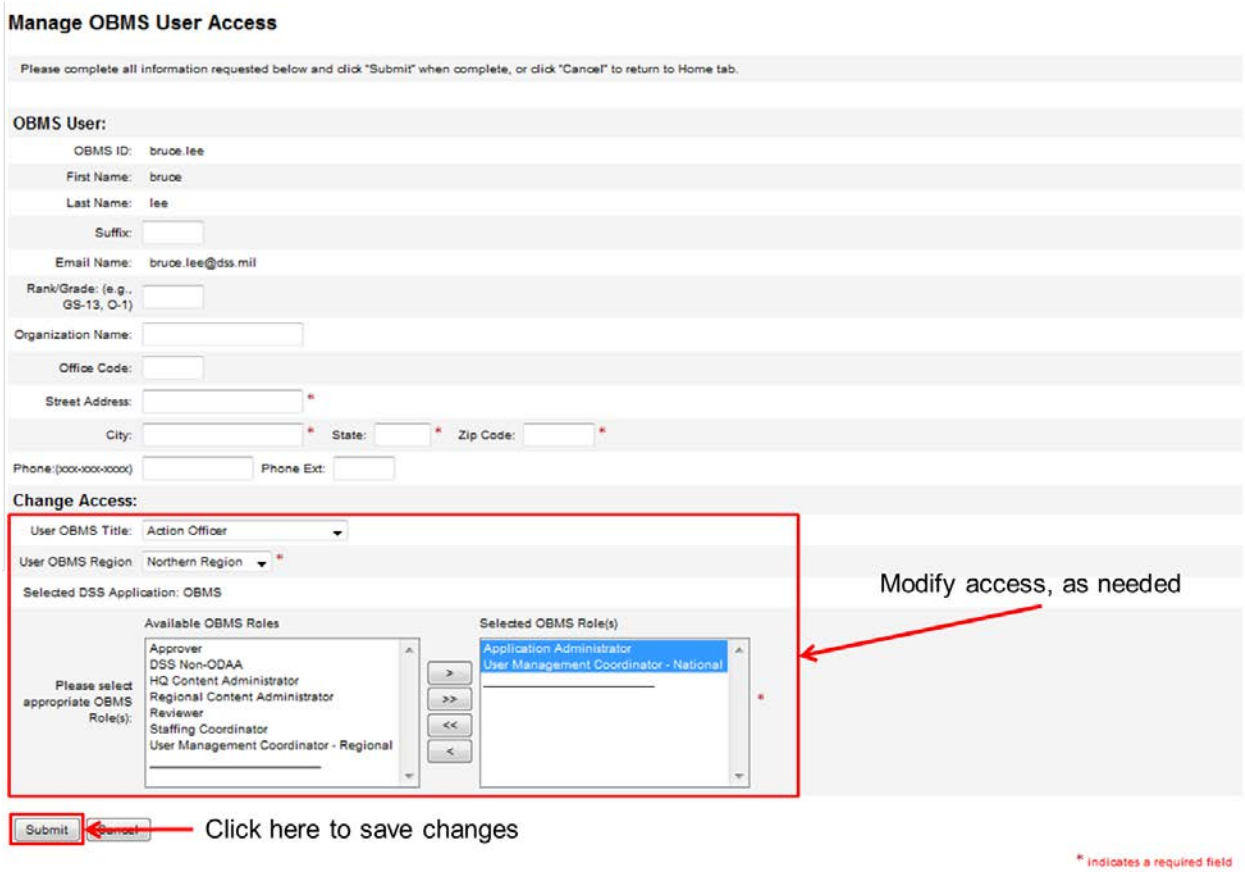


Figure 89: Manage OBMS User Profile

12.4.2 Managing OBMS External Contractor Submitter User Accounts

1. Log into OBMS, as described in Section 12.1.
2. Click the "Edit Role" or "Edit Title," as appropriate, from the "User Management" tab within the OBMS User Management Coordinator interface, as shown in Figure 86.
3. OBMS re-directs you to NCAISS and the NCAISS Solution starts the User Management workflow. Search for the desired OBMS user by inputting search parameters and clicking "Search."
   a. You may search for a user by entering any combination of: OBMS user ID, First Name, Last Name, or Email Address
   b. Entering no search criteria will display a list of all available OBMS users
4. NCAISS will display the results of the OBMS user search. Click the "Manage Access" button, as shown in Figure 88.
5. NCAISS displays the desired user's record, as shown in Figure 90. Modify the user's account, as necessary.
   Note: To disable a user's access to OBMS, remove all OBMS roles from the user's account.
   Note: To reinstate a disabled user's access to OBMS, add a role to the user's account.
6. Click "Save" to store the changes that you have made to the user's account. **Note:** Clicking "Cancel" will discard any changes that have been made to the user's account.

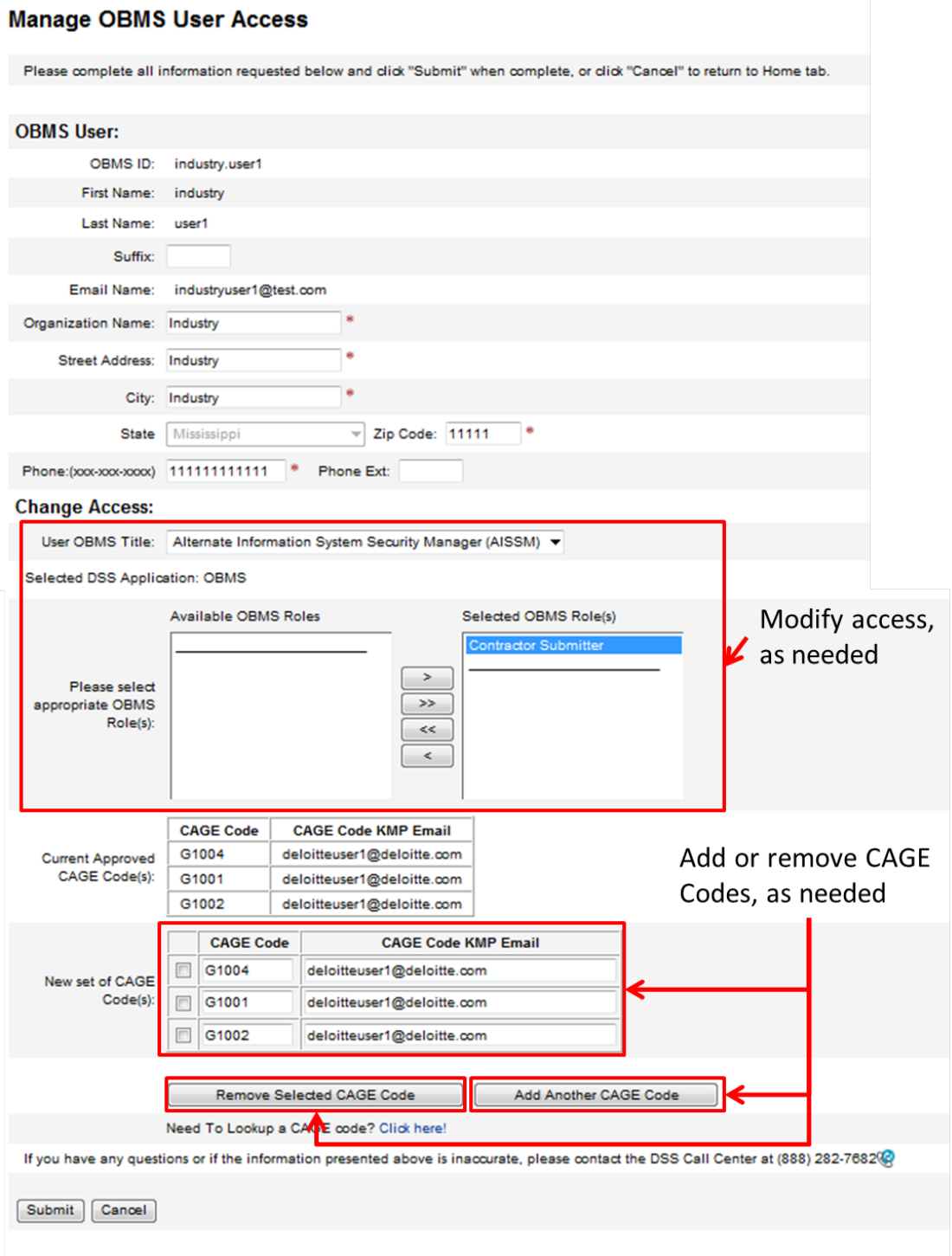


Figure 90: Manage OBMS Contractor Submitter User

12.5 Produce OBMS User Report

This section provides step-by-step instructions related to the process that allows an OBMS User Management Coordinator to run and produce a report that lists all OBMS users and their assigned OBMS role(s) using the NCAISS Solution.

1. Log into OBMS, as described in Section 12.1.
2. Click the “Reports” tab from within the OBMS User Management Coordinator interface, as shown in Figure 91.

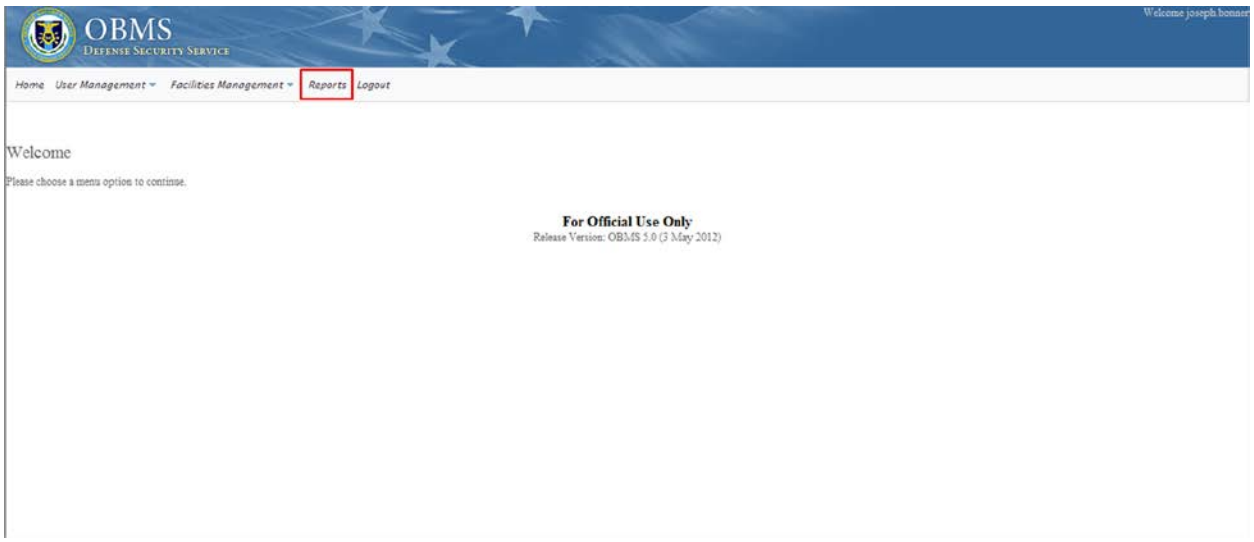


Figure 91: OBMS User Management Coordinator Interface

3. OBMS re-directs you to the NCAISS Reports tab; select the desired report from the list of available options.
4. Click "Run" to produce the desired report in a web browser window. **Note:** Reports can also be downloaded in .csv (MS Excel) or .pdf formats.

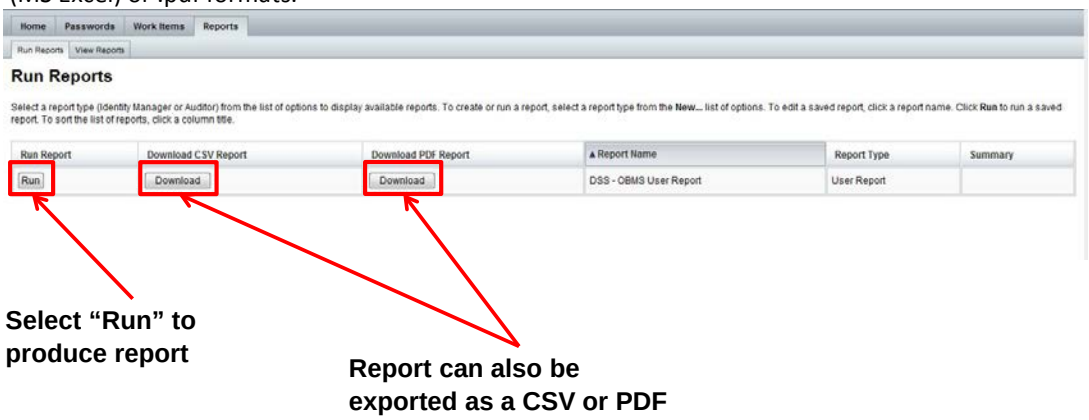
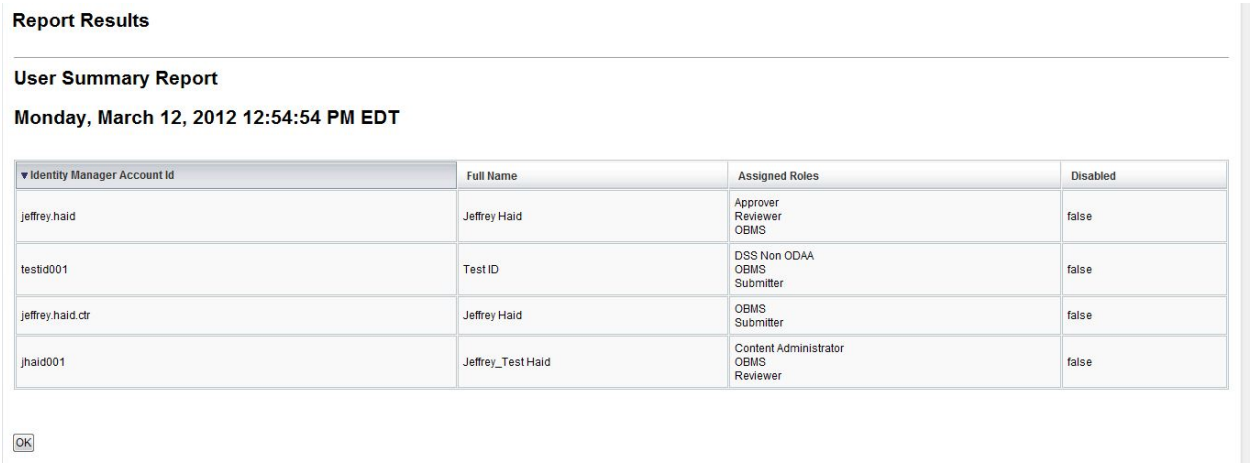


Figure 92: OBMS Report Options



Report Results

User Summary Report

Monday, March 12, 2012 12:54:54 PM EDT

Identity Manager Account Id	Full Name	Assigned Roles	Disabled
jeffrey.haid	Jeffrey Haid	Approver Reviewer OBMS	false
testid001	Test ID	DSS Non ODAA OBMS Submitter	false
jeffrey.haid.ctr	Jeffrey Haid	OBMS Submitter	false
jhaid001	Jeffrey_Test Haid	Content Administrator OBMS Reviewer	false

OK

Figure 93: Sample OBMS User Summary Report

13 STEPP Application NCAISS User Guide

This section describes the step-by-step processes for requesting access to and accessing the STEPP application using the NCAISS Solution. **Note:** this portion of the User Guide focuses exclusively on use of the NCAISS Solution as it relates to the STEPP application. Actions that a user may take within the STEPP application, following successful authentication, are out of scope for this User Guide. This section assumes that a STEPP access requestor already has a valid NCAISS user account. If a valid NCAISS user account does not exist, refer to Section 3 for step-by-step instructions for NCAISS self-enrollment.

13.1 Accessing STEPP

Following STEPP's integration with NCAISS, STEPP users are able to use their existing CAC/PKI credentials to gain access to STEPP application. **Note:** Use of CAC/PKI credentials for access to STEPP is optional; STEPP users may continue to access the application using their existing username/password.

For convenience, there are three ways in which a user may authenticate to STEPP, including:

- Navigate to the public-facing STEPP home page and click "CAC/PKI Login" (CAC/PKI Authentication from the STEPP Homepage)
- Access STEPP from NCAISS (CAC/PKI Authentication from NCAISS)
- Login to STEPP using existing username/password authentication process (STEPP Username/Password Authentication)

The following sections provide step-by-step instructions for accessing STEPP using the three methods described above. **Note:** This section assumes that the User already possesses valid NCAISS and STEPP application accounts.

13.1.1 CAC/PKI Authentication from the STEPP Homepage

The steps below describe the process for accessing STEPP via NCAISS from the STEPP homepage through the use of a CAC or DoD-approved ECA certificate.

1. Navigate to the unauthenticated STEPP homepage (http://www.dss.mil/seta/enrol/stepp.html).
2. Select the "CAC/PKI Login" button, as shown in Figure 94.

Figure 94: CAC/PKI Login from STEPP Homepage

3. You are redirected to NCAISS Disclaimer page, as shown in Figure 68. Select "I Accept" to proceed.

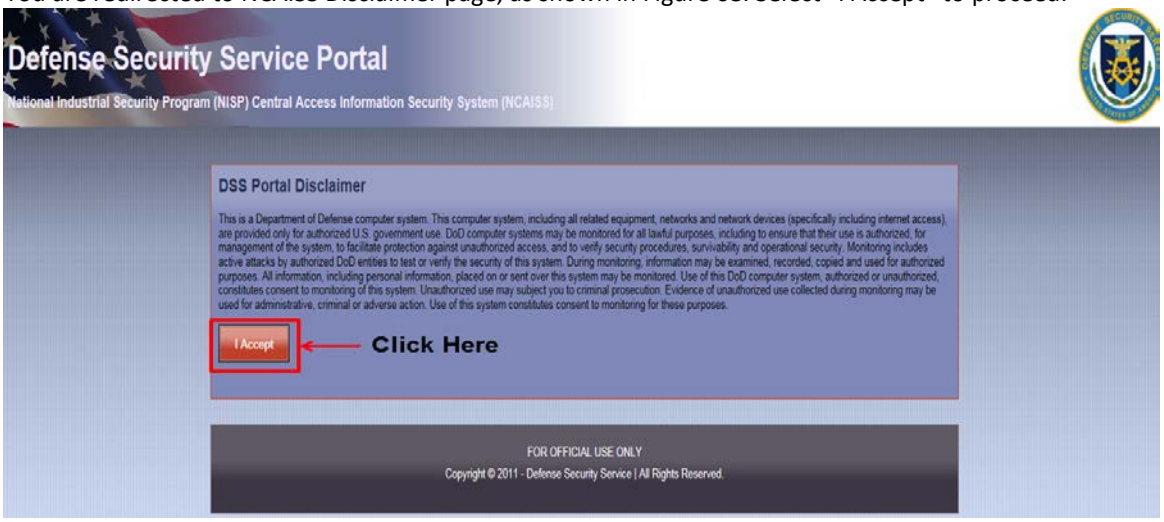


Figure 95: NCAISS Disclaimer

4. The unauthenticated NCAISS page is displayed, as shown in Figure 69. Select "CAC/ECA Login" to proceed.

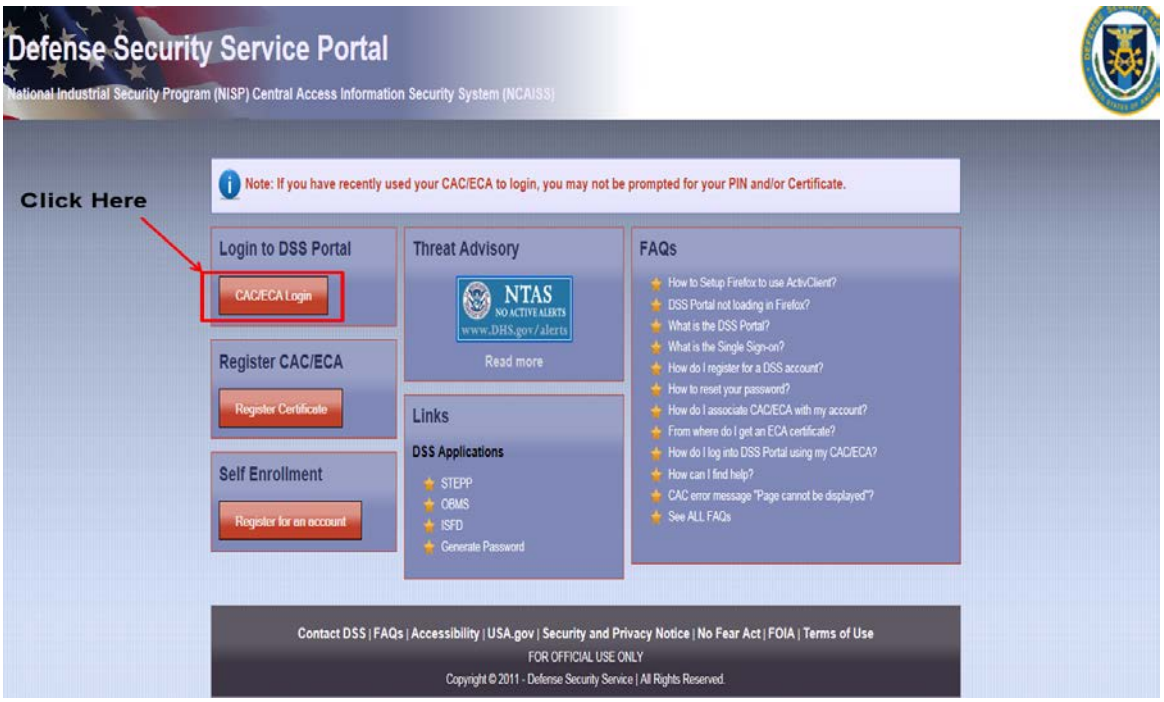


Figure 96: Unauthenticated NCAISS Home Page

5. Select the certificate that you would like to use. **Note:** You must use the certificate that has been associated to your NCAISS account.

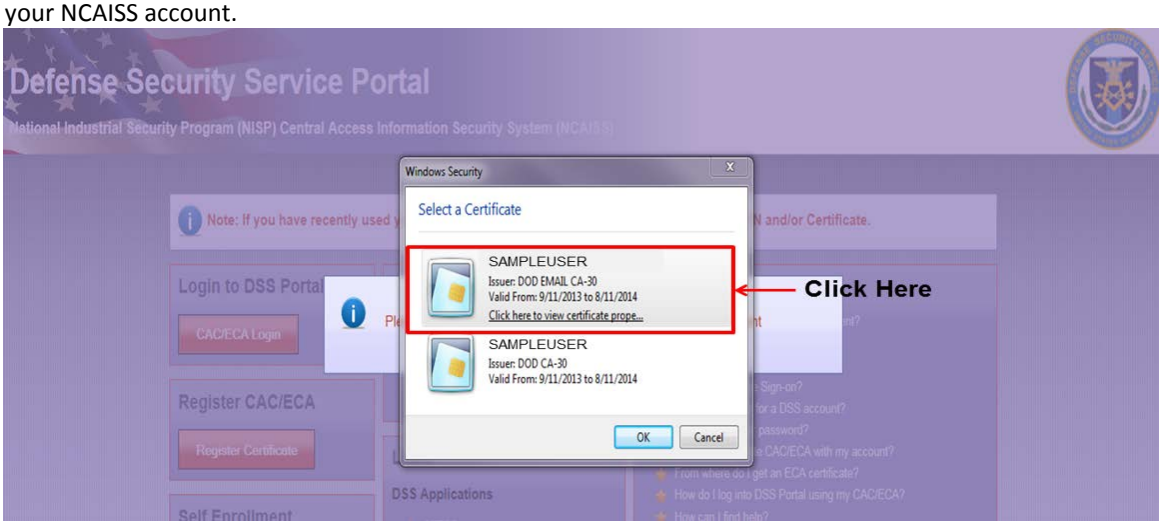


Figure 97: Certificate Selection

6. Enter your PIN.

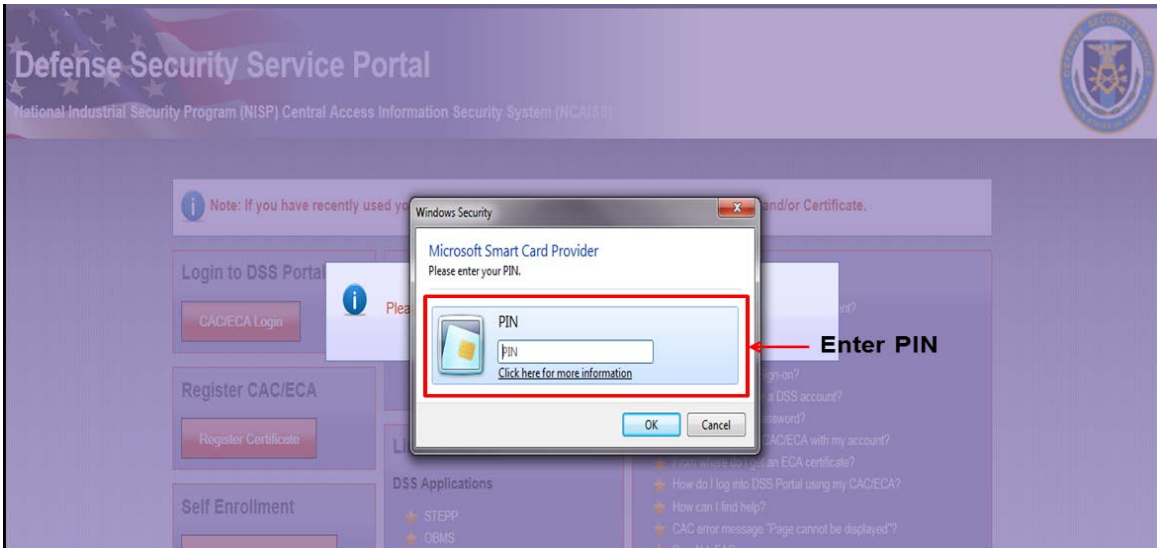


Figure 98: PIN Entry

7. The NCAISS Solution authenticates you and determines if you have multiple STEPP accounts correlated with NCAISS. **Note:** If you have only a single STEPP account correlated with NCAISS, then proceed to Step 9.
8. If multiple STEPP accounts have been correlated with NCAISS, then the NCAISS Solution will prompt you to select which account you wish to use, as shown in Figure 99. Select the desired account and click "Continue."

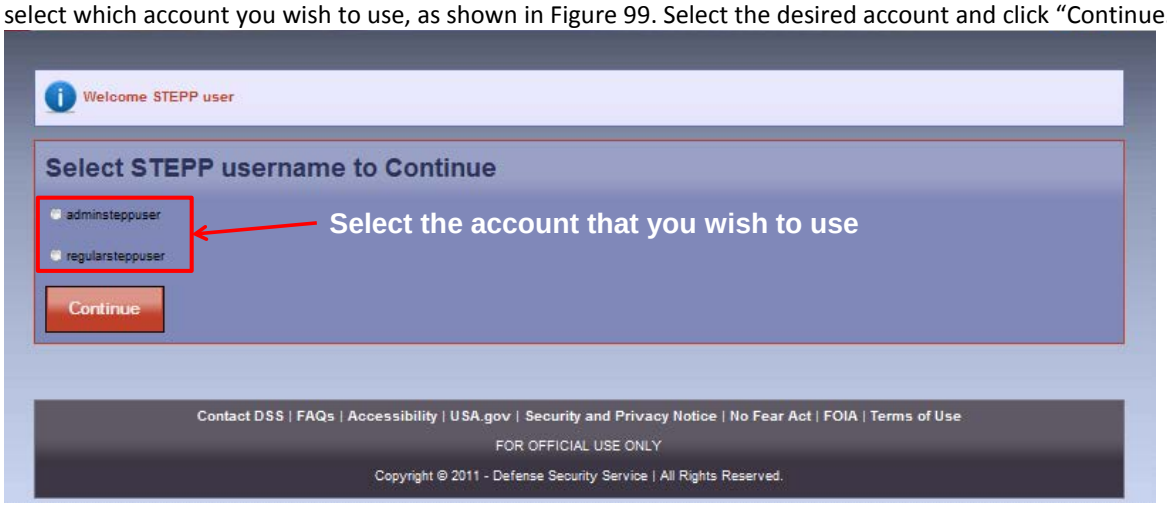


Figure 99: Multiple STEPP Account Selection

9. NCAISS directs you to STEPP. The STEPP user's homepage is displayed, as shown in Figure 100.

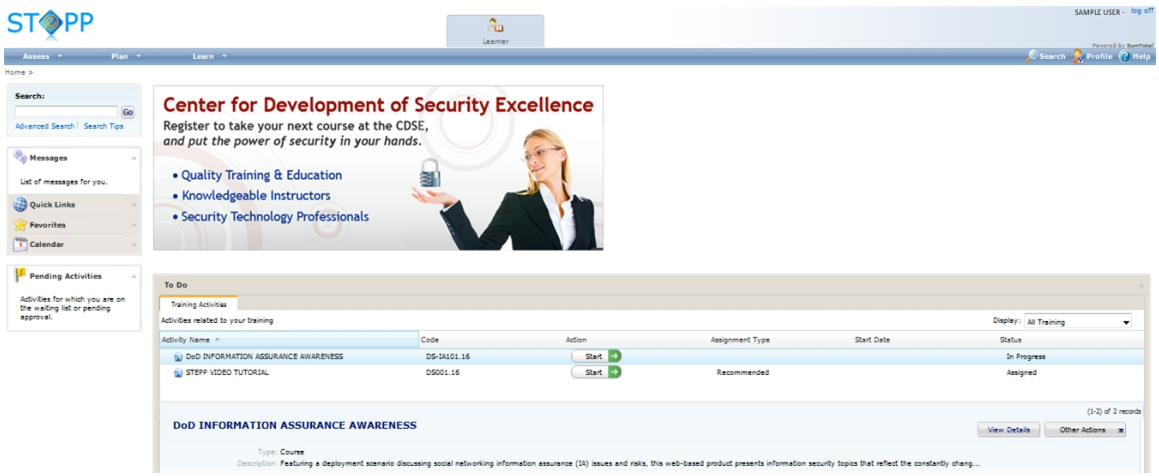


Figure 100: STEPP User Homepage

Note: If you have a multiple STEPP accounts correlated with NCAISS and wish to log into STEPP via NCAISS with another STEPP account, you must log out of STEPP and NCAISS and close your web browser. After you have closed the browser session, open a new browser session and access NCAISS. After accessing NCAISS, follow steps 8 thru 10 above selecting the appropriate STEPP account to access STEPP.

13.1.2 CAC/PKI Authentication (to STEPP) from NCAISS

The steps below describe the process for accessing STEPP via NCAISS from NCAISS through the use of a CAC or DoD-approved ECA certificate.

1. Navigate to NCAISS (https://sso.dss.mil) in your web browser.
2. Authenticate to NCAISS, as described in Section 5.
3. Upon successful authentication, the NCAISS Home Page is displayed.
4. Click the “Access STEPP” link within the “STEPP Quick Links,” as shown in Figure 101.

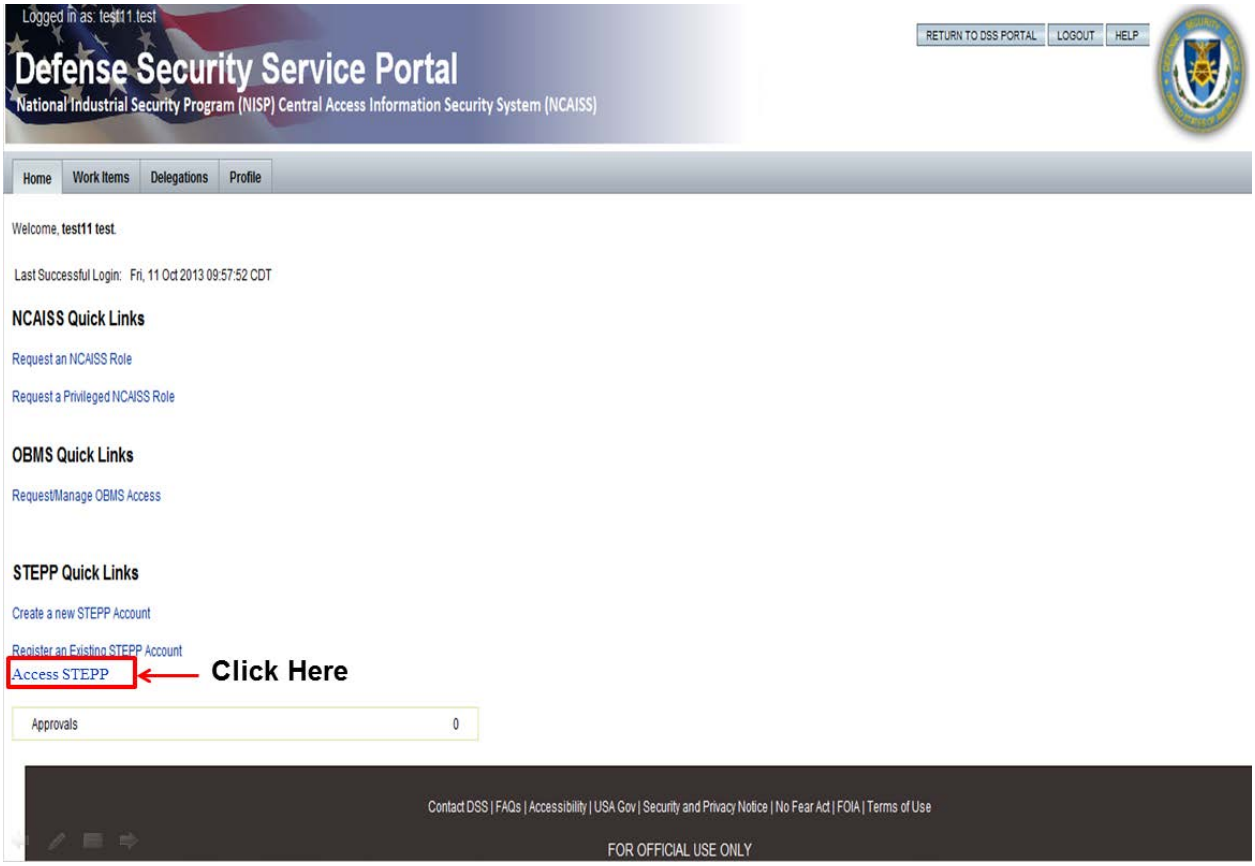


Figure 101: Access STEPP from the NCAISS Home Page

5. The NCAISS Solution authenticates you and determines if you have multiple STEPP accounts correlated with NCAISS. **Note:** If you have only a single STEPP account correlated with NCAISS, then proceed to Step 7.
6. If multiple STEPP accounts have been correlated with NCAISS, then the NCAISS Solution will prompt you to select which account you wish to use, as shown in Figure 99. Select the desired account and click "Continue."
7. NCAISS directs you to STEPP. The STEPP user's homepage is displayed, as shown in Figure 100.

Note: If you have a multiple STEPP accounts correlated with NCAISS and wish to log into STEPP via NCAISS with another STEPP account, you must log out of STEPP and NCAISS and close your web browser. After you have closed the browser session, open a new browser session and access NCAISS. After accessing NCAISS, follow Steps 6 thru 7 above selecting the appropriate STEPP account to access STEPP.

13.1.3 Username/Password Authentication (to STEPP)

STEPP users that wish to continue to use STEPP username and password credentials to access STEPP may do so without the need to login to NCAISS. For step-by-step instructions for logging into STEPP with username and password, refer to the STEPP FAQs (http://www.dss.mil/seta/enrol/enrol-log-in.html).

13.2 First Time Access to STEPP via NCAISS (Existing STEPP Users)

Existing STEPP users (i.e., users that have a STEPP account prior to September 2012) that wish to use their CAC/PKI credentials to access STEPP will be required to go through a one-time process to link (correlate) their STEPP account with their NCAISS account. The steps below describe the one-time process that an existing STEPP user will undergo during their first attempt to access STEPP via NCAISS. **Note:** This section assumes that the user already possesses valid STEPP and NCAISS accounts.

1. Attempt to login to STEPP by completing Steps 1-6 in Section 13.1.1.

2. NCAISS will authenticate you and determine that a STEPP account has not yet been correlated with NCAISS. NCAISS will display a query to determine whether an existing STEPP account exists, as shown in Figure 102. Select "Yes" and click "Next." **Note:** If you do not have an existing STEPP account click "No," then refer to Section 5.

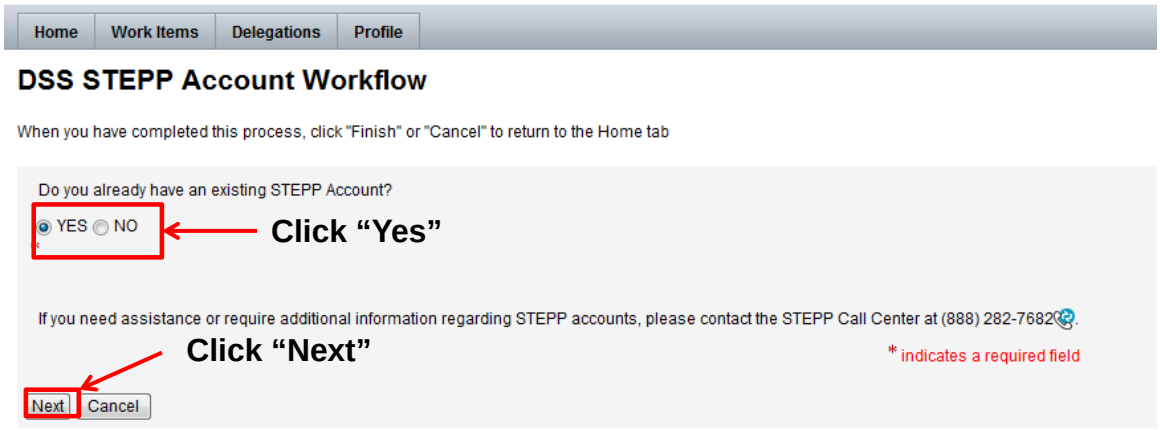


Figure 102: Existing STEPP Account Query

3. Enter your STEPP Username and STEPP Password when prompted and select "Finish," as shown in Figure 103. **Note:** If you have forgotten your password you may use the STEPP password reset capability by clicking the link.

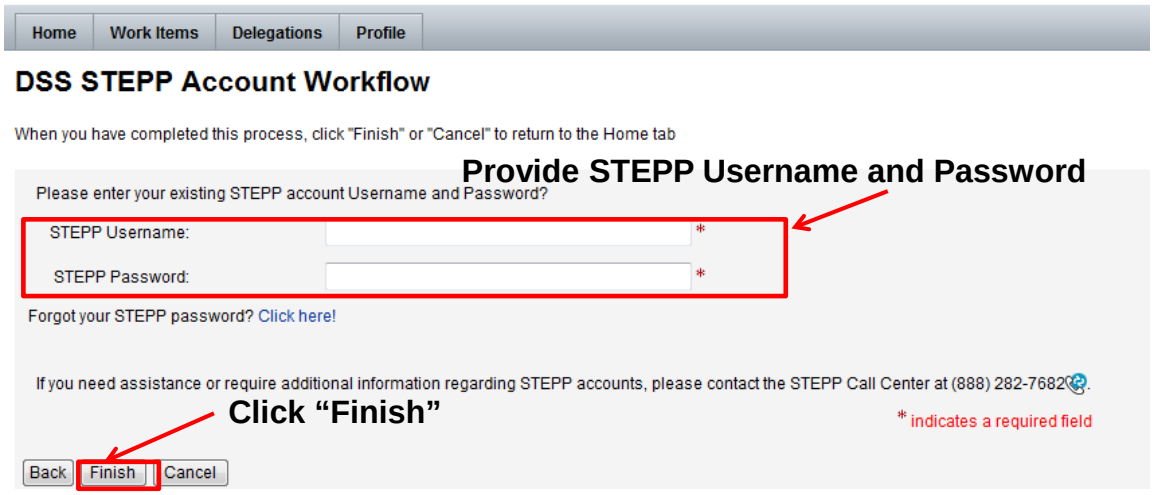


Figure 103: STEPP Username/Password Entry

4. NCAISS will validate your username and password with STEPP and, if successful, notify you that your account has been correlated with NCAISS, as shown in Figure 104. Click the "Go to STEPP" button to proceed to STEPP.

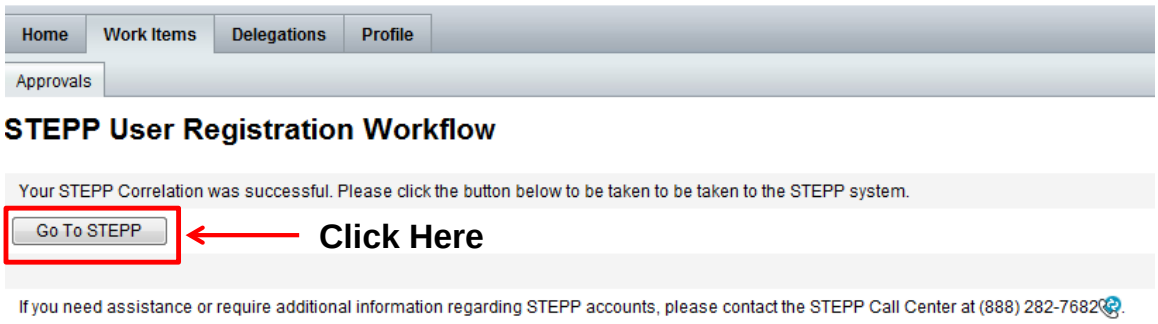


Figure 104: STEPP Account Correlation Successful

5. NCAISS directs you to STEPP. The STEPP user's homepage is displayed, as shown in Figure 100.

13.3 Requesting a STEPP User Account (via NCAISS)

NCAISS users may request access to STEPP through the Portal by completing the STEPP account request form. When requesting a new STEPP account via NCAISS, users will not need to correlate their account, as described in Section 13.2, this occurs automatically as part of the workflow. **Note:** Individuals may continue to request access to STEPP from the STEPP Homepage; however, doing so requires that the user correlate his/her STEPP account in NCAISS via the process described in Section 13.2.

The steps below describe the process for requesting a new STEPP account via the STEPP account request form in NCAISS.

1. Log into NCAISS, as described in Section 5. From the NCAISS Home Page, select the "Create a new STEPP Account" link, as shown in Figure 105. **Note:** Selecting "No" to the Existing STEPP Account Query, shown in Figure 102, will initiate the STEPP account creation workflow and direct the user to Step 2, below.

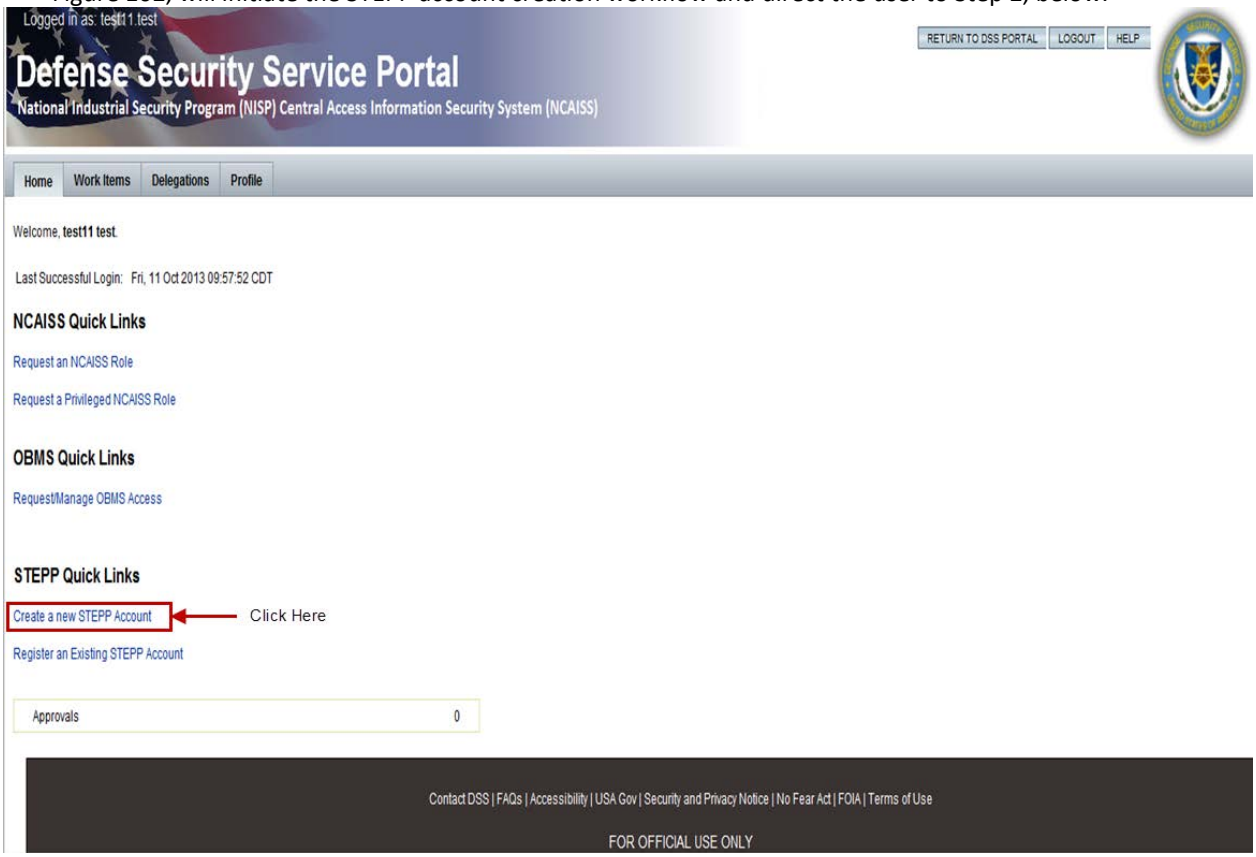


Figure 105: Create a New STEPP Account

2. NCAISS displays the STEPP account request form; review the form for accuracy and click "Finish," as shown in Figure 106. **Note:** The information on the STEPP account request form is locked and cannot be edited by the user; if you find that the form contains incorrect information, please contact the DSS Call Center.

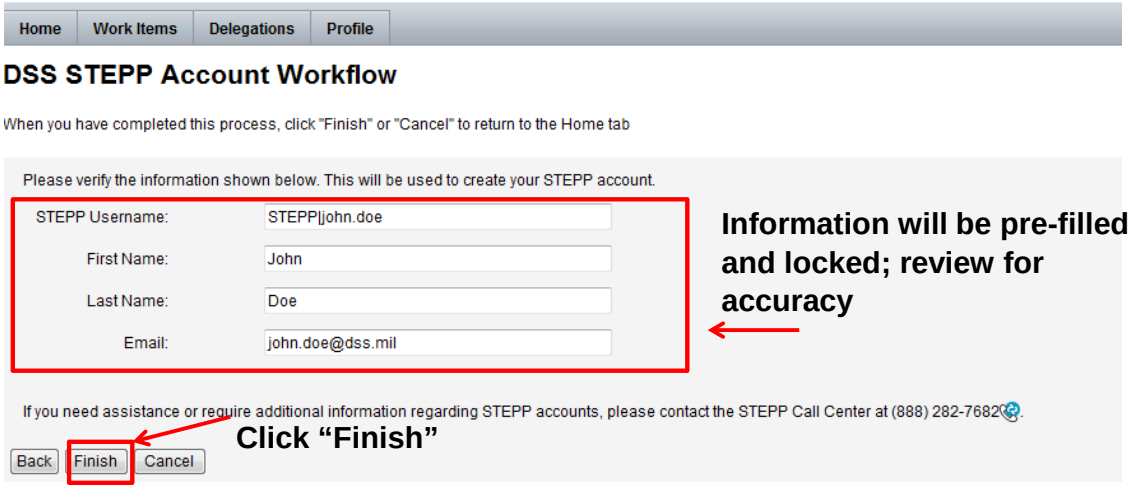


Figure 106: STEPP Account Request Form in NCAISS

3. NCAISS will create a basic STEPP user profile using the information contained in the STEPP account request form and will redirect the user to STEPP to complete the remainder of the account creation process, as shown in Figure 107. Click the "Go to STEPP" button to proceed.

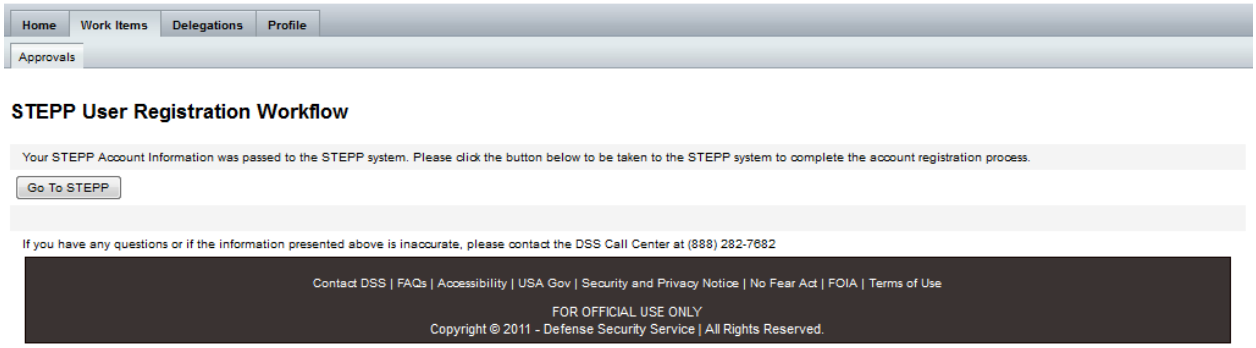


Figure 107: STEPP Account Request - Basic STEPP Profile Created

4. STEPP displays a form requesting additional information from the user, as shown in Figure 108. Complete the form and click "Submit." **Note:** The image below is a sample, refer to STEPP for an up-to-date inventory of the information that is collected from the user.

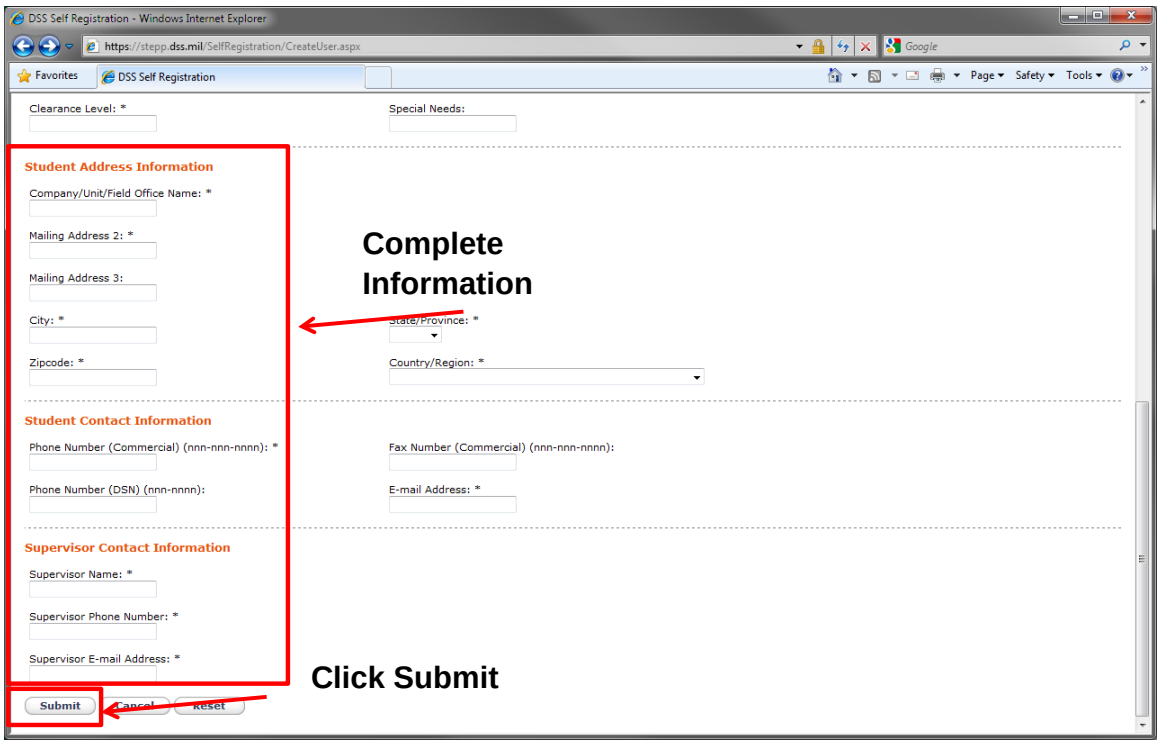


Figure 108: STEPP Account Request - Additional STEPP Information

5. Upon submission of the form, the STEPP account creation process is complete and the user is granted full access to the STEPP application, as shown in Figure 109.

Figure 109: STEPP User Page

13.4 Correlating Additional STEPP Accounts

Existing STEPP users (i.e., users that have a STEPP account prior to September 2012) that wish to use their CAC/PKI credentials to access STEPP will be required to link (correlate) their STEPP account with their NCAISS account. Users with multiple STEPP accounts (e.g., users that have both STEPP user and administrator accounts) will need to correlate each account that they wish to use their CAC/PKI credentials to access. Once a user has correlated their first STEPP account via the process described in Section 13.2, they will be required to log into the NCAISS Solution directly to correlate additional STEPP accounts via the steps outlined below.

1. Log into NCAISS, as described in Section 5. From the NCAISS Home Page, select the “Register an Existing STEPP Account,” as shown in Figure 110.

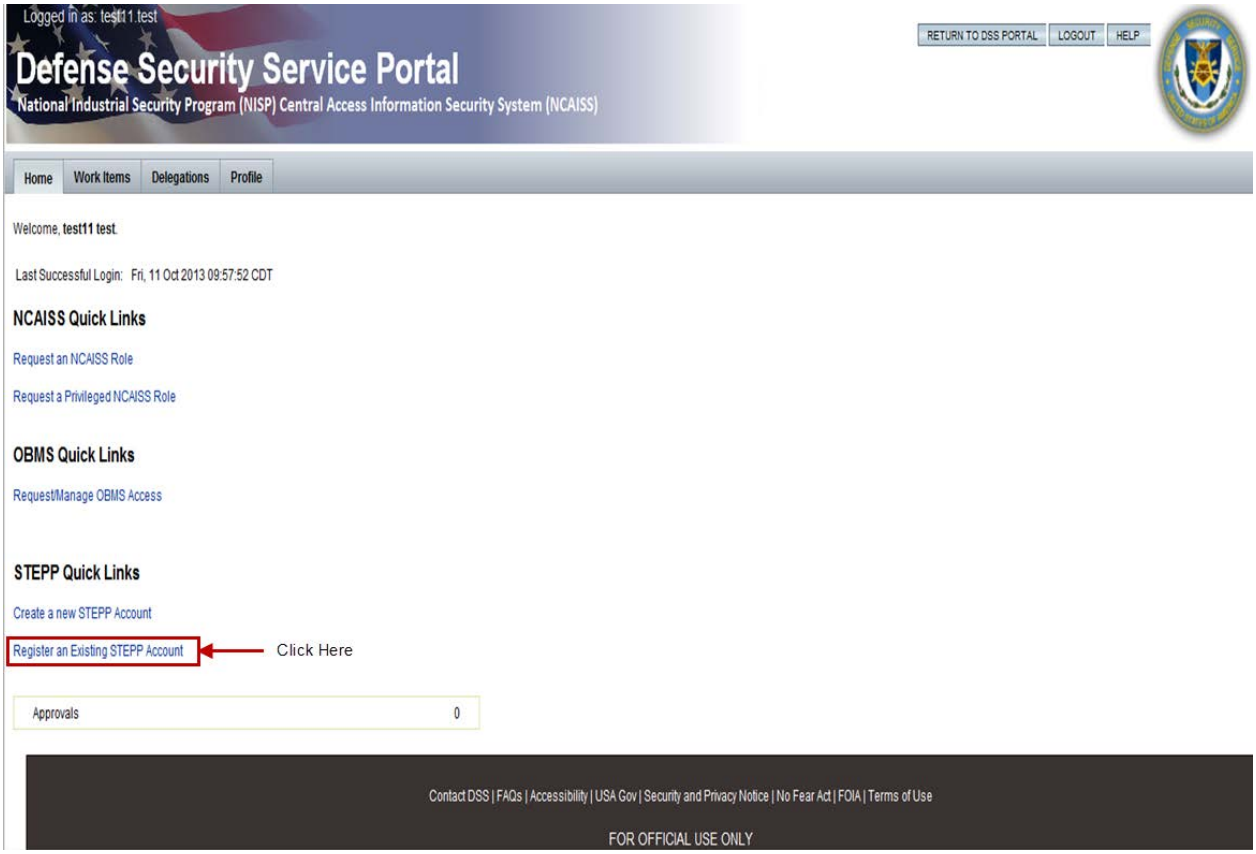


Figure 110: Correlate Additional STEPP Account

2. Enter your STEPP username and password for the account that you wish to correlate, when prompted. Click "Finish" to proceed, as shown in Figure 103. **Note:** If you have forgotten your password you may use the STEPP password reset capability by clicking the link.
3. NCAISS will validate your username and password with STEPP and, if successful, notify you that your account has been correlated with NCAISS, as shown in Figure 111. Click the "Go to STEPP" button to proceed to STEPP.

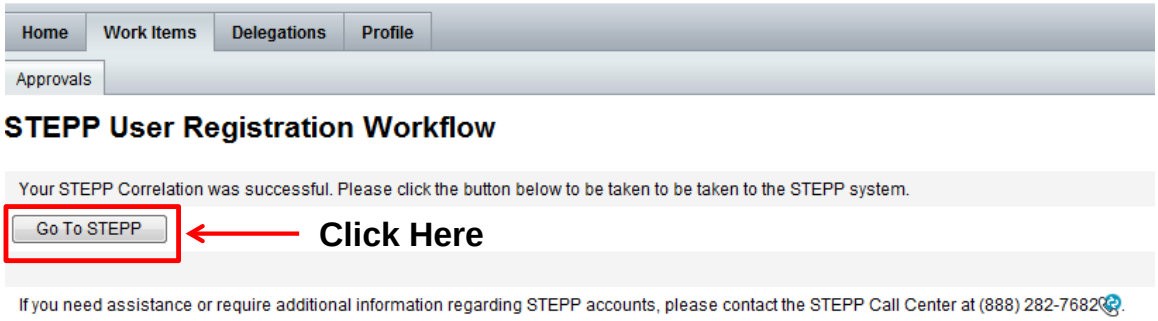


Figure 111: STEPP Account Correlation Successful

4. Once you have correlated multiple STEPP accounts, NCAISS will prompt you to select the account that you wish to use during a given session, prior to directing you to STEPP, as shown in Figure 99. Select the desired account and click "Continue."
5. NCAISS directs you to STEPP. The STEPP user's homepage is displayed, as shown in Figure 100.

14 Glossary

Term	Definition
ADAA	Assistant Designated Approval Authority
Application Sponsor	One or more individuals that have the necessary privileges to Sponsor or reject an individual's application access request. For OBMS, this is the Organization KMP and DSS Call Center for External users and the DSS Supervisor for Internal users.
Attribute	A claim of a named quality or characteristic inherent in or ascribed to someone or something.
Audit Trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure or event in a security relevant transaction from inception to final result.
Authentication	The process of verifying that a claimed identity is genuine and based on valid credentials.
Authorization	The process of granting or denying specific requests for obtaining and using information processing services or data and to enter specific physical facilities.
Certificate	A data object containing a subject identified, a public key, and other information that is digitally signed by a Certification authority. Certificates convey trust in the relationship of the subject identifier to the public key.
Certificate Revocation List (CRL)	A signed artifact composed of all revoked or otherwise suspended certificated issues from a CA that can be used to verify the current status of a PKI certificate.
Certificate Status Servers	The counterpart to the Certification Authority that passes revocation and expiration status to relying parties in real time.
Certification Authority	An authority trusted by one or more users to use and manage X.50- public key certificate and CRLs.
Common Access Card (CAC)	A physical artifact (e.g. identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g. photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to an entity.
DD/DAA	Deputy Director of Designated Approval Authorities
Defense Security Service (DSS)	DSS is an agency within the Department of Defense. It provides the military services, Defense Agencies, 23 federal agencies, and approximately 13,000 cleared contractor facilities with security support services.
DSS Call Center	Responsible for sponsoring External OBMS access requests and verifying that the External Requestor's Organization's KMP matches the KMP on record in JPAS for a specified CAGE Code.
Department of Defense (DoD)	The U.S. Federal Government department charged with coordinating and supervising all agencies and functions of the government relating directly to national security and the United States armed forces.
DSS NCAISS	A gateway that provides access to much of DSS's information and applications in one place.

External Certification Authority (ECA)	An organization that has been approved to issue DoD-approved PKI certificates to industry partners and other external entities and organizations. ECA certificates provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD Information Systems.
FOC	Field Office Chief
Identity	The set of an attribute values (i.e. characteristics) by which entity is recognizable and that, within the scope an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.
National Industrial Security Program (NISP) Central Access Information Security System (NCAISS) Solution	A technology solution that has been developed to provide DSS applications with Public Key Infrastructure (PKI)-based authentication services using DoD-issued CAC or DoD-approved ECA certificates.
Industrial Security Facilities Database (ISFD)	Provides users with a nationwide perspective on National Industrial Security Program related facilities, as well as facilities under DSS oversight in the DoD conventional Arms, Ammunition, and Explosives (AA&E) program. ISFD data will also provide source data for the DoD Joint Personnel Adjudicative System (JPAS) and the Facility Verification Request (FVR) application.
Information System	A discrete set of information resources organized for the collecting, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
ISR	Industrial Security Representative
ISP	Information System Professional
ISSP	Information System Security Professional
Java Database Connectivity (JDBC)	An application programming interface (API) for the Java programming language that defines how a client may access a database. It provides methods for querying and updating data in a database.
Organization KMP	Key Management Personnel for an industry organization; responsible for managing one or more CAGE Codes.
Lightweight Directory Access Protocol (LDAP)	An application protocol for accessing and maintaining distributed directory information services over network.
ODAA Business Management System (OBMS)	A DSS application that serves as a business operations support tool for the mission-focused operations of the Office of the Designated Approval Authority (ODAA).
Office of Designated Approving Authority (ODAA)	DSS organization that offers certification, accreditation, oversight, and management of cleared contractor's security systems.
OGC	Office of General Council
Password	An attribute linked to a user identity that provides some level of confidence in the identity of the user.

Private Key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.
Provisioning	Creating user access accounts and assigning privileges or entitlements within the scope of a defined process or interaction; provide users with access right to applications and other resources that may be available in an environment, may include the creation, modification, suspension, or restoration of a defined set of privileges.
Public Key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.
Public Key Infrastructure (PKI)	The framework and services that provide for generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purposed of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.
RDAA	Regional Designated Approval Authority
Representational State Transfer (REST)	A style of software architecture for distributed hypermedia systems. REST provides a definition for services that are stateless and also follow the client-server model.
Security Training, Education and Professionalization Portal (STEPP)	Serves as a DoD platform for delivering education, training, and professional development to members of the Federal Government and industry as part of the National Industrial Security Program.
Session Management	Allows for the sharing of data among multiple relying parties as part of an authenticated user session; includes protocol translation services for access to systems needing different authentication protocols; manages automatic time-outs and requests for re-authentication.
Single Sign-On	A mechanism by which a single act of user authentication and log on enables access to multiple independent resources.
Sun Identity Manager	Manages user account and credential information and can provide workflow management/automation support for user registration and account modification processes.
Sun OpenSSO	Provides web-based DSS applications with CAC/PKI-based authentication and can enable single sign-on (SSO) to integrated applications. User data is accessed through a single load balancer deployed in front of two instances of Sun Java System Directory Server.
System Access Request (SAR)	A document that is used to request access to one or more DSS information systems and becomes the focal point for a system's processing of that action.
User	Any user of the NCAISS Solution, or its integrated applications (e.g., OBMS, STEPP, ISFD, ODAA Content Manager, etc.), regardless of role.
User Management Coordinator	A role within the OBMS application that is responsible for managing OBMS user accounts across the user management lifecycle.
Workflow	A sequence of connected steps aimed at achieving a stated objective. Within the NCAISS Solution, workflow refers to those processes most commonly associated with user account creation, modification, management, and suspension.