Defense Information System for Security Joint Verification System

JVS FOR INDUSTRY

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Agenda

- Brief DISS Overview
- Orientation to Higher Echelon Users Roles and Permissions
- Orientation to End-user functions
- Q&A

Learning Objectives

- Users will be able to describe the general framework of DISS
- Users will be able to identify and navigate the various functions of DISS JVS
- Users will be able to identify and explain the roles and responsibilities of higher level and end users
- Users will be able to define and compare various user relationships and functions within DISS JVS

DISS Components

System of Record for of all DoD employees, military personnel, civilians and DoD contractors in support of:

- Personnel Security
- Suitability
- Credential Management

Secure communications between Adjudicators, Security Officers, and Component Adjudicators.

There are three components of DISS

- Joint Verification System (JVS)
- Consolidated Adjudication Tracking System (CATS)
- Appeals System

Industry uses the Joint Verification System side of DISS

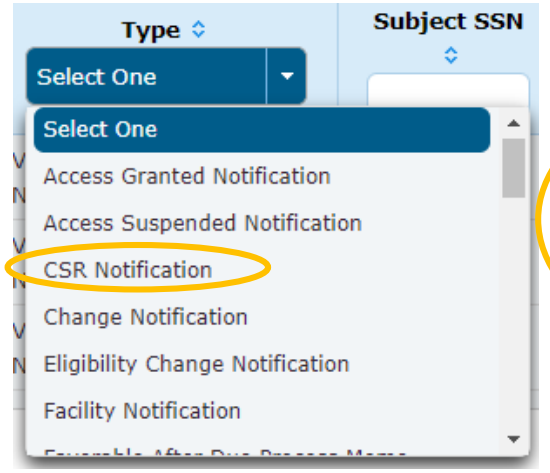
What is DISS

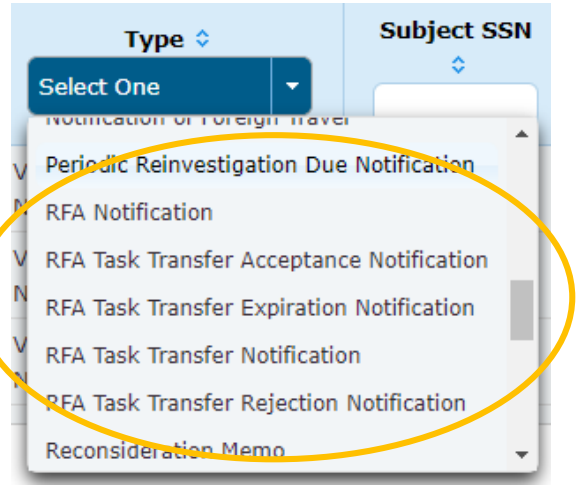
- A key component of the DoD's strategy to modernize personnel vetting and improve mission readiness

- An enterprise-wide system that offers accelerated workflows, electronic adjudications, and secure document exchange

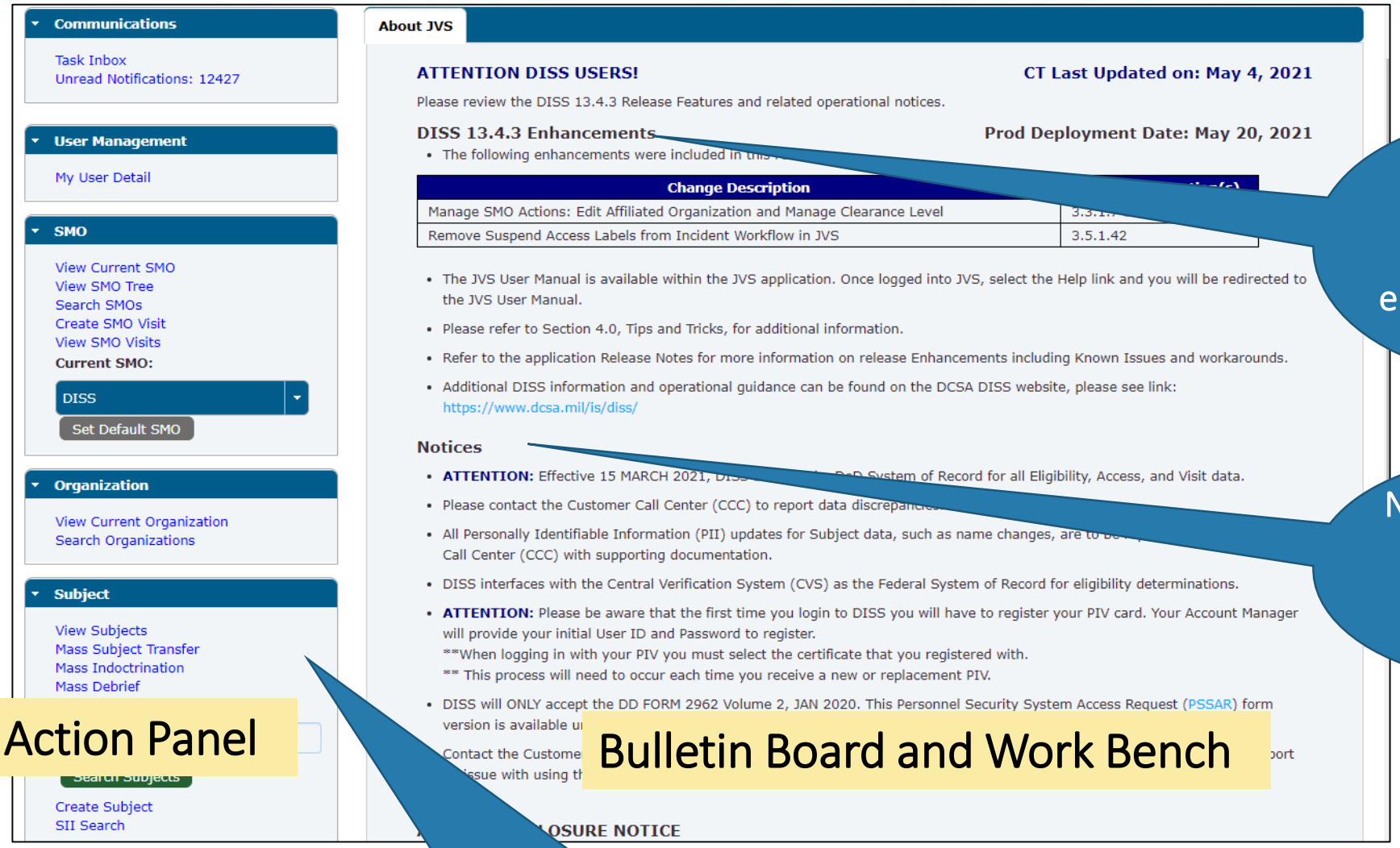
Key features

- Customer Service Requests (CSRs)
- Request for Action (RFA)





JVS Home Page Orientation



Notifies users of newly implemented enhancements to JVS

Notices for users of important information in support of JVS

Action Panel

Bulletin Board and Work Bench

The Action Side brings up work to be done on the work bench

HIGHER ECHELON USERS

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Who We Are, What are Our Roles

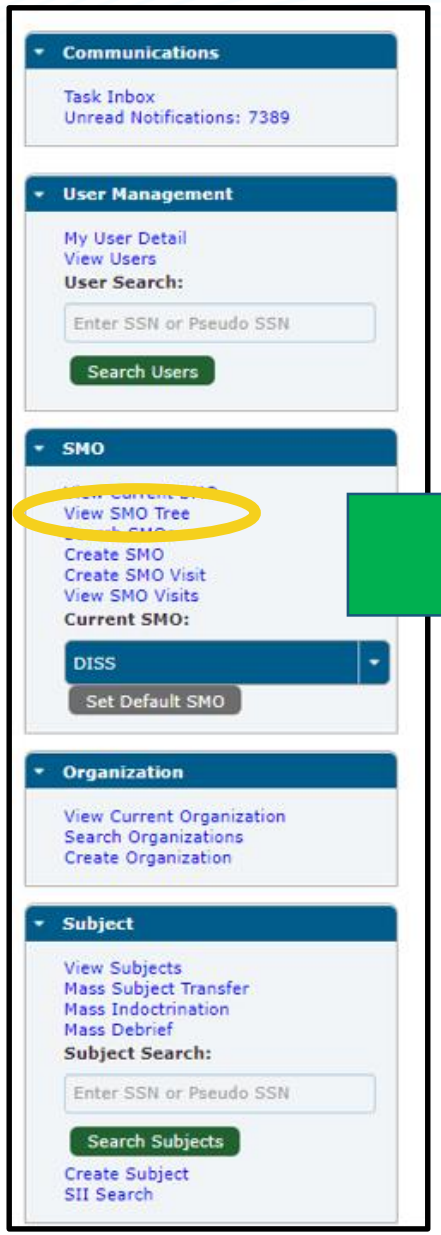
Hierarchy Manager:

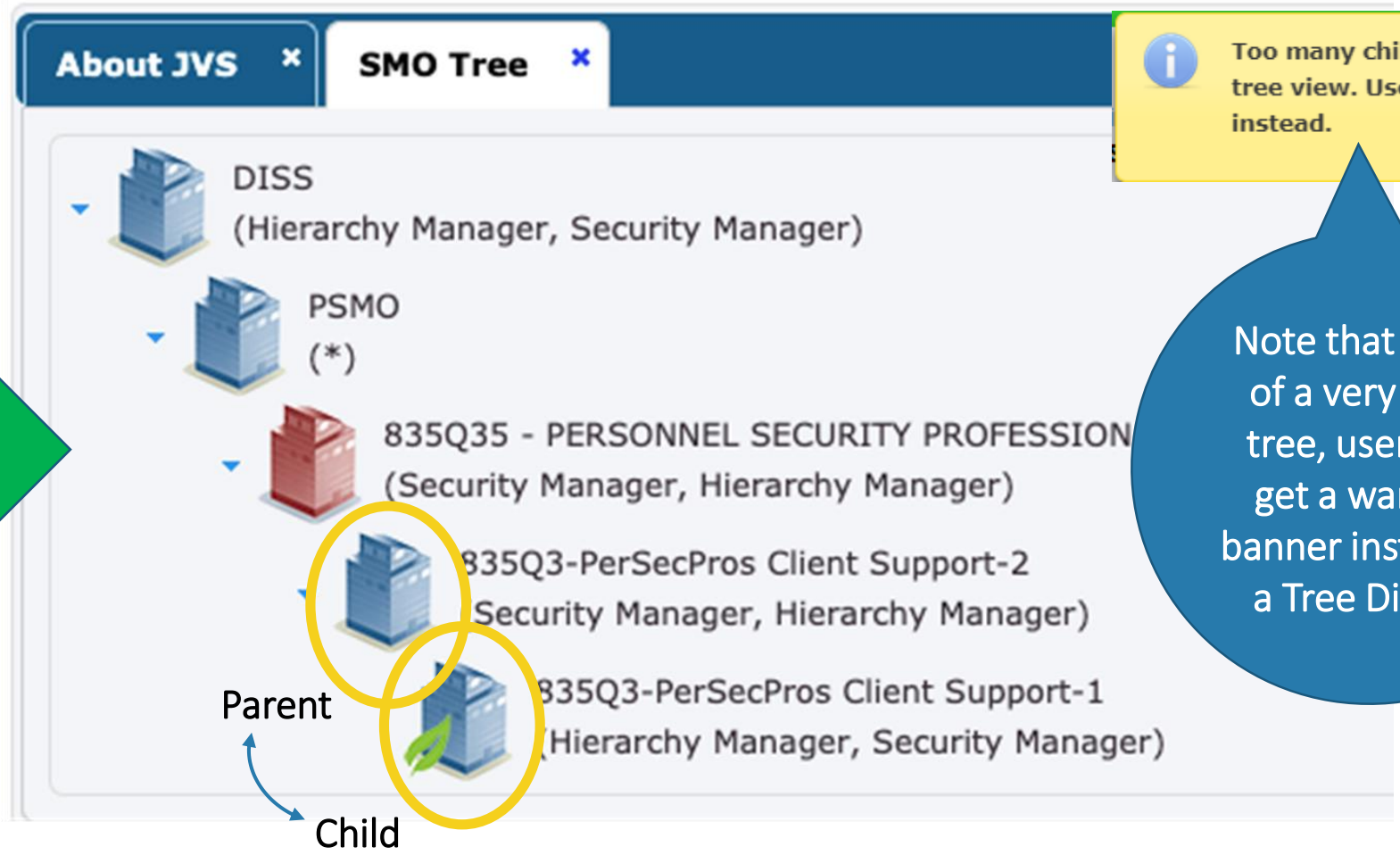
- Head of the Security Management Office (SMO)
- Create SMO Tree
- In addition to all privileges of an Account Manager

Account Manager:

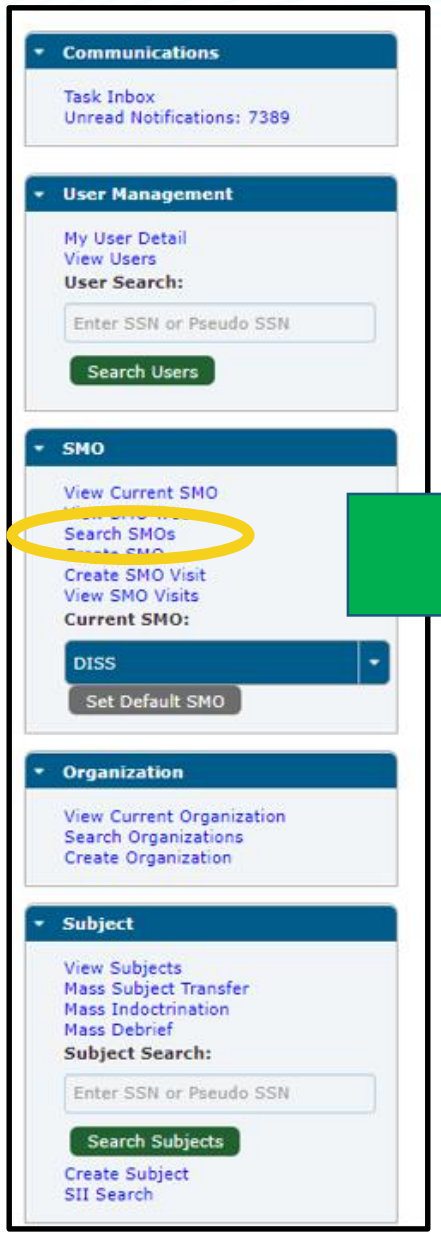
- Manages user provisioning within organization
- Performs tasks such as creating and maintaining user profiles, roles, and permissions
- May work in subordinate “child” SMOs

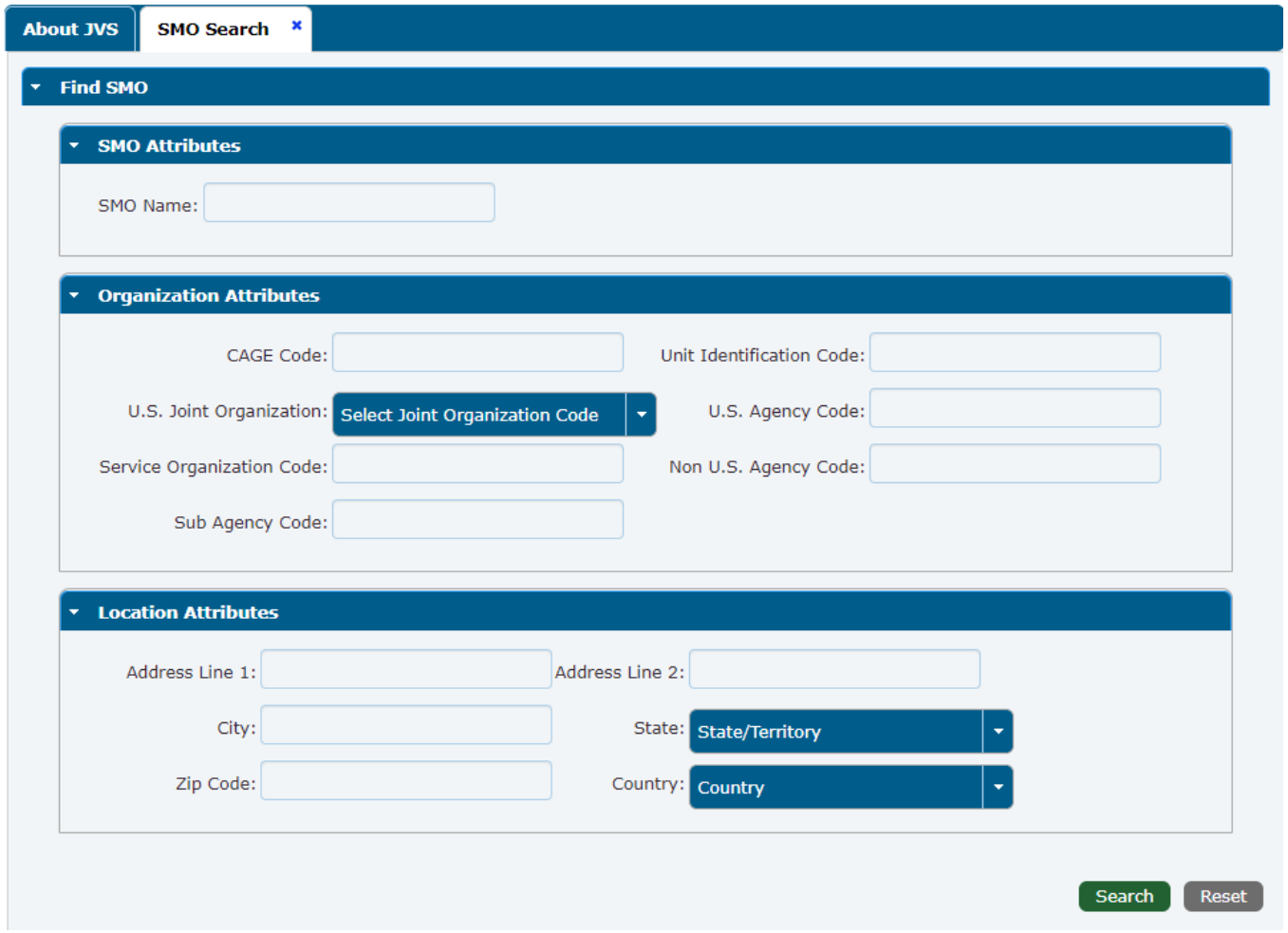
View the SMO Tree



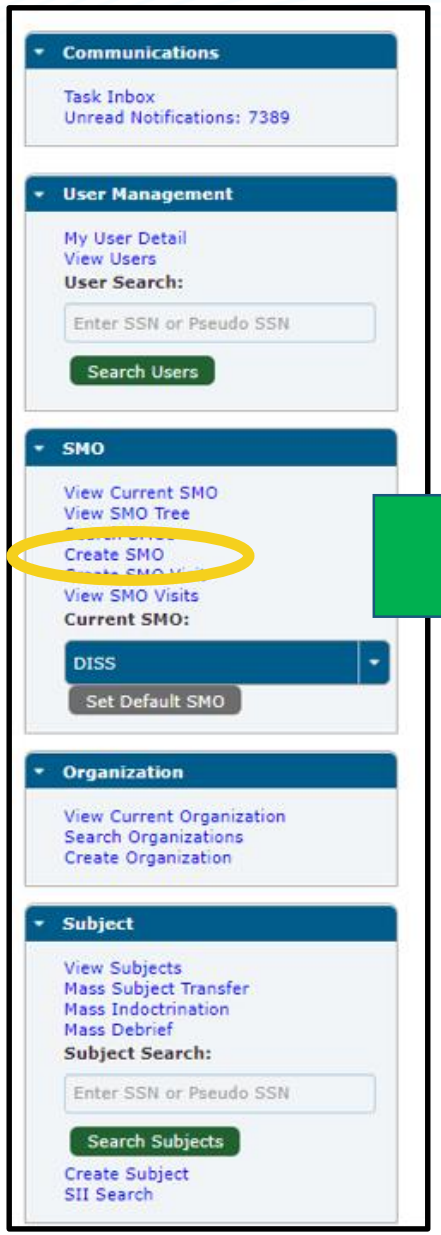


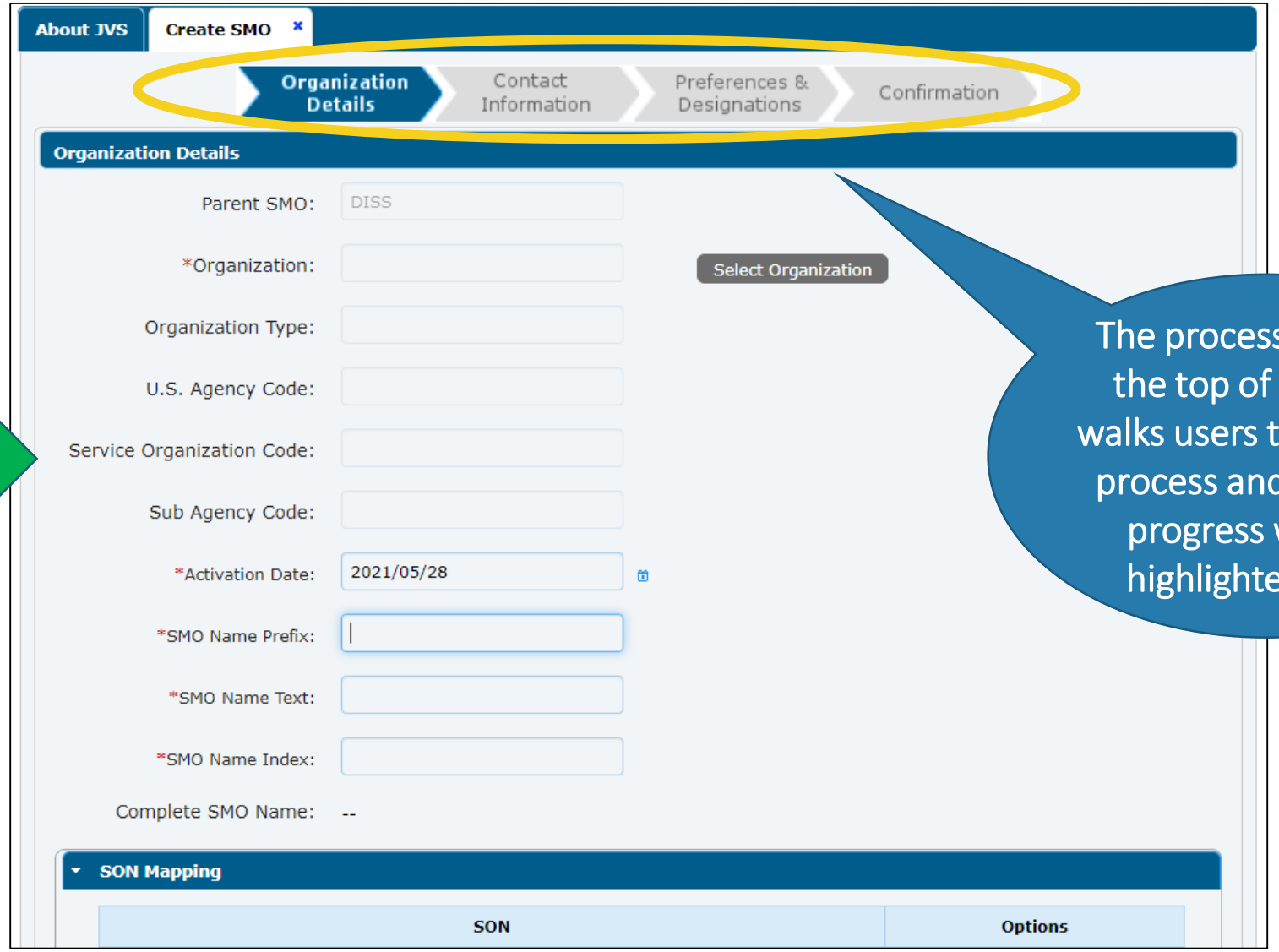
Search SMOs


Communications
Task Inbox
Unread Notifications: 7389
User Management
My User Detail
View Users
User Search:
Enter SSN or Pseudo SSN
Search Users
SMO
View Current SMO
Search SMOs
Create SMO Visit
View SMO Visits
Current SMO:
DISS
Set Default SMO
Organization
View Current Organization
Search Organizations
Create Organization
Subject
View Subjects
Mass Subject Transfer
Mass Indoctrination
Mass Debrief
Subject Search:
Enter SSN or Pseudo SSN
Search Subjects
Create Subject
SII Search


About JVS
SMO Search
Find SMO
SMO Attributes
SMO Name:
Organization Attributes
CAGE Code:
Unit Identification Code:
U.S. Joint Organization:
Select Joint Organization Code
U.S. Agency Code:
Service Organization Code:
Non U.S. Agency Code:
Sub Agency Code:
Location Attributes
Address Line 1:
Address Line 2:
City:
State:
State/Territory
Zip Code:
Country:
Country
Search
Reset

Create SMOs





The process model at the top of the page walks users through the process and indicates progress with the highlighted arrow

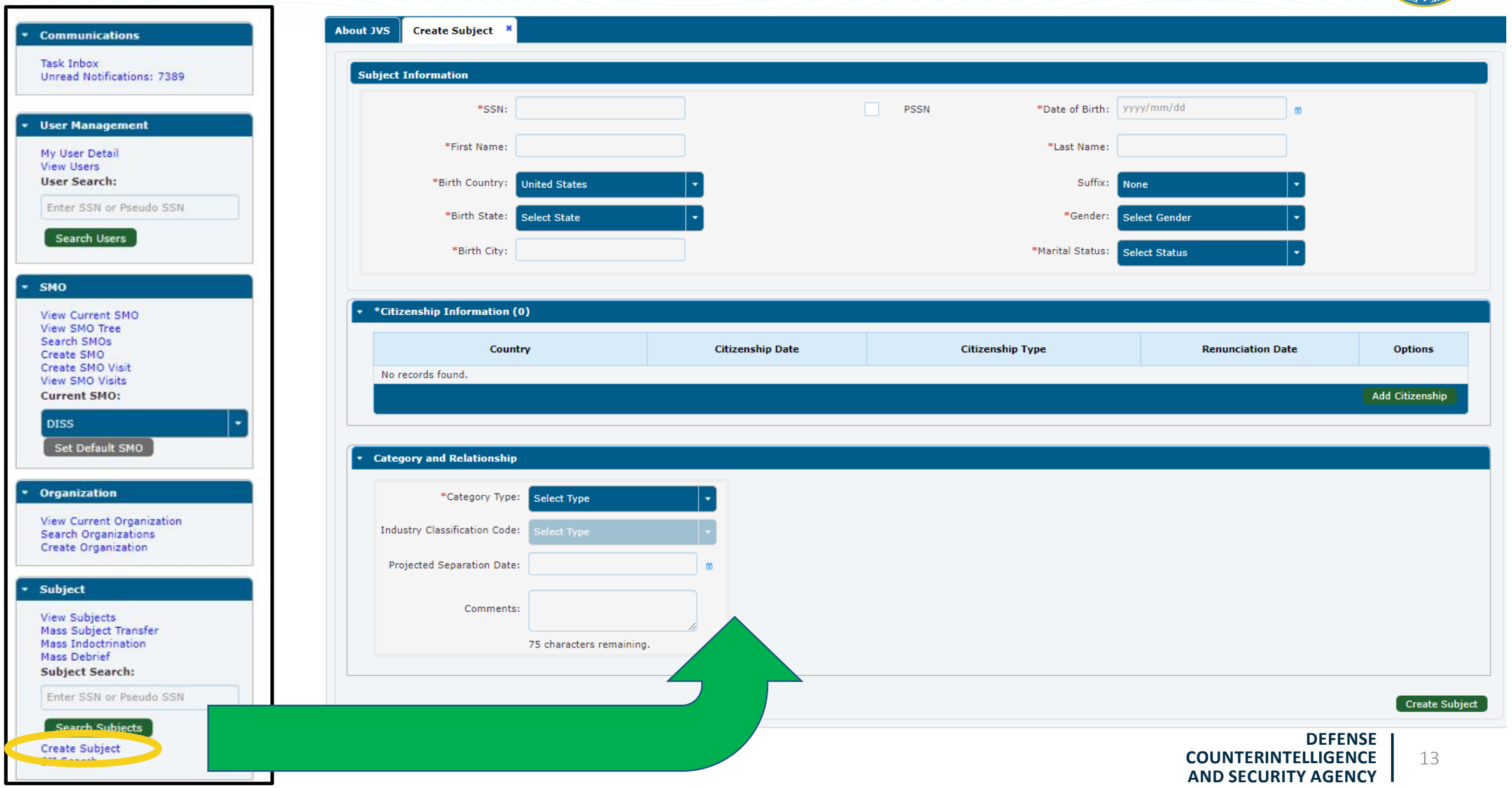
Move SMOs (Hierarchy Change Request)

- If there are SMOs not within your hierarchy and you are not provisioned for the SMO, you will need to submit a Hierarchy Change Request (HCR).

	HIERARCHY CHANGE (Parent-Child)	
	SMO CHILD TO BE MOVED	NEW PARENT SMO
**	835Q3-PerSecPros Client Support 1	835Q3 - PerSecPros Client Support-2

- Send the HCR to dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil.

Create Subject

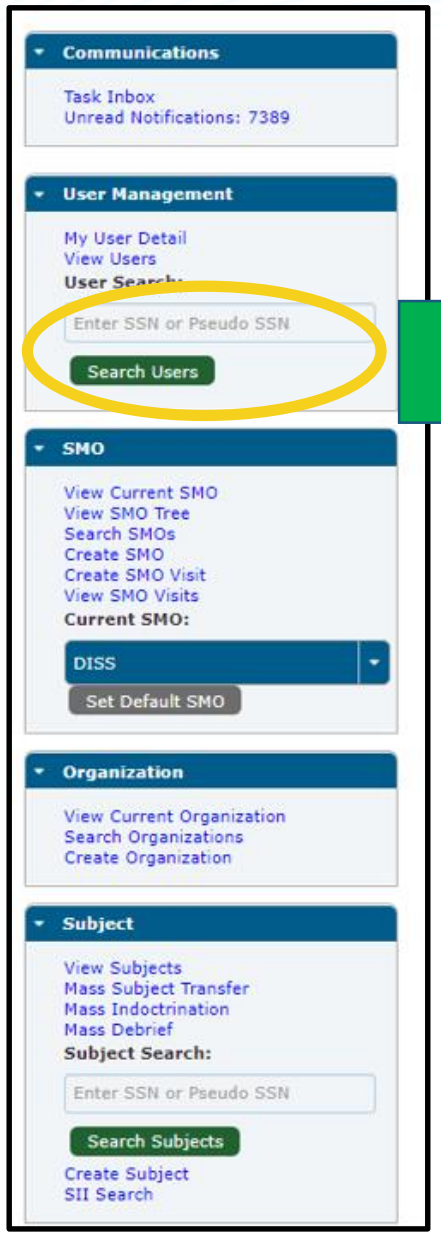


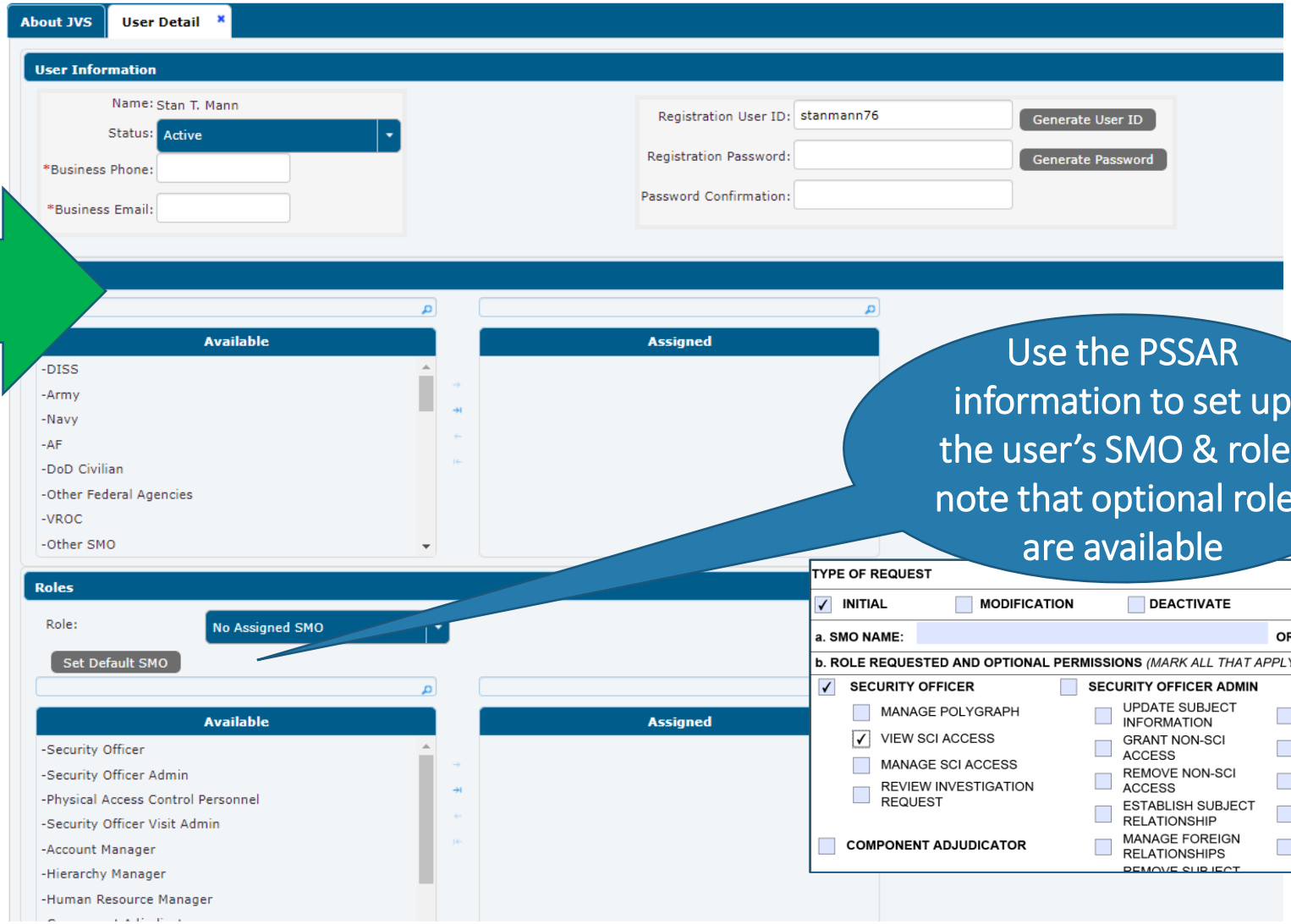
Create User—Program Security System Access Request (PSSAR)

- Use the DCSA DD FORM 2962 and complete in its entirety (**not** P&R form)
- Industry sends PSSAR to dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil

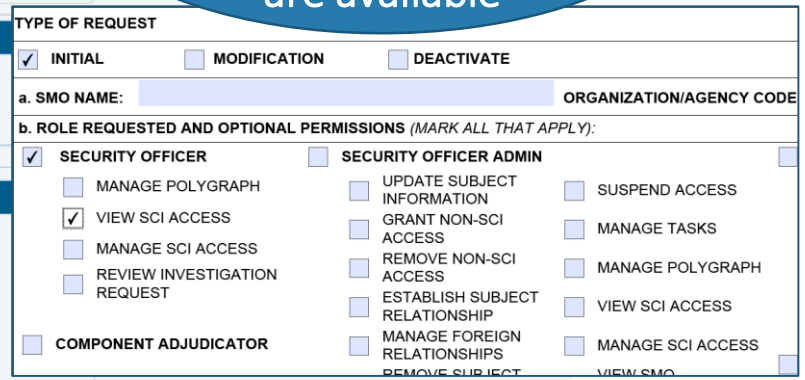
Note: PSSAR FAQs are at https://www.dcsa.mil/is/diss/dissresources/

Create User





Use the PSSAR information to set up the user's SMO & roles note that optional roles are available



USER FUNCTIONS

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

User Roles and Permissions

User Roles

- Security Managers
- Security Officers
- Security Officer Administrator
- Security Officer Visit Administrator

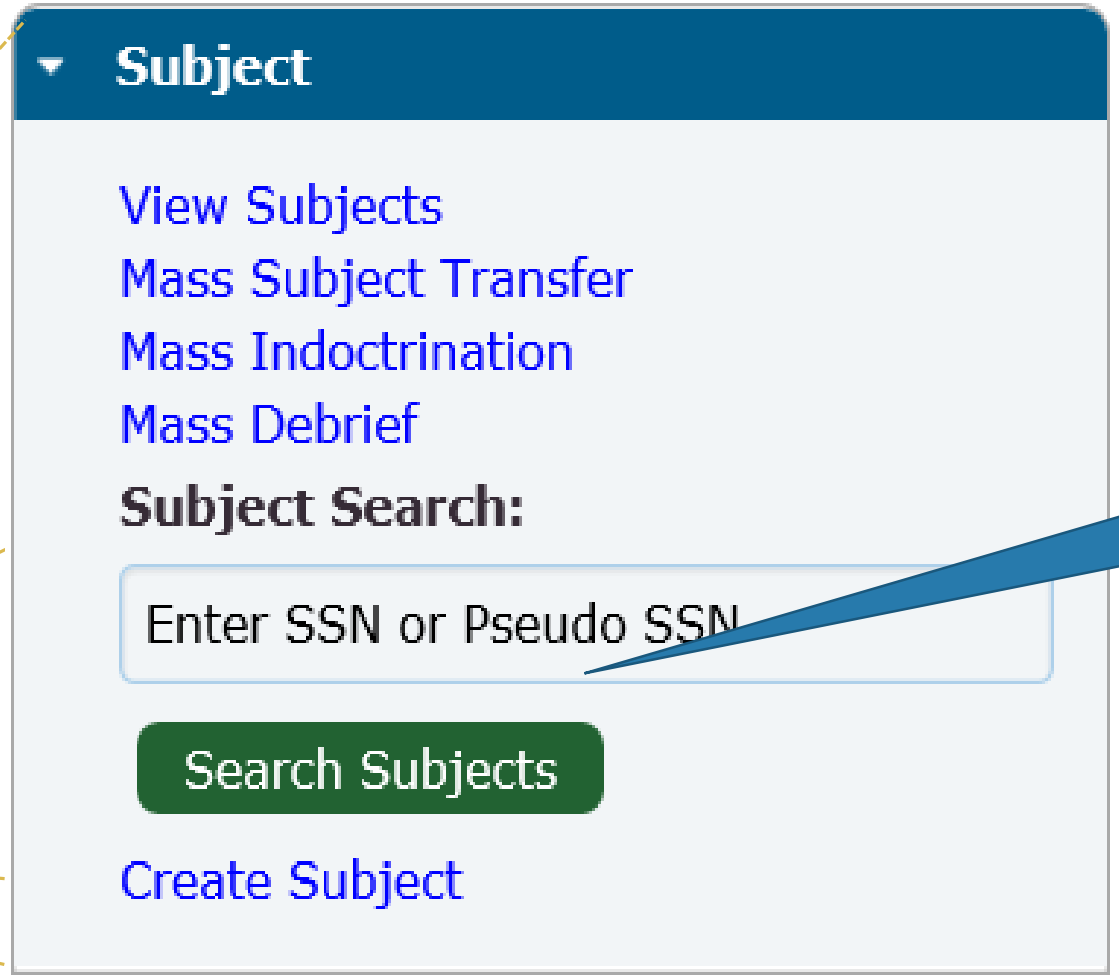
User Permissions

- Subject Management
- NDA Submission Process
- Access Management
- Visit Requests

SUBJECT MANAGEMENT

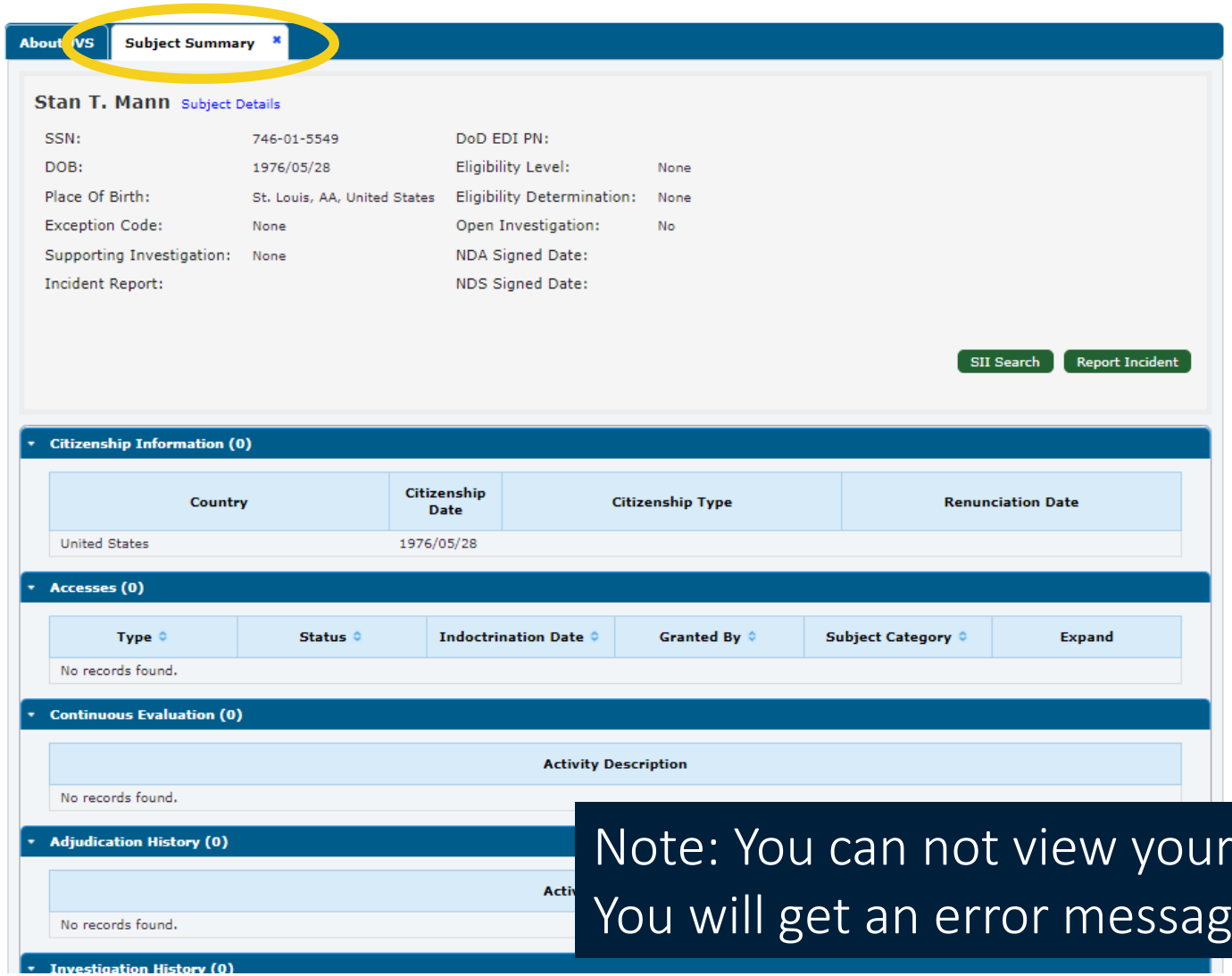
DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Search Subject



User enters either an SSN or PSSN in the search box and Clicks "Search Subjects"

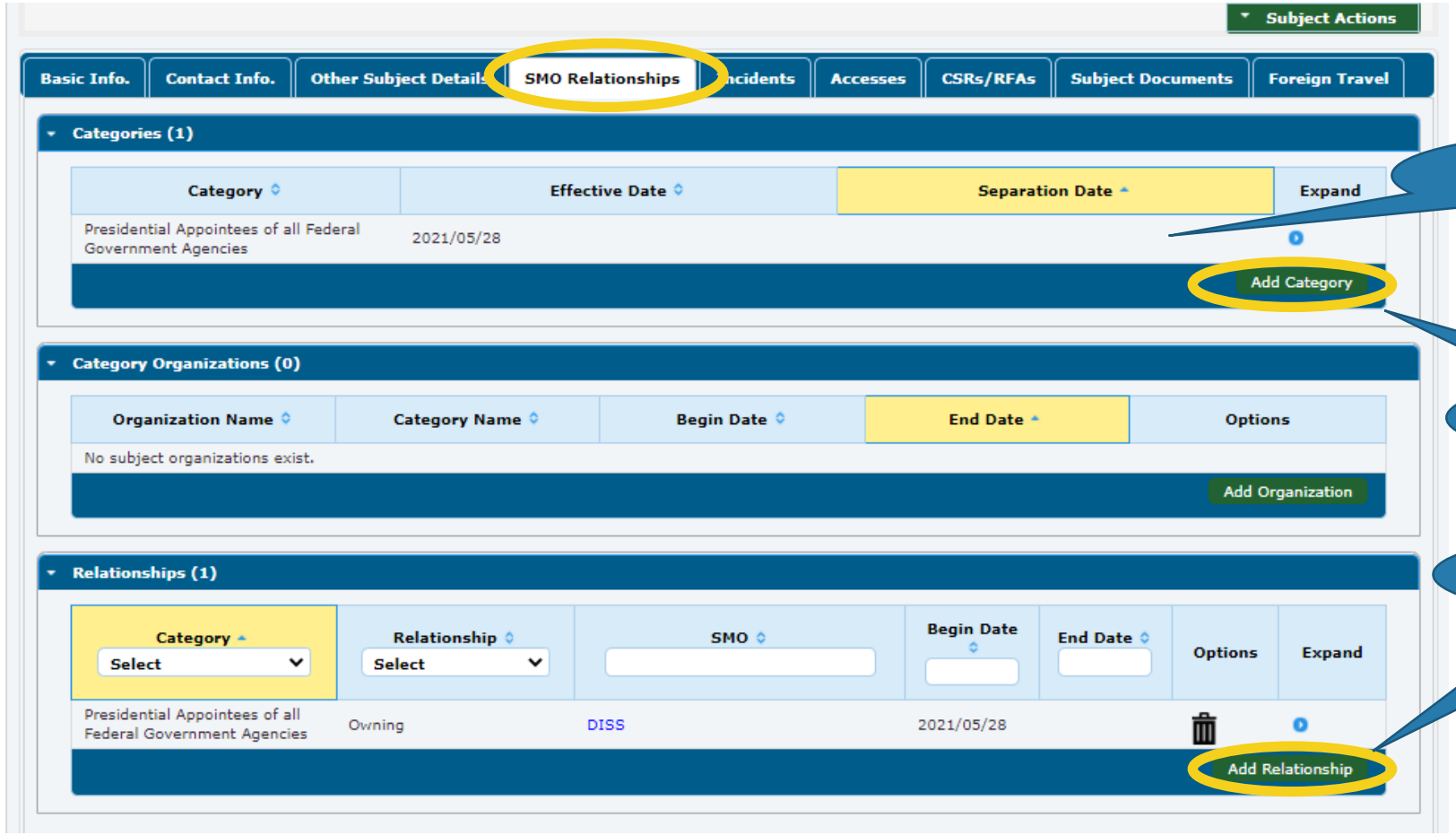
Subject Summary



Note: You can not view your own record. You will get an error message.

Subject Details

Subject Details—Example SMO Relationships



If no SMO details…

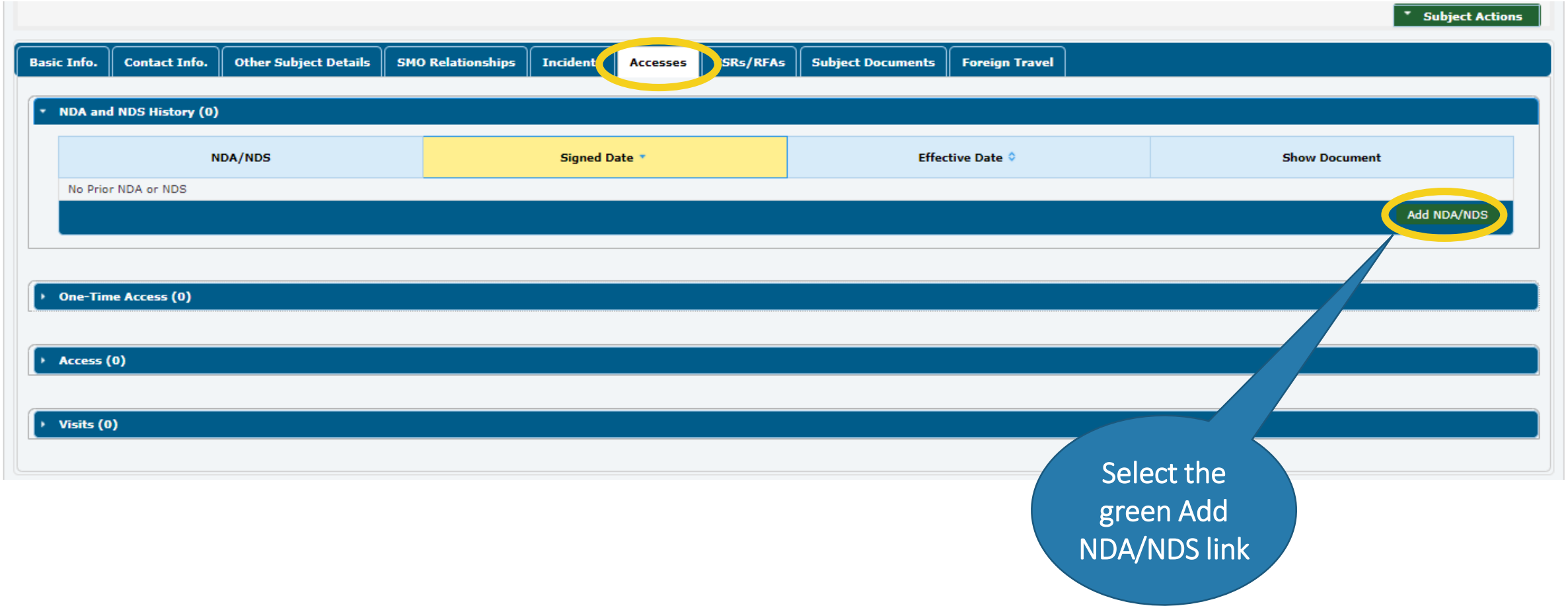
Add a category…

And a relationship

NDA SUBMISSION PROCESS

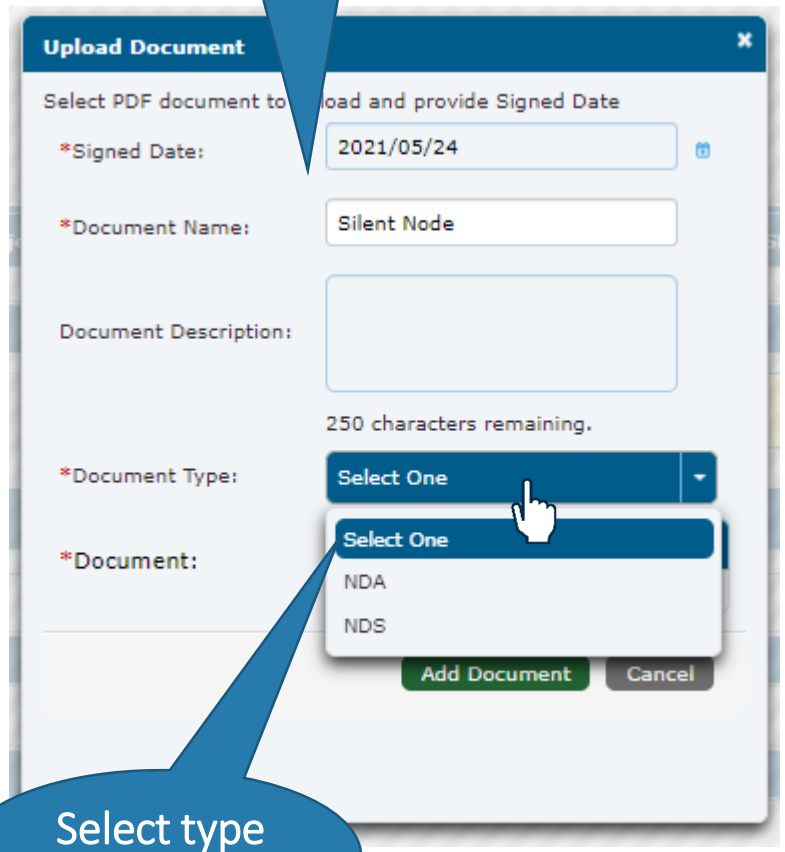
DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Subject Details—Accesses > Add NDA

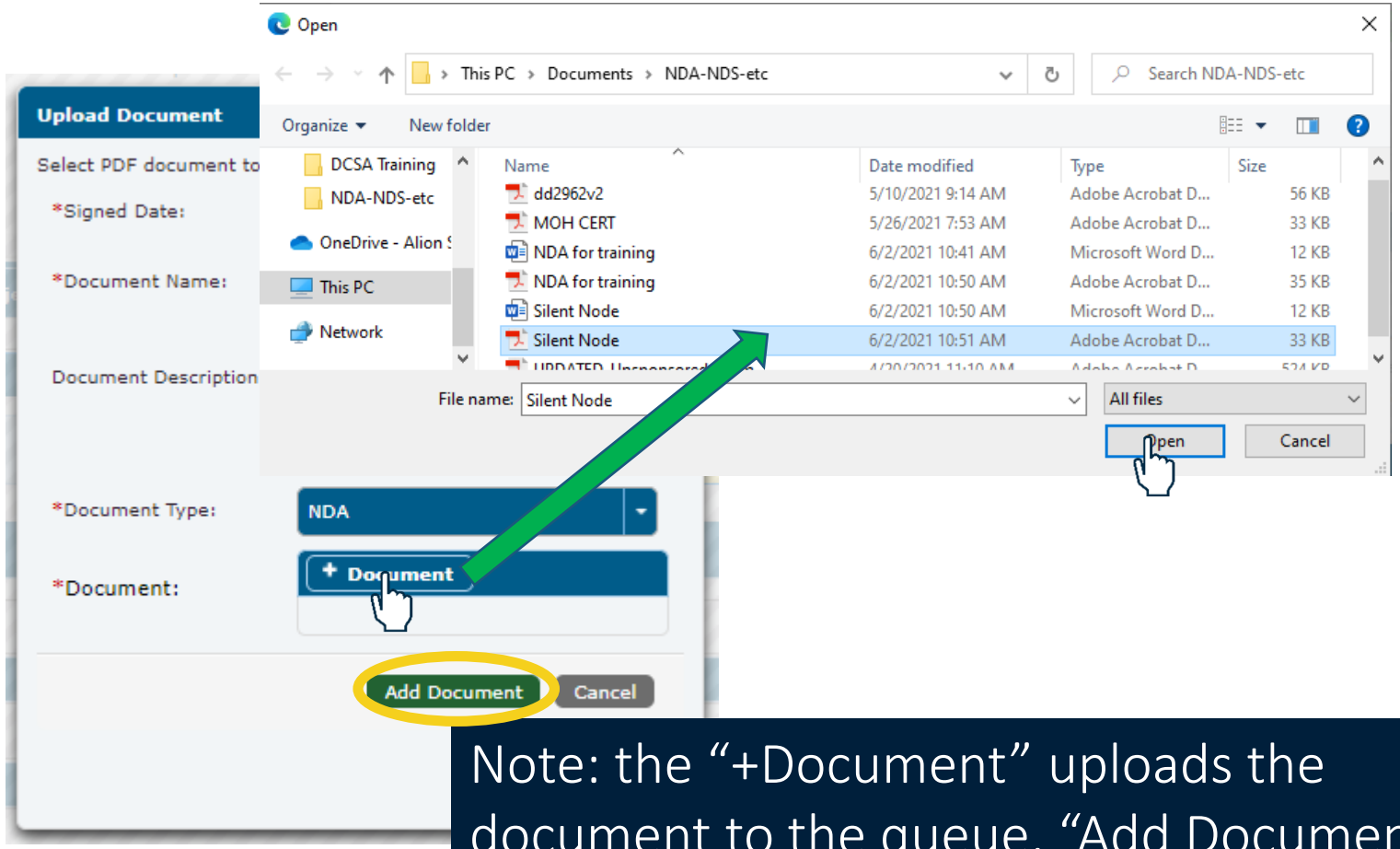


Add NDA/NDS—Upload Document

Enter Date and Doc name



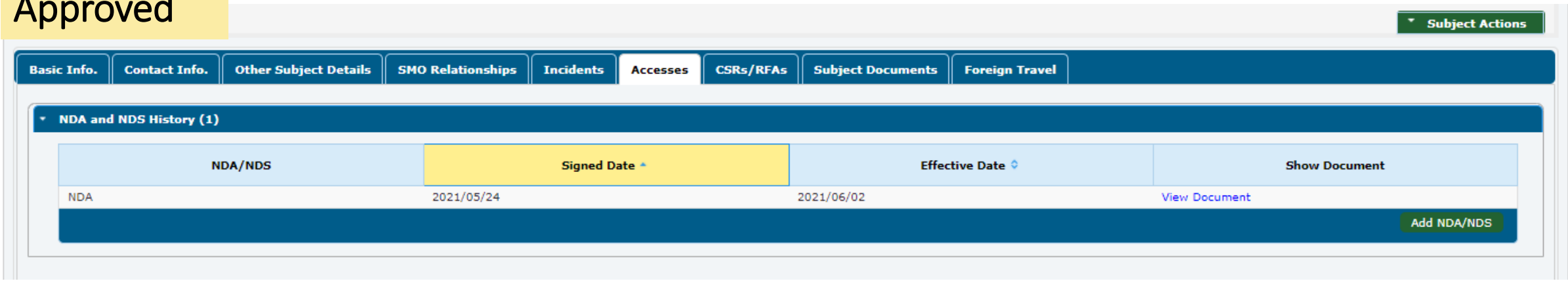
Select type from pulldown



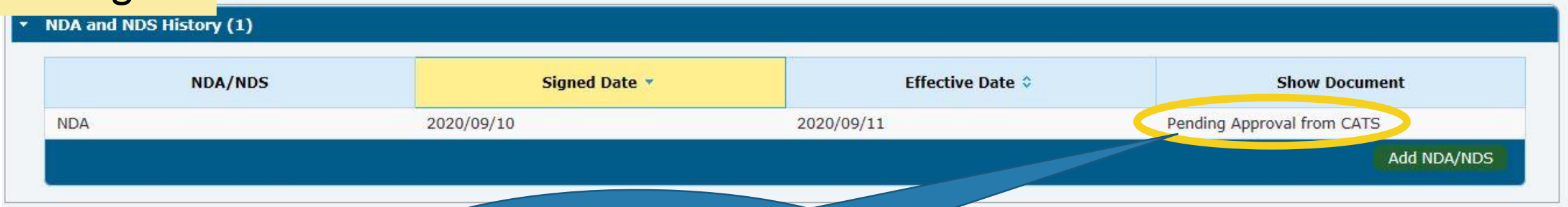
Note: the "+Document" uploads the document to the queue, "Add Document" uploads that document to JVS

NDA/NDS History

Approved

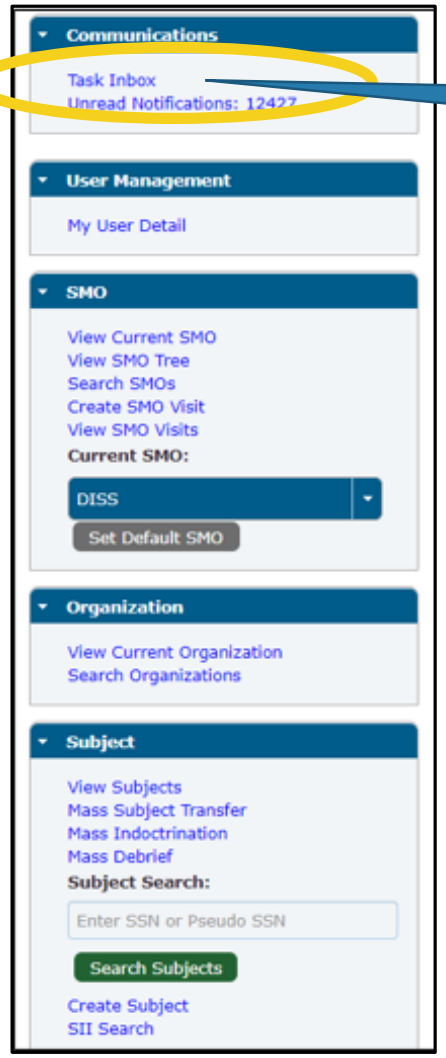


Pending

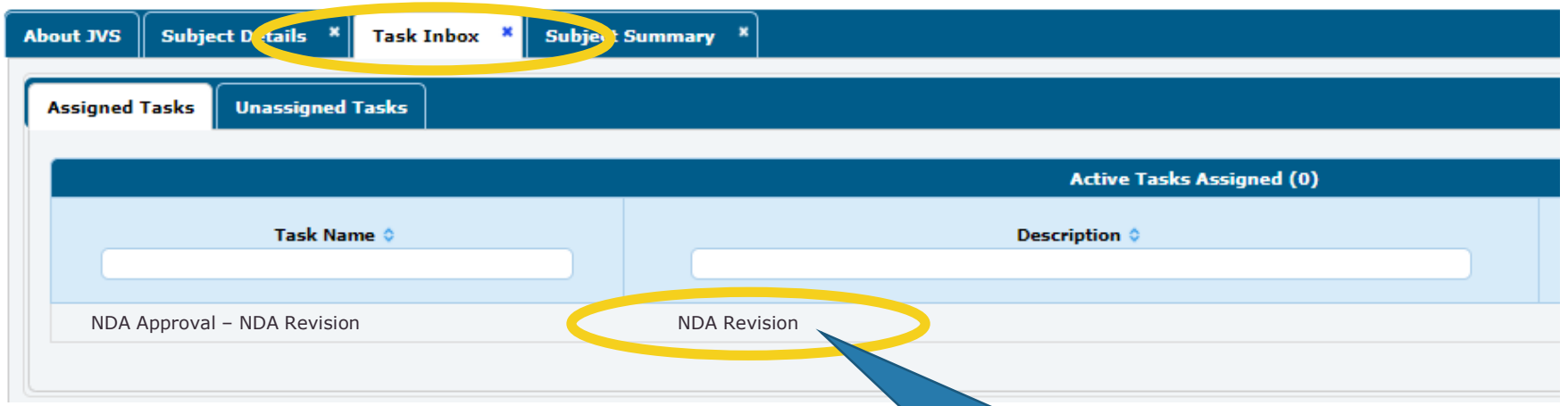


When submitted, JVS automatically sends an NDA/NDS Review task to CATS

Rejected NDA



If rejected, a message will appear in the Task Inbox

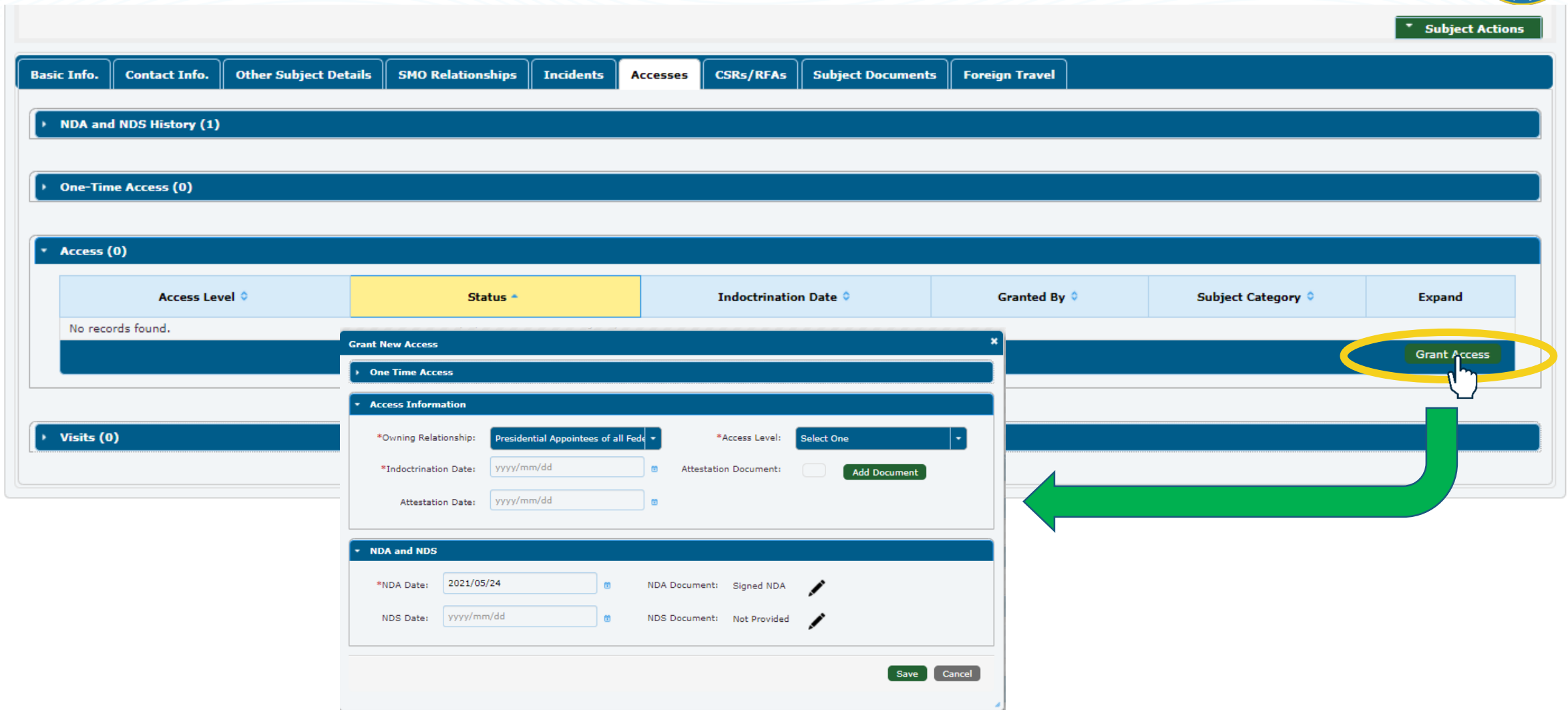


When rejected, the Security Officer has a task to revise the NDA before resubmitting

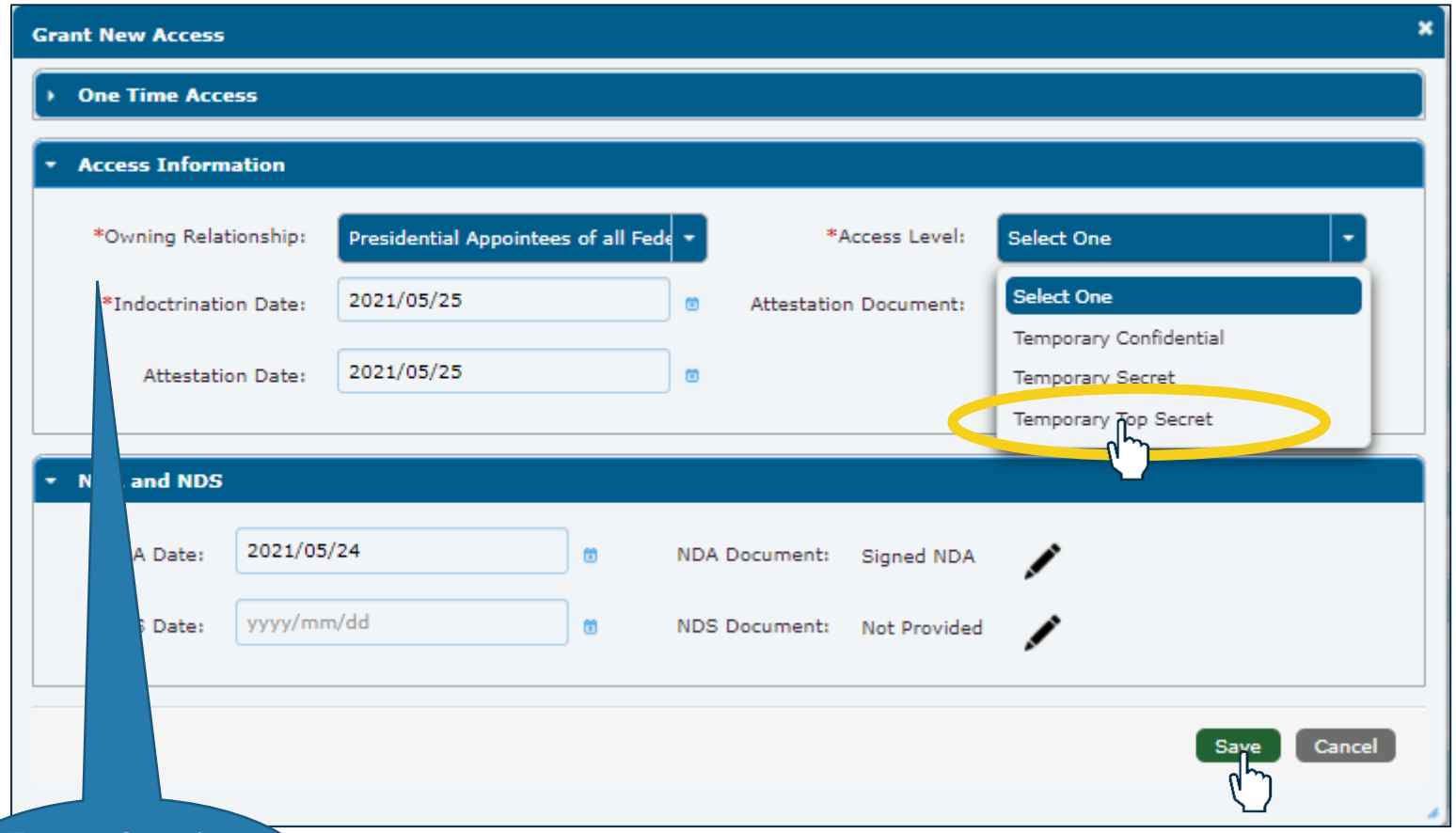
ACCESS MANAGEMENT

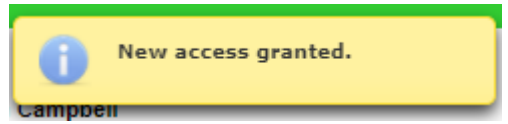
DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Granting Access



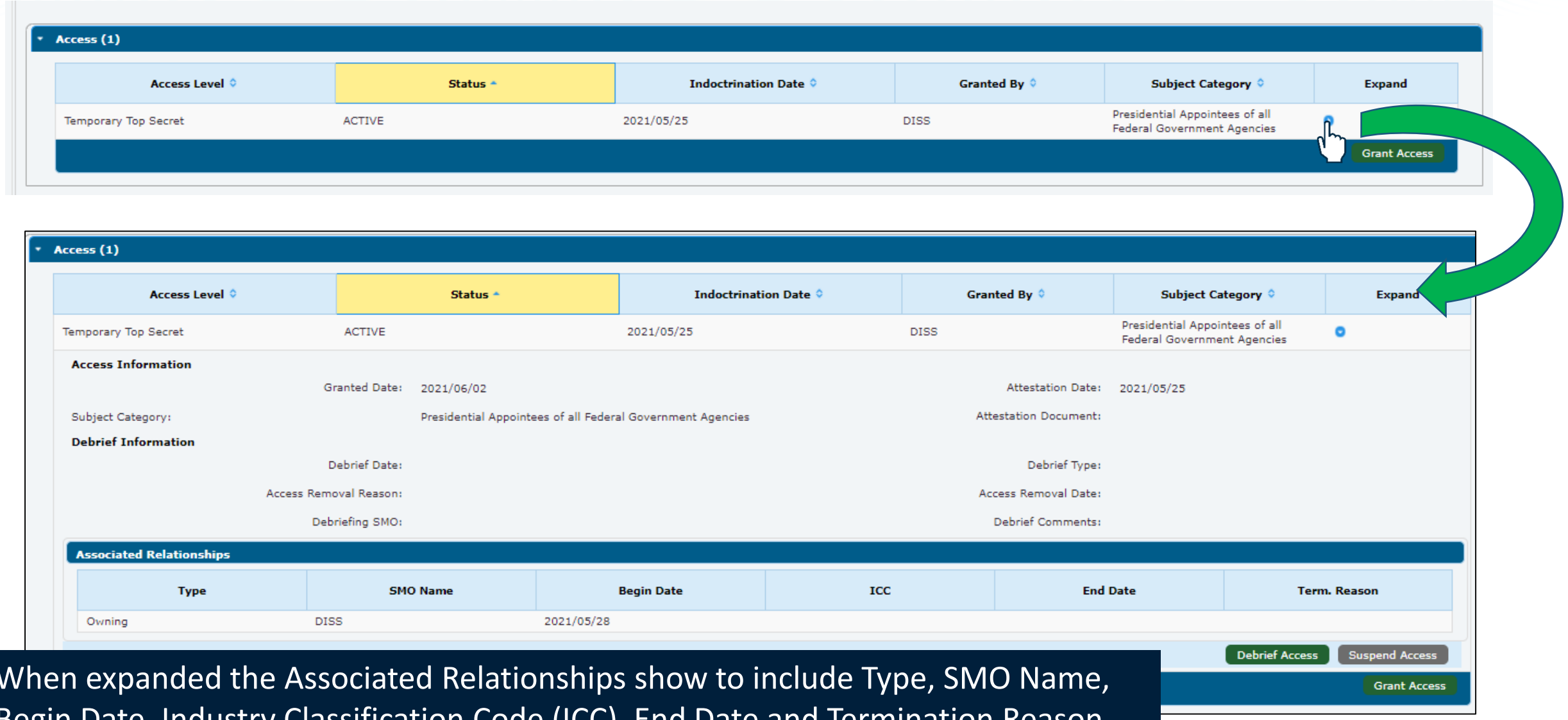
Grant New Access





Enter Owning Relationship and Date

Access Status

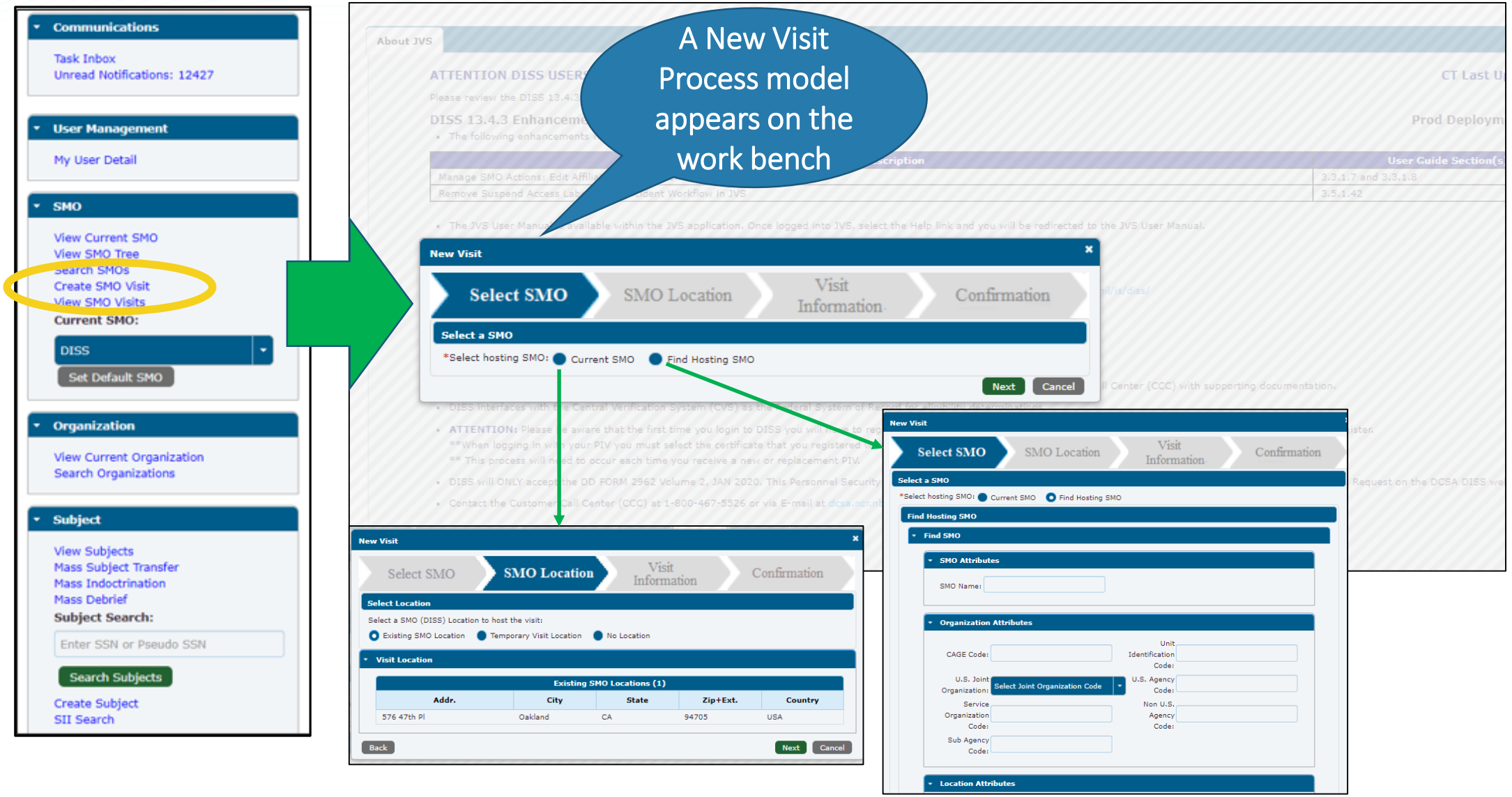


When expanded the Associated Relationships show to include Type, SMO Name, Begin Date, Industry Classification Code (ICC), End Date and Termination Reason.

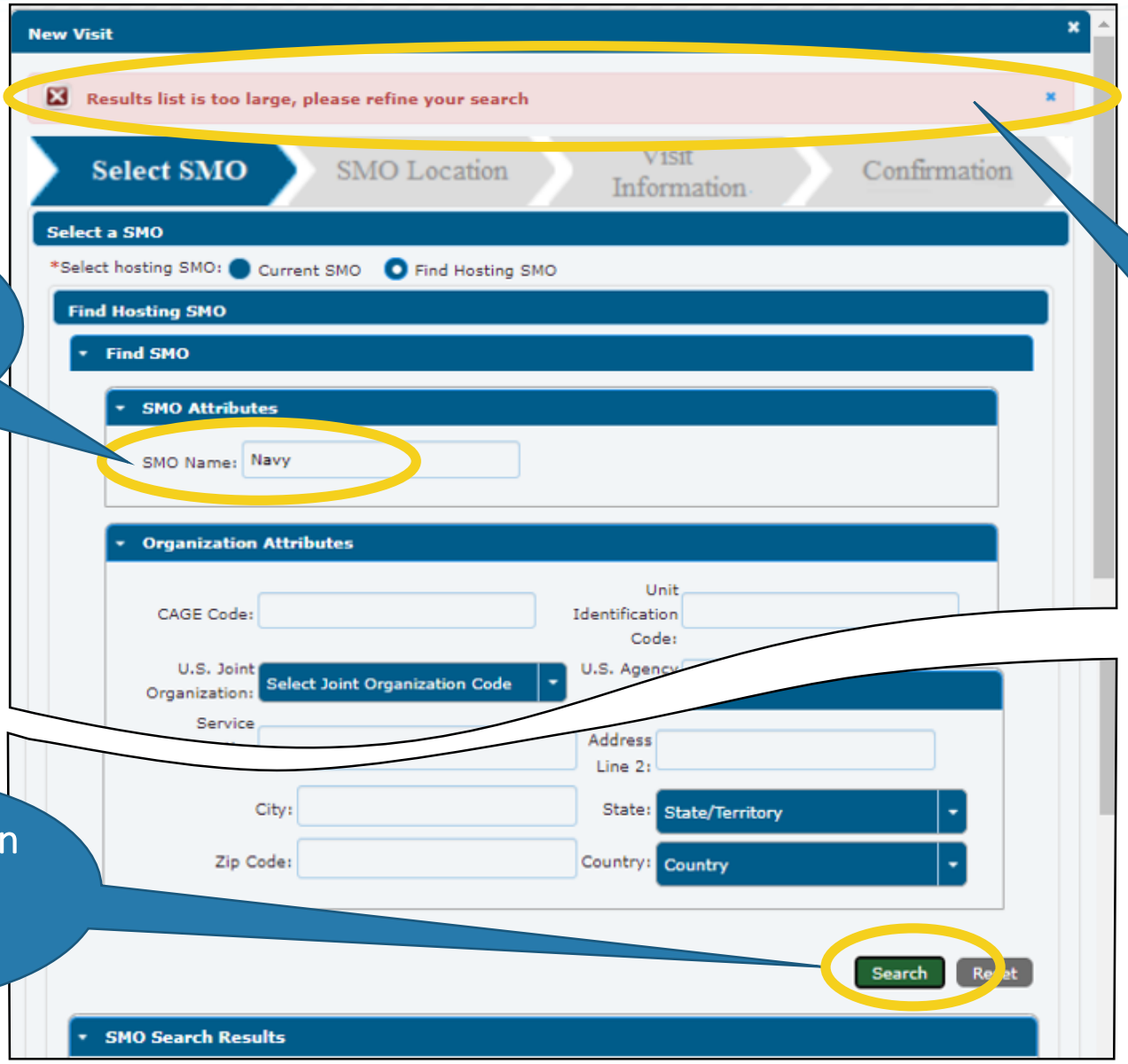
VISIT REQUESTS

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Create SMO Visit



Find & Select SMO

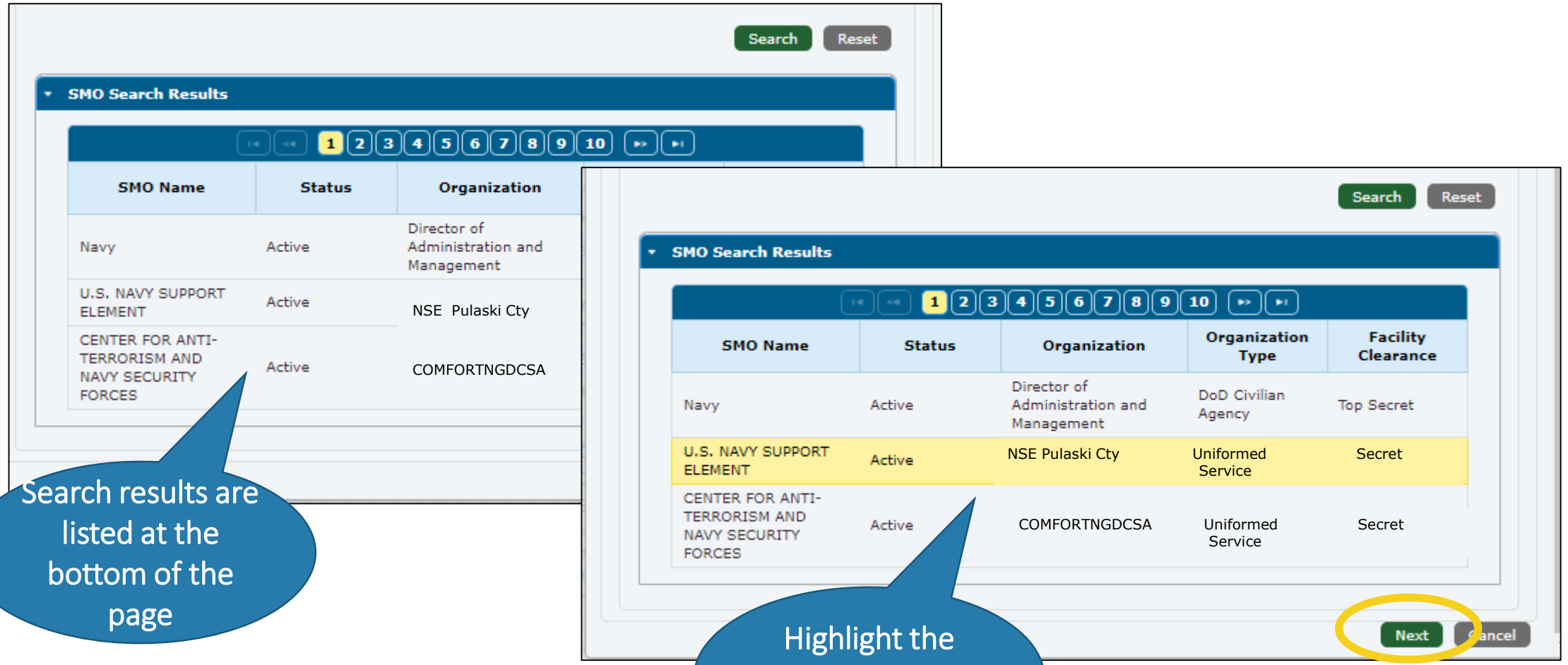


Enter data into one of the data fields, such as SMO Name

If the search is too broad, it will generate an error banner

Search based on the criteria entered

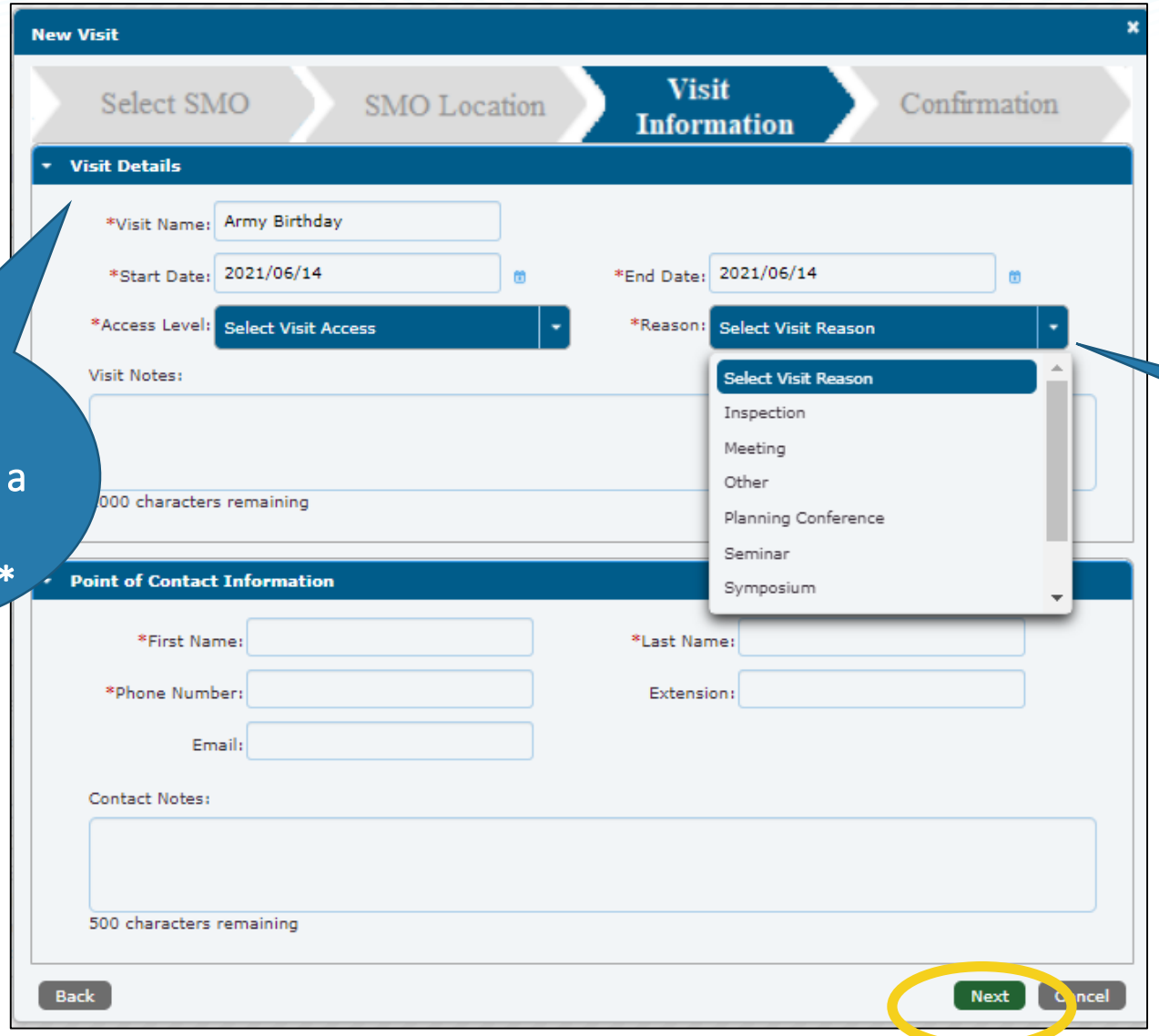
Select SMO



Search results are listed at the bottom of the page

Highlight the desired SMO and click next

Visit Information



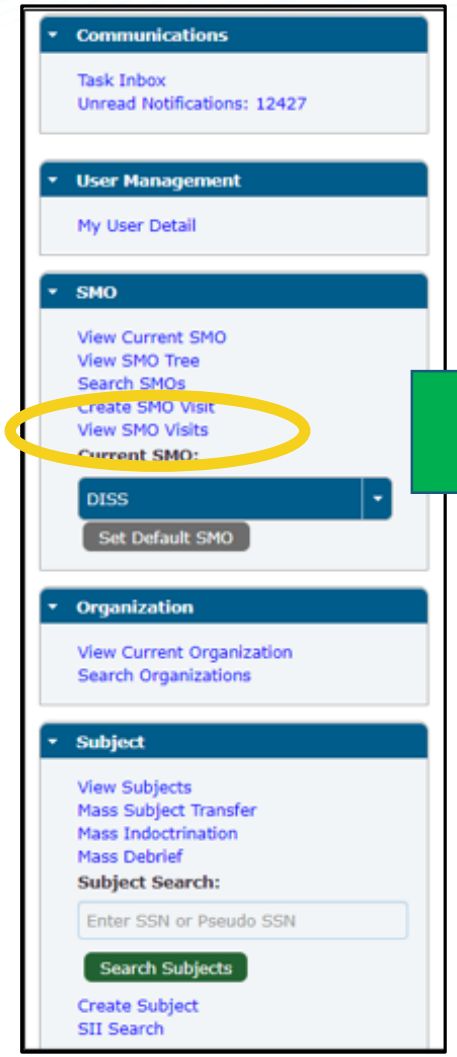
Fill in all pertinent information; at a minimum, all boxes with an *

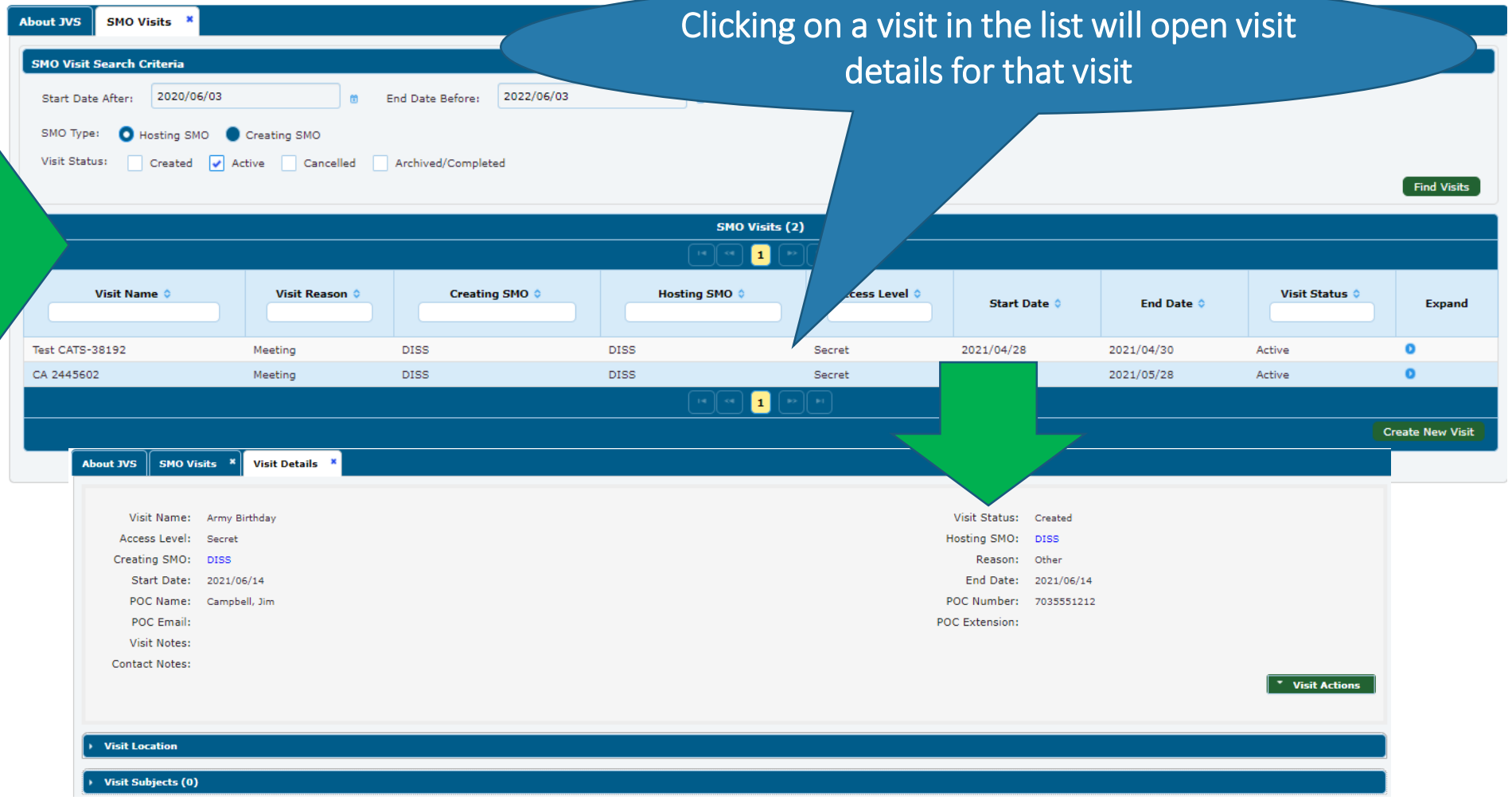
Pull downs provide a menu for Reason and Access level

Visit Confirmation

Upon completion of the Visit information, a Confirmation page will appear: completing the process

View SMO Visits—Visit Management





Clicking on a visit in the list will open visit details for that visit

View SMO Visits—Visit Actions

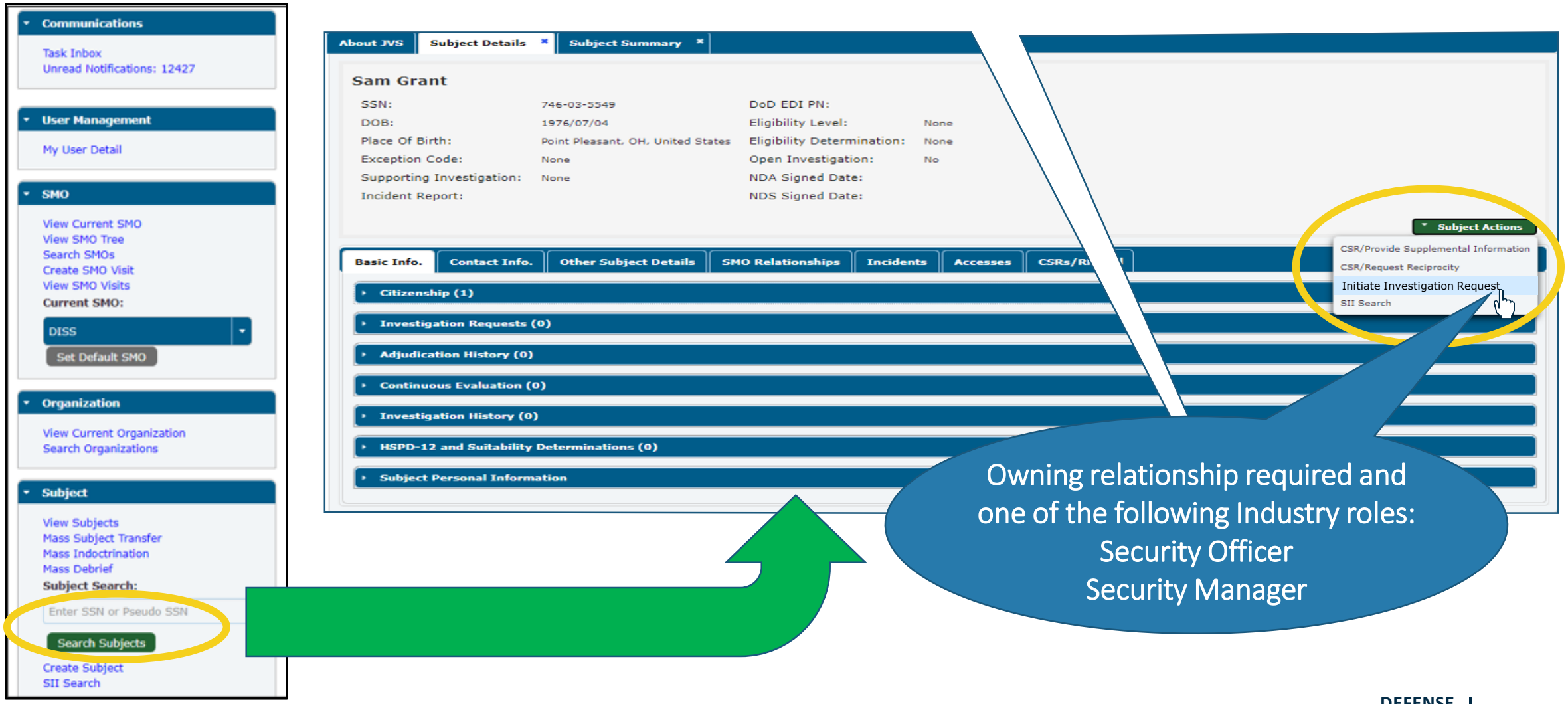
Visit Details allows users to manage the SMO visits via the Visit Actions pull down

Users can edit, cancel, and change visit information here

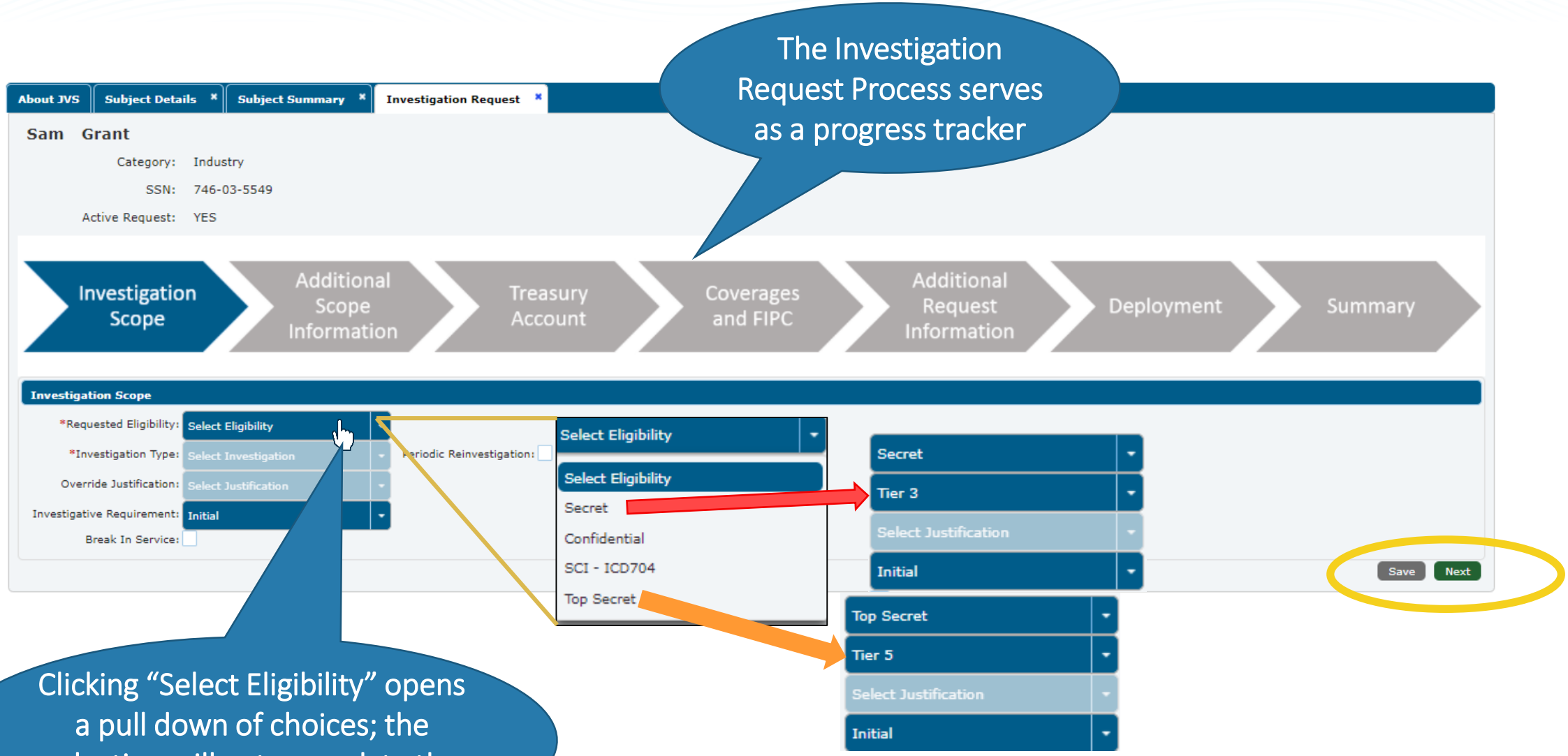
INVESTIGATION REQUESTS
(INDUSTRY ONLY)

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

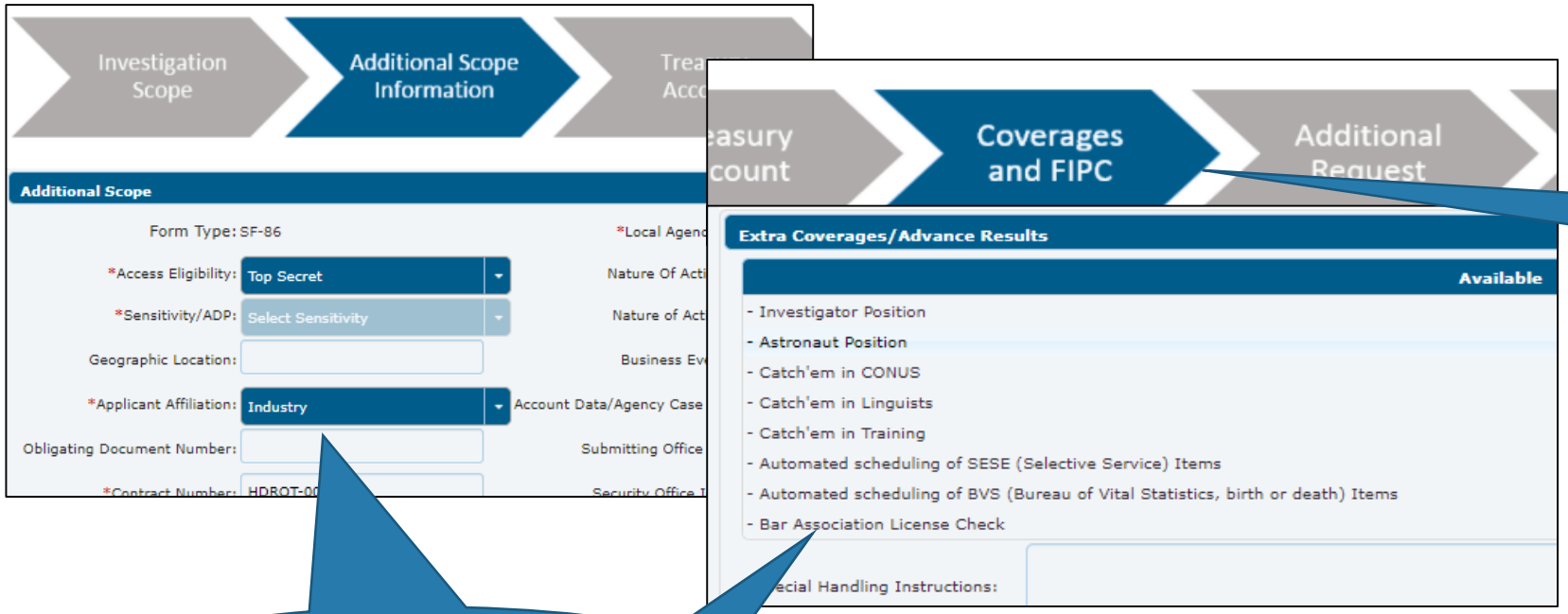
Initiate Investigation Request



Investigation Scope



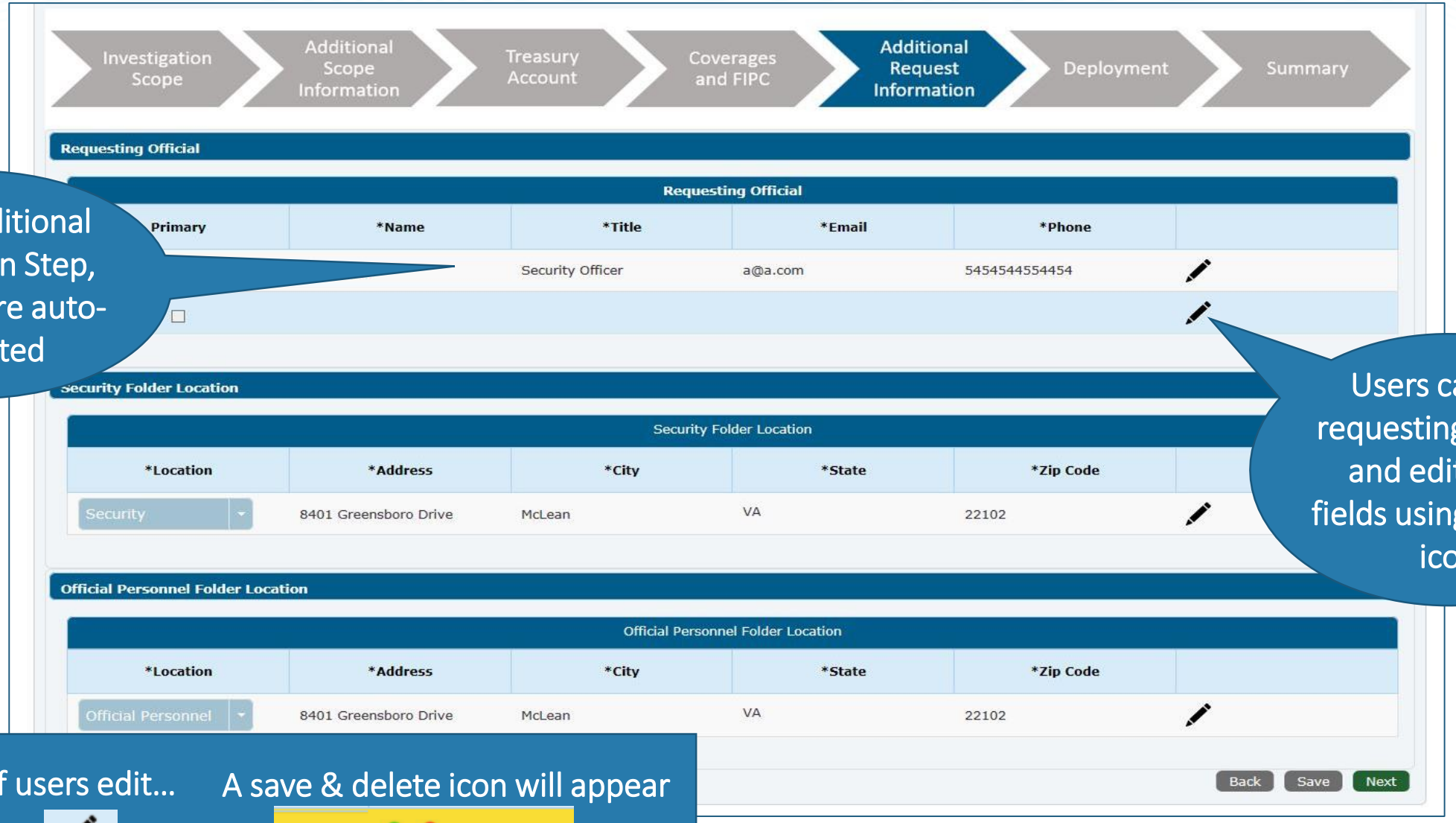
Investigation Request Tracking



Progress Tracker highlights open step in the process

User populates data fields as required, or additional information as appropriate

Add Additional Information

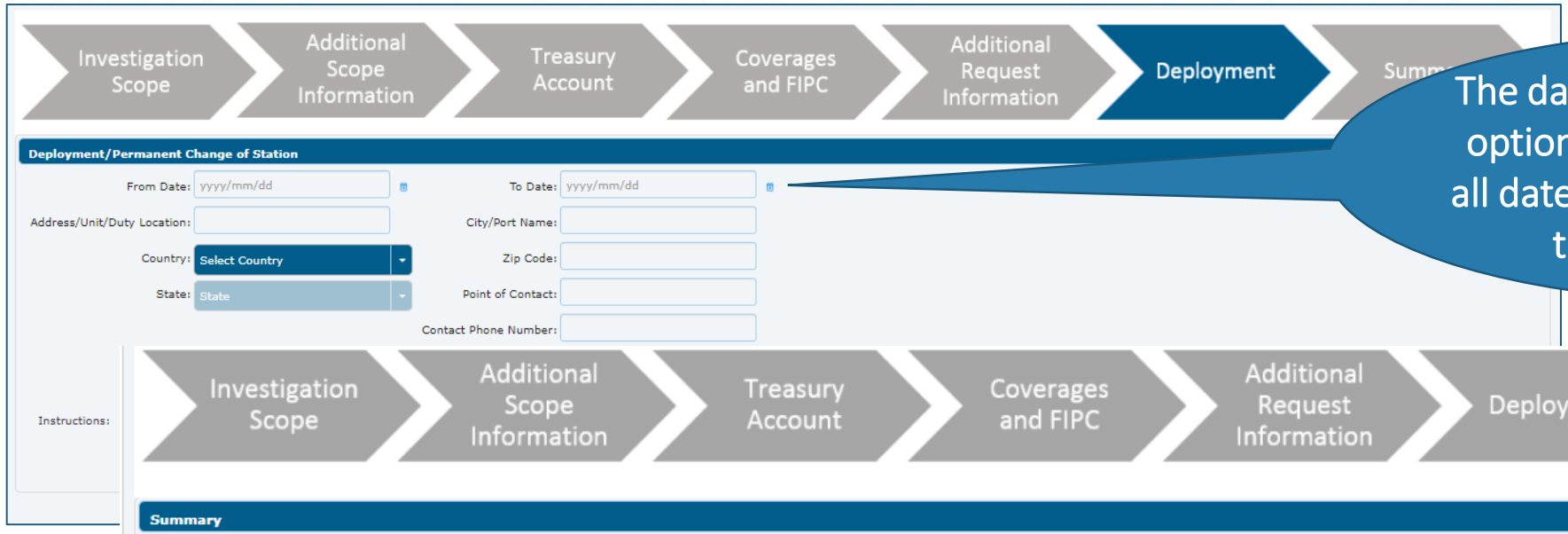


At the Additional Information Step, the fields are auto-populated

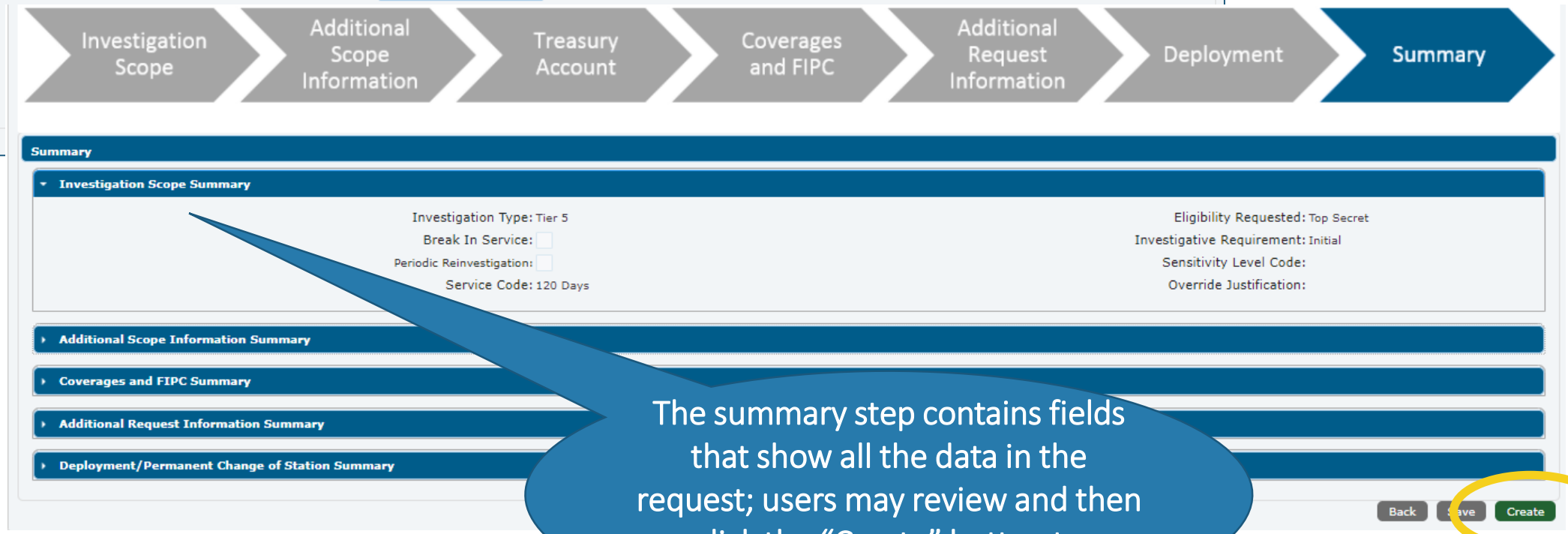
Users can add requesting officials and edit other fields using the edit icon

If users edit… A save & delete icon will appear

Wrapping up the Request

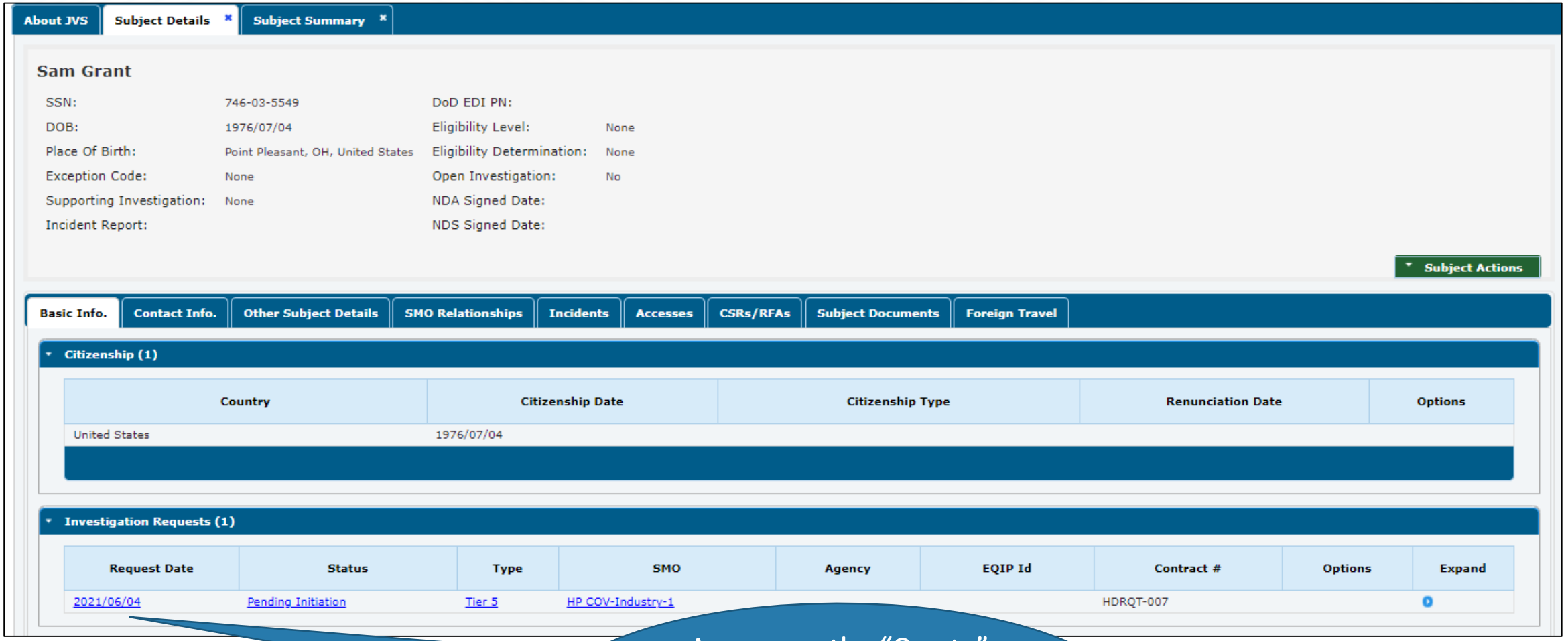


The data fields in Deployment are optional; it should be noted that all date fields have a calendar icon to facilitate date input



The summary step contains fields that show all the data in the request; users may review and then click the “Create” button to complete/initiate

Investigation Initiation



As soon as the "Create" investigation request button has been clicked a status will appear in the Subject Details

TAKE-AWAYS

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Quick Tips

- ✓ When searching SMOs in DISS the asterisk (*) is not required for a “wild card” search
- ✓ DISS application works best with the following web browsers: Edge, Version 11 or above, Mozilla Firefox, or Chrome. Inactivity in DISS for more than 10 minutes will cause log out; a warning is posted at 8 minutes
- ✓ If you haven’t been provisioned for the right SMO(s), and cannot see your hierarchy, you’ll need to contact DCSA at dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil to request changes to your provisioned account
- ✓ If your hierarchy is inaccurate (missing SMOs, incorrect parent to child relationships, etc.) you will need to complete a Hierarchy Change Request (HCR) form
- ✓ Failure to login within 30 days will lock your account; 45 days the account will be deactivated

Support Contacts

Knowledge Center Inquiries

Other DCSA Offices

DCSA Policy	DSS.quantico.DSS-hq.mbx.policyhq@mail.mi
DCSA Facebook	https://www.facebook.com/DCSA.Stakeholders
DCSA Twitter	https://twitter.com/DSSPublicAffair

Background Investigations

DCSA's System Liaison	724-794-5612, Ext. 4600 or eQIP@nbib.gov
For Technical Issues with e-QIP	866-631-3019
For Agent's/ Investigator's Identity or Status	1-888-795-5673 or RMFSIMSST@nbib.gov

DoD CAF Call Center

Phone	301-833-3850* (SSOs and FSOs ONLY)
Menu Options	5 -Industry
Email	dcsa.meade.dcsa-dvd.mbx.dodcaf-callcenter@mail.mil

* Temporarily suspended due to COVID-19

DOHA

Phone	866-231-3153
Website	dohastatus@ssdgc.osd.mil

Q & A

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY