DISS JVS JOB AID

Defense Information System for Security
Joint Verification System

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

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

DISS
Defense Information System for Security

DMDC LINKS

DISS CATS LOGIN	DISS JVS LOGIN	DISS APPEALS LOGIN

https://www.dcsa.mil/is/diss/

DCSA Website - DISS

DISS Resources

- General Information
- Access Request
- Data Quality
- Training Aids

- Instructions for Adding DISS as a Trusted Site
- Contact Center Encryption
- DISS Fielding Plan
- DISS Fact Sheet

DISS Resources

- General Information
- Access Request
- Data Quality
- Training Aids

- DISS Account Management Policy
- DISS Account Request Procedure
- PSSAR Form
- PSSAR Industry FAQs

- DISS
- DISS Resources
- DISS FAQs
- DISS Alerts
- DISS Contact Information

DISS Resources

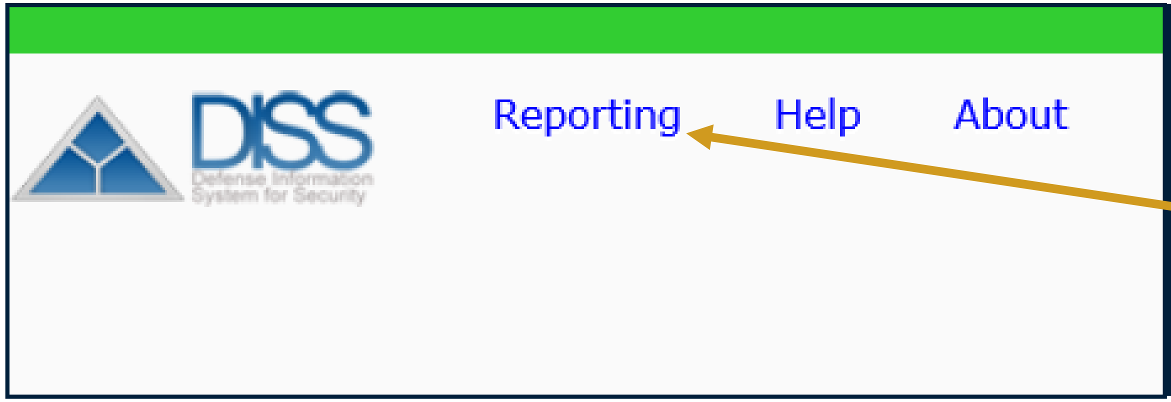
- General Information
- Access Request
- Data Quality
- Training Aids

1. Creating and Viewing a Subject in DISS
2. Removing Subject Relationship from SMO in DISS
3. Submitting NDAs in DISS
4. Granting Access and Temporary Access in DISS
5. Debriefing and Suspending Access in DISS
6. Creating Visit Requests in DISS
7. Changing Visit Requests in DISS
8. DISS Visit Request FAQs
9. Moving SMOs in DISS
10. DISS Tips and Tricks
11. Investigation Requests (Industry Only)

DISS Virtual Training Presentation

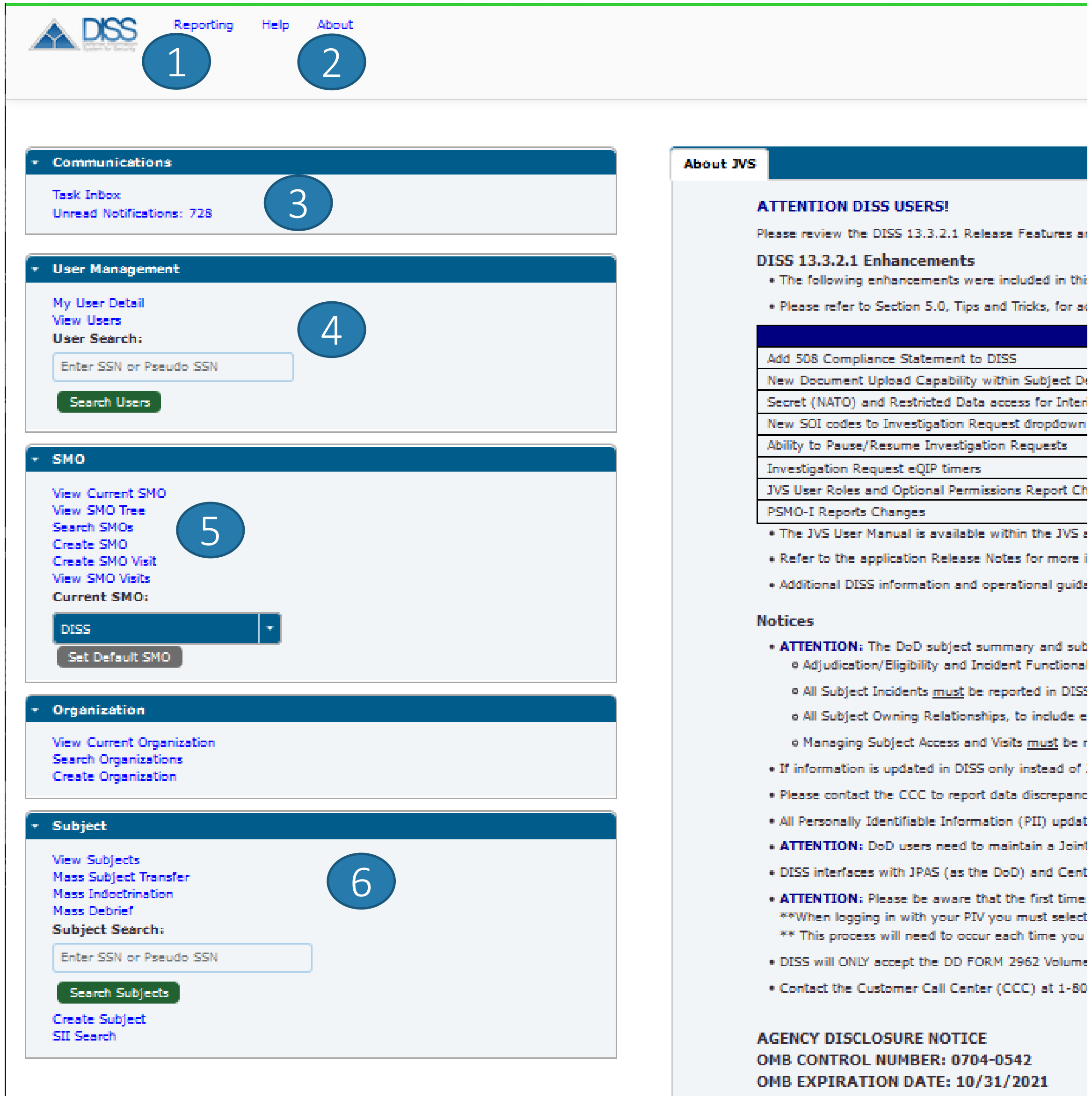
User Manual

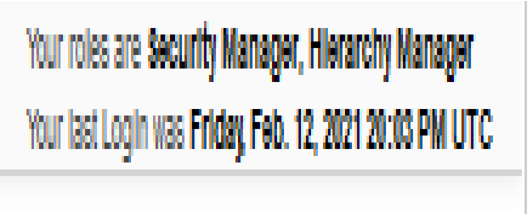
The User Manual for JVS and Reporting is designed for the users in the Security Management Office (SMO) who have access to view and edit personnel security information. The User Manual guides users through all of the functionalities of JVS and Reporting by following the control panels and menu options from the top of the webpage to the bottom.



DISS JVS User Manual is accessible inside DISS. To access the user manual click on Help link located at the top of the home page once you log into JVS.

Navigation Links





1. Reporting Link
2. Help – User Manual
3. Task Inbox
4. View Users
5. SMO (Tree, Create, Visits)
6. View Subjects

Select Your Topic…

Accounts & SMO Hierarchy

Account Manager process, roles, permissions and SMO Hierarchy alignment

Relationships

Create Subject and establish relationship within SMO

NDA Submission Process

NDA (SF312) Submission Process within JVS

Access Management

Manage Subject Access within SMO (Grant, Debrief, and Suspend)

Visit Requests

Create and Change Visit Request within JVS

Investigation Requests

Industry - Investigation Request using JVS

Tips and Tricks

Quick Tips and Tricks in JVS for users

Personnel Security Support

DSCA Contact Information

ACCOUNTS AND SMO HIERARCHY

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Program Security System Access Request (PSSAR):

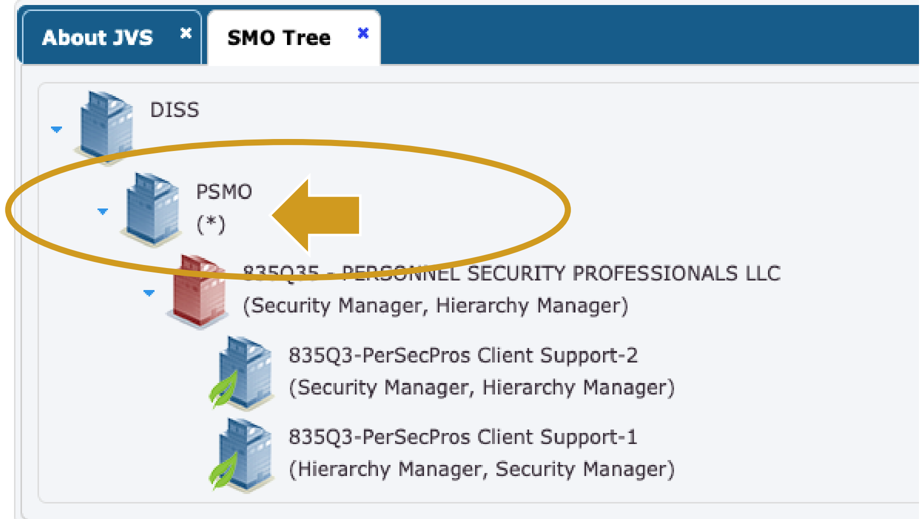
- Account access information/process is provided in the DISS Account Management Policy and the Account Request Procedure.
- Industry is **no longer required** to submit LOA to receive a DISS account. KMP must sign the DISS PSSAR.
- Industry send PSSAR to dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil

- DISS PSSAR (account access request): make sure you are using the latest version of the DD FORM 2962 and completed in its entirety. For guidance refer to the **PSSAR FAQs** found on the Personnel Security/Assurance DISS webpage https://www.dcsa.mil/is/diss/dissresources/
- For proper **User Roles and Permissions** review the DISS Account Management Policy. (Note: Manage SCI Users and Manage SCI Access, if required)
- **Common Rejections**
  - PSSAR Part 2, Section 16b: Selecting everything in this section or alternatively selecting nothing at all.
  - PSSAR Part 3, Sections 18 and 19: Certificates/training expired (more than one-year old) or dates on certificates do not match dates on PSSAR form.

Hierarchy Management 101

- When data migration occurred, JPAS Levels were transferred to different SMOs in DISS. This means if a user was provisioned for Level 2, 4 and 5 for SMO 12AB3 in JPAS, there are now three SMOs in DISS, one for each level (12AB32, 12AB34 and 12AB35).
- In order to accurately assess the Hierarchy needs, users should understand the scope of their hierarchy by searching for all SMOs associated with their CAGE Code.
- All SMOs should be managed at the highest Parent with at least one Hierarchy Manager.
- It is important that all CAGE Codes within the hierarchy tree can be accessed and managed by a Security Manager/Officer. This can be done through provisioning for each SMO, or configuring the hierarchy to account for all SMOs and provisioning for Security Manager at the highest Parent level.

Know Your Current Hierarchy



- Within the SMO Tree you have Parent SMOs and Child SMOs, these are at different levels within the SMO tree.
- Hierarchy Managers should ensure they are operating at the highest SMO with PSMO (VROC) as the parent SMO for Industry.

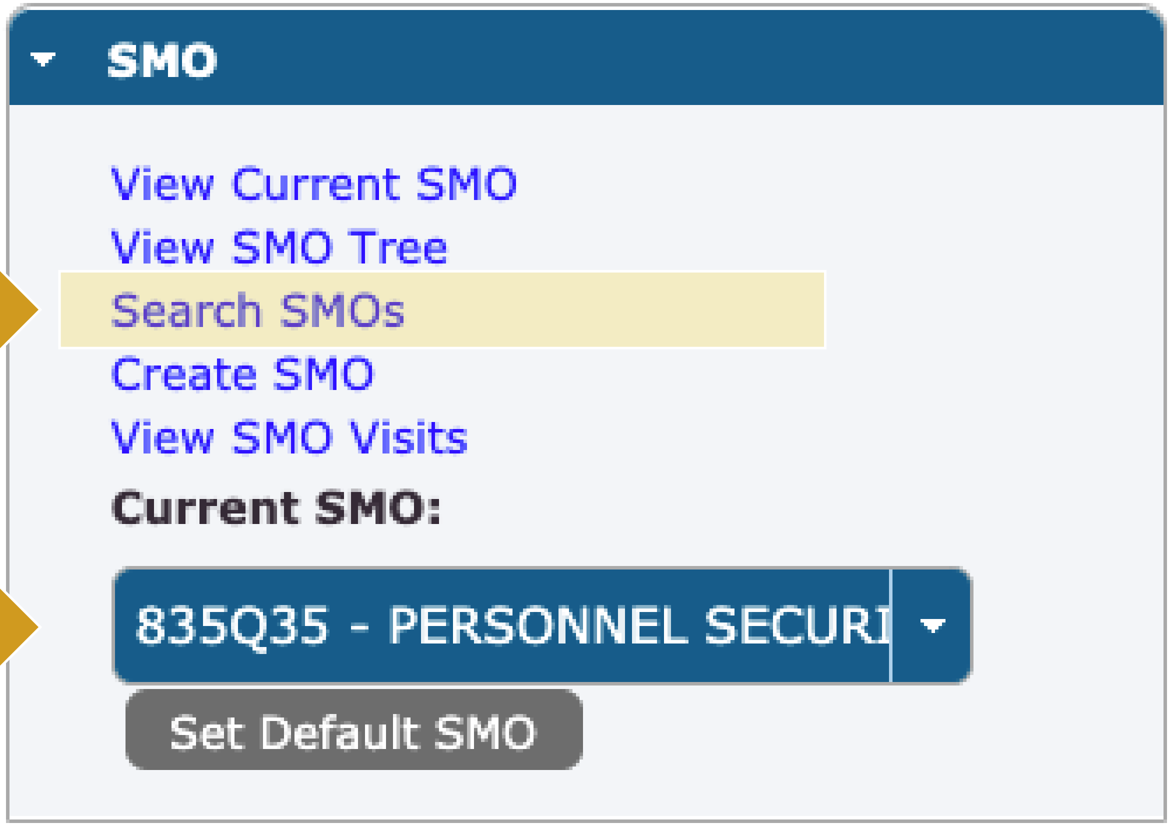
- Think of a SMO (Security Management Office) tree like a company's org chart, the person at the top is responsible for the organization(s) below them. A manager in one branch can't take action on another manager's team that is at a higher level.
- The SMO tree is the same concept. As an example, let's replace people in the org chart with SMOs, a small company may have a flat org chart and only one SMO they are responsible for, while larger companies may have many and need to segment certain SMOs from others.
- If you have more than 75 children/grandchildren SMOs, you will not be able to see your Hierarchy in the application. For resolution, you will need to contact the DMDC Contact Center / VROC.

Process to Move a SMO

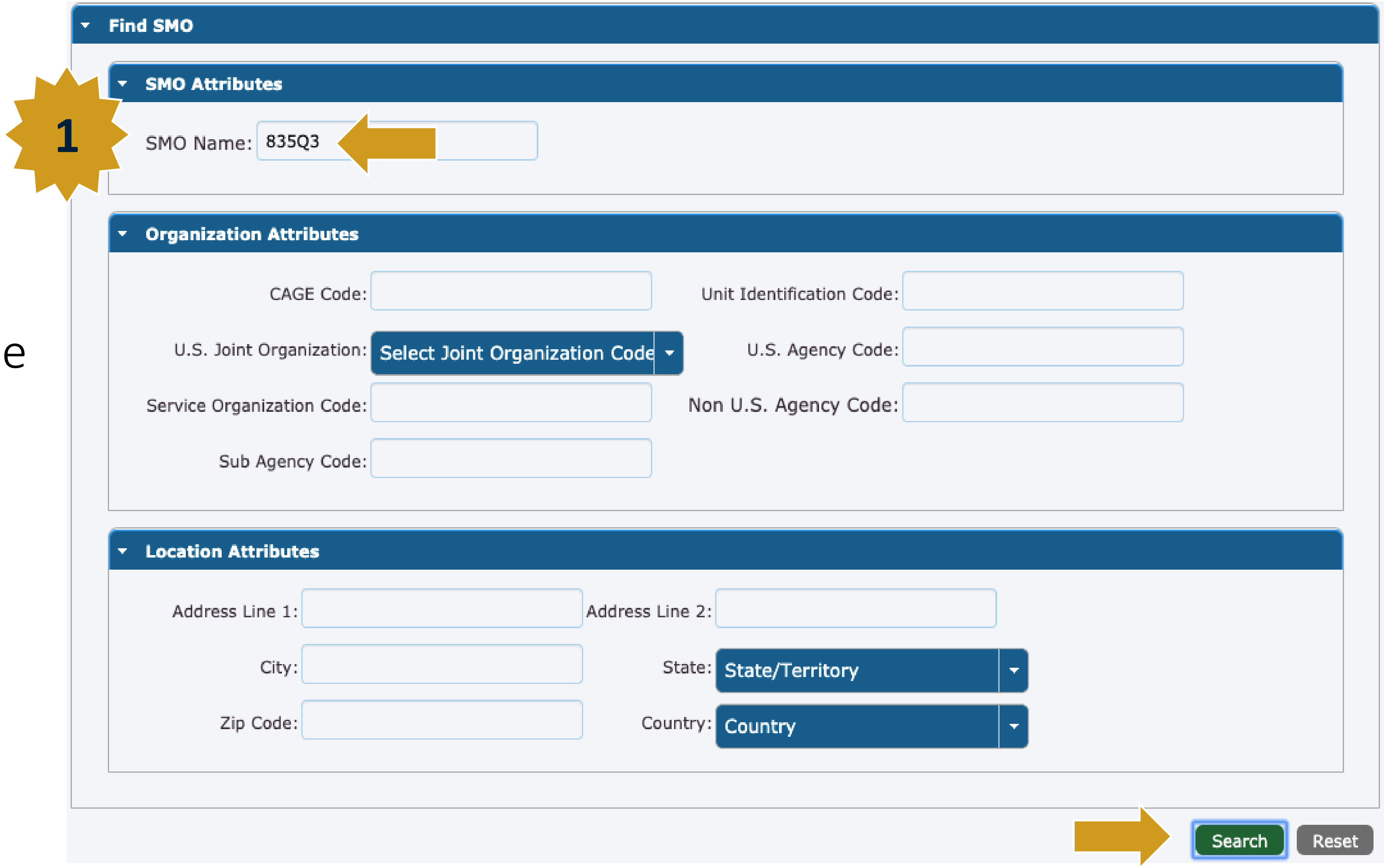
Select Search SMO:

If you do not have the **Search SMOs** option, please work with your Hierarchy Manager to determine your role/permission setup.

Ensure that your current SMO is set for the SMO you are working or at the Highest SMO in your branch.



Step 1: Search SMOs



1. Type the 5 digit CAGE Code in the SMO Name and select *Search*.

Step 2: SMO Results

2. Select the appropriate SMO to be moved.

*In many instances, searching for the 5 digit CAGE will result in multiple SMOs. The SMO Parent identifies where in the hierarchy that SMO sits. If the SMO Parent is not accurate, a SMO move or Hierarchy Change Request will be required.

SMO Name	Status	Organization	Organization Type	SMO Parent
835Q35 - PERSONNEL SECURITY PROFESSIONALS LLC	Active	PERSONNEL SECURITY PROFESSIONA	Contracting Organization or Vendor	PSMO
835Q3-PerSecPros Client Support-2	Active	PERSONNEL SECURITY PROFESSIONA	Contracting Organization or Vendor	835Q35 - PERSONNEL SECURITY PROFESSIONALS LLC
835Q3-PerSecPros Client Support-1	Active	PERSONNEL SECURITY PROFESSIONA	Contracting Organization or Vendor	835Q35 - PERSONNEL SECURITY PROFESSIONALS LLC

2

Step 3: SMO Actions

3. Select *Move SMO* from the **SMO Actions** tab, this will bring up the ability to search for the new Parent.

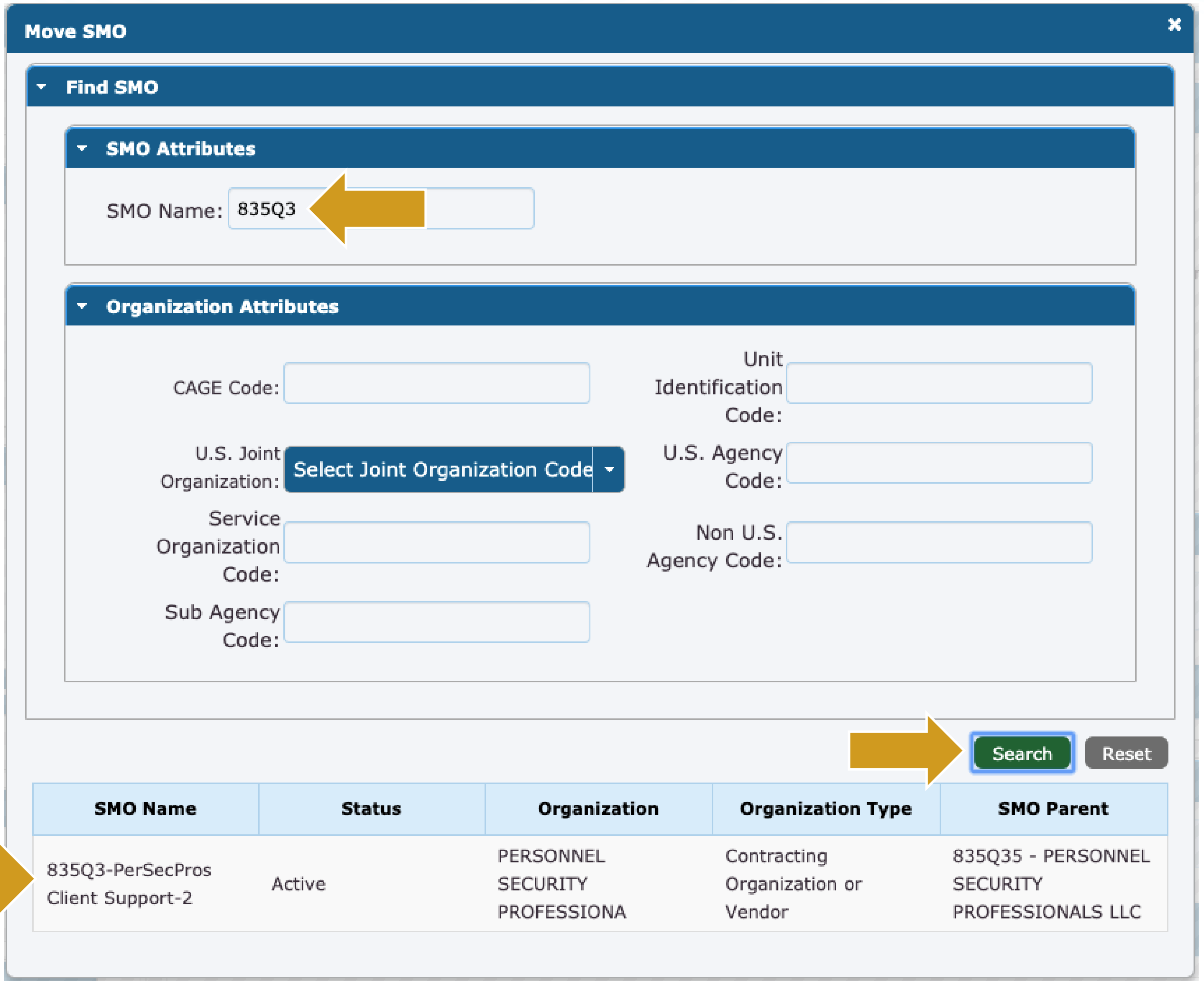
* If you do not get the *Move SMO* option, you can select *Make Current SMO* if available. This is due to the SMO not being in the hierarchy of the SMO you're currently operating as. If no SMO Actions are available, a Hierarchy Change Request (HCR) will need to be submitted.

Step 4-5: Search for New Parent

4. Type the 5-digit CAGE Code or SMO Name for the desired Parent. Select ***Search***.

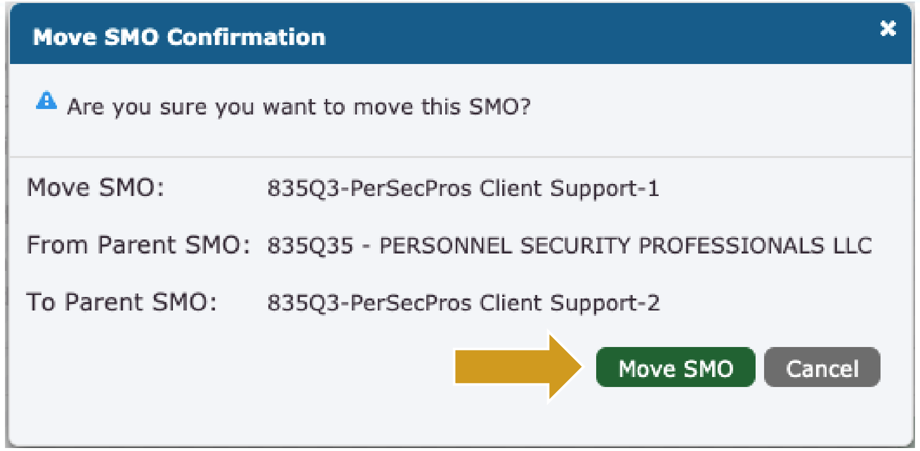
   The SMO Name appears below.

5. Select the desired Parent.

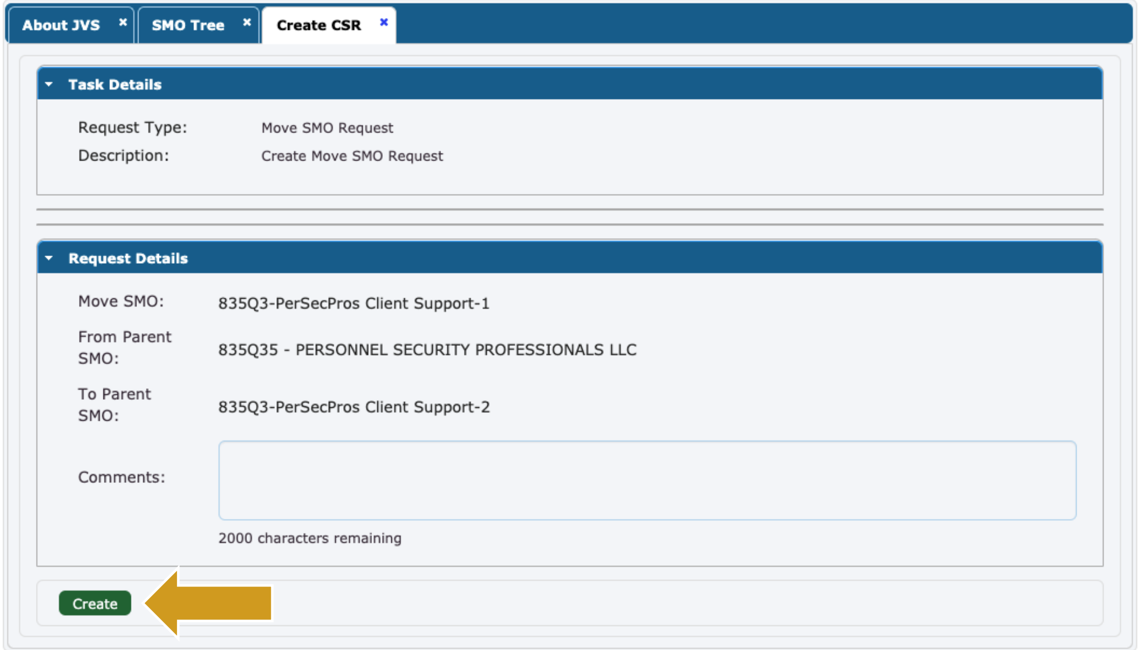


Slide 5a-b: Move SMO Confirmation and Create CSR

5a. If the SMO is already in your Hierarchy, a pop-up will confirm the movement with the chosen parent. Selecting *Move SMO* will finalize the process.

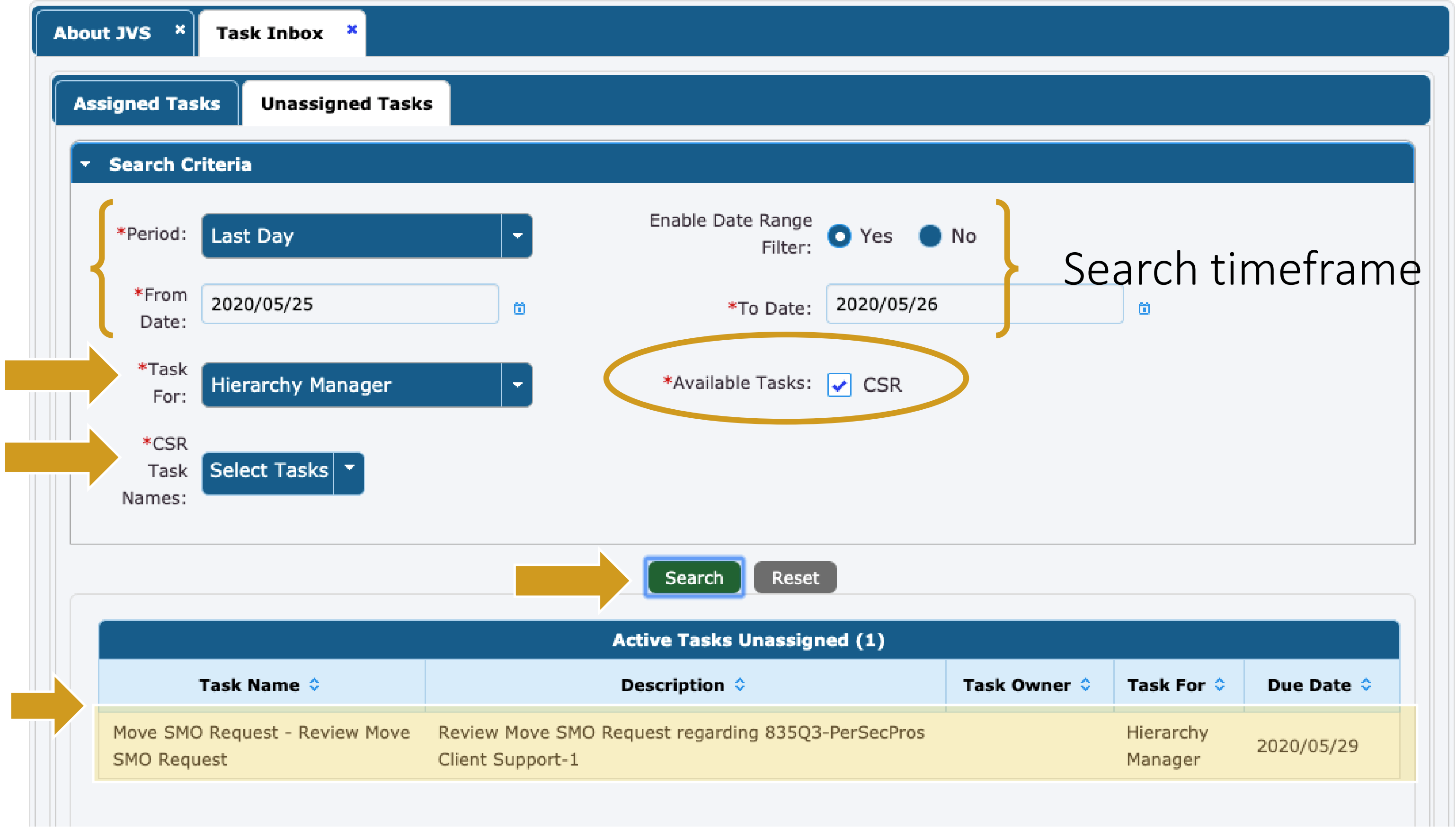


5b. If the SMO is currently outside of the chosen Hierarchy, a Customer Service Request (CSR) will be created and sent to the new Parent SMO. This may also occur if the SMO is in a Transient status.



Step 6: Finding Move SMO CSR (Unassigned Tasks)

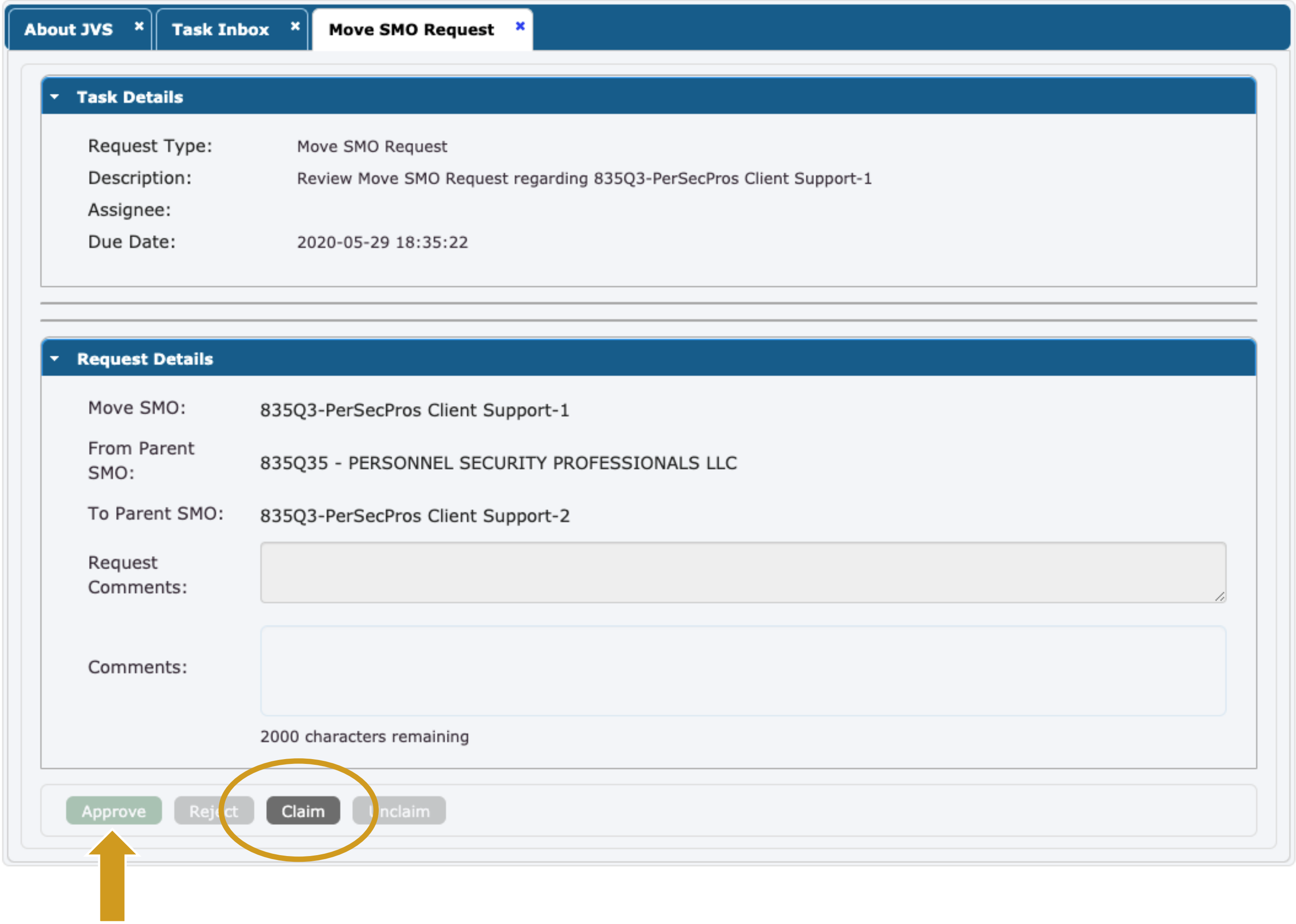
6. If a CSR was created, the Hierarchy Manager of the new Parent can view the CSR under the **Task Inbox** by searching for the CSR. Ensure that the timeframe is accurate or disabled. The task will be for **Hierarchy Manager**, select the checkbox for **CSR** and select ***Move SMO Request*** under the **CSR Task Names**, select search.



Step 7-8: Claim and Approve/Reject SMO Move

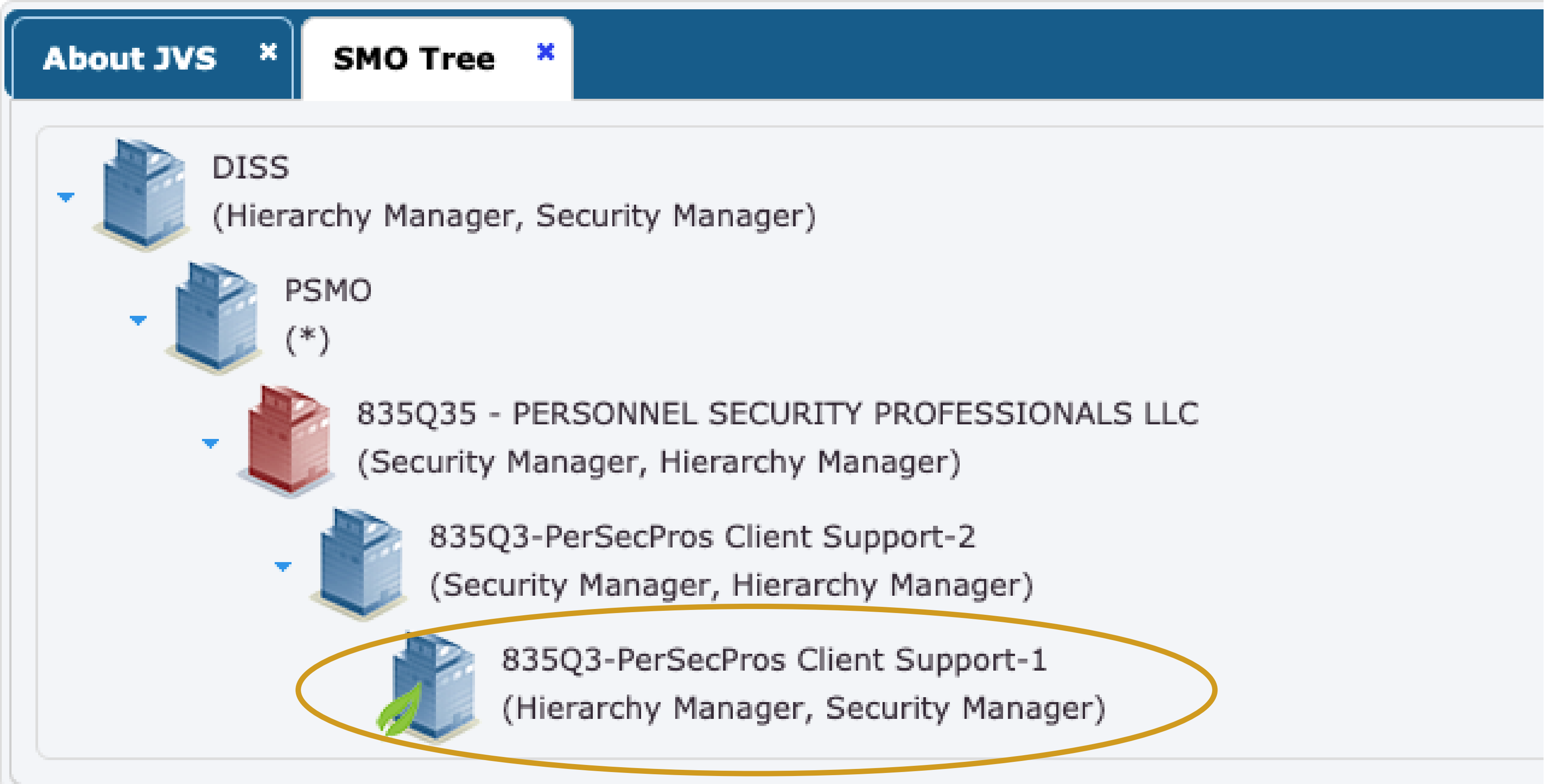
7. After selecting the appropriate CSR, select *Claim* to process CSR.

8. Once claimed, the Hierarchy Manager will have the ability to *Approve* the request which will finalize the move. Rejecting the request will close out the CSR and the move will be terminated.



Updated SMO Tree

When the SMO Move has been completed, your SMO Tree will reflect the change upon next login.



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).
  - o The HCR must contain ALL SMOs related to your CAGE Code.
  - o The HCR must show ONE parent that the Hierarchy Manager is provisioned under.

	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.
  - o All identified SMOs will be moved to the ONE Parent.
  - o The Hierarchy Manager will be able to configure their Hierarchy under the identified Parent SMO.

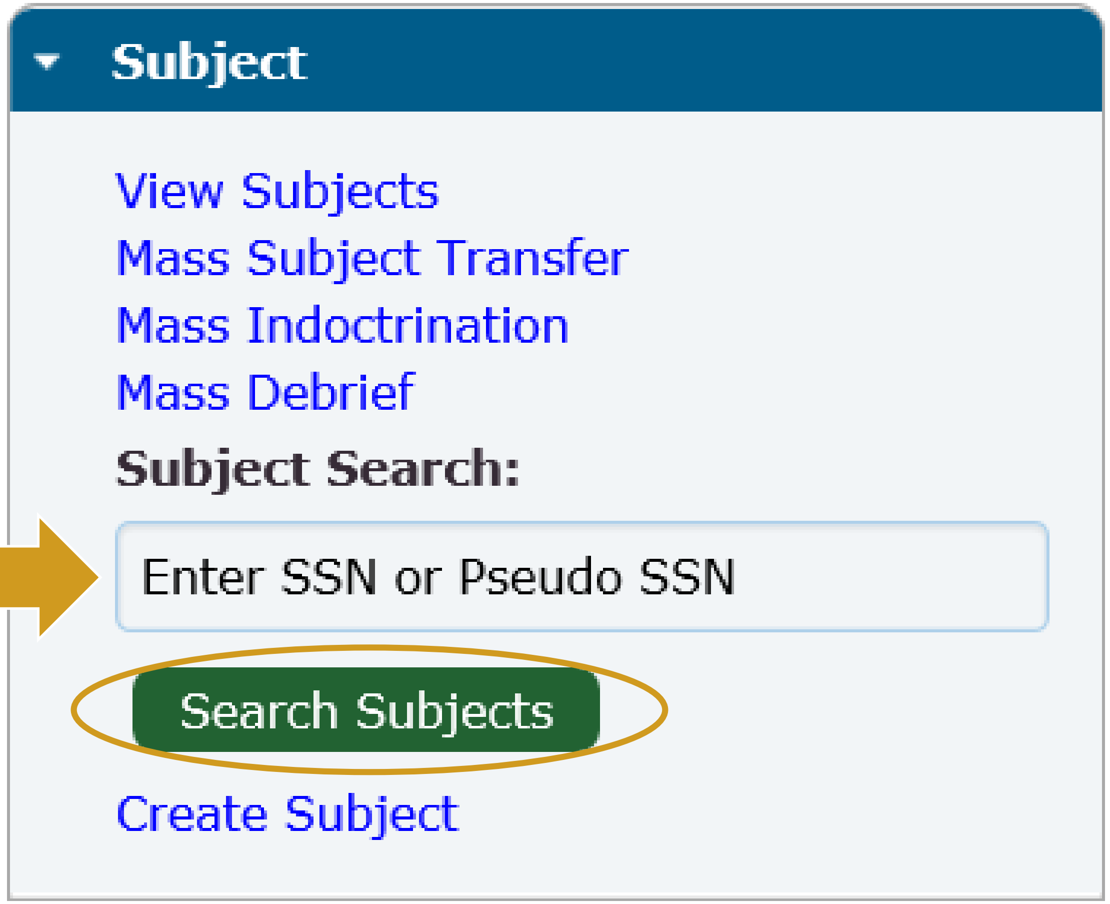
RELATIONSHIPS

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Search Subject

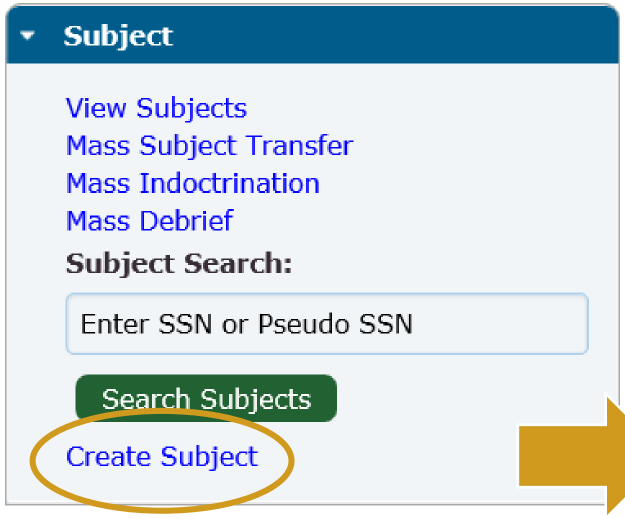
To find a Subject in the **Subject Management** control panel, search for a subject by entering their nine-digit SSN or PSSN in the **Subject Search** field and clicking on ***Search Subjects***.

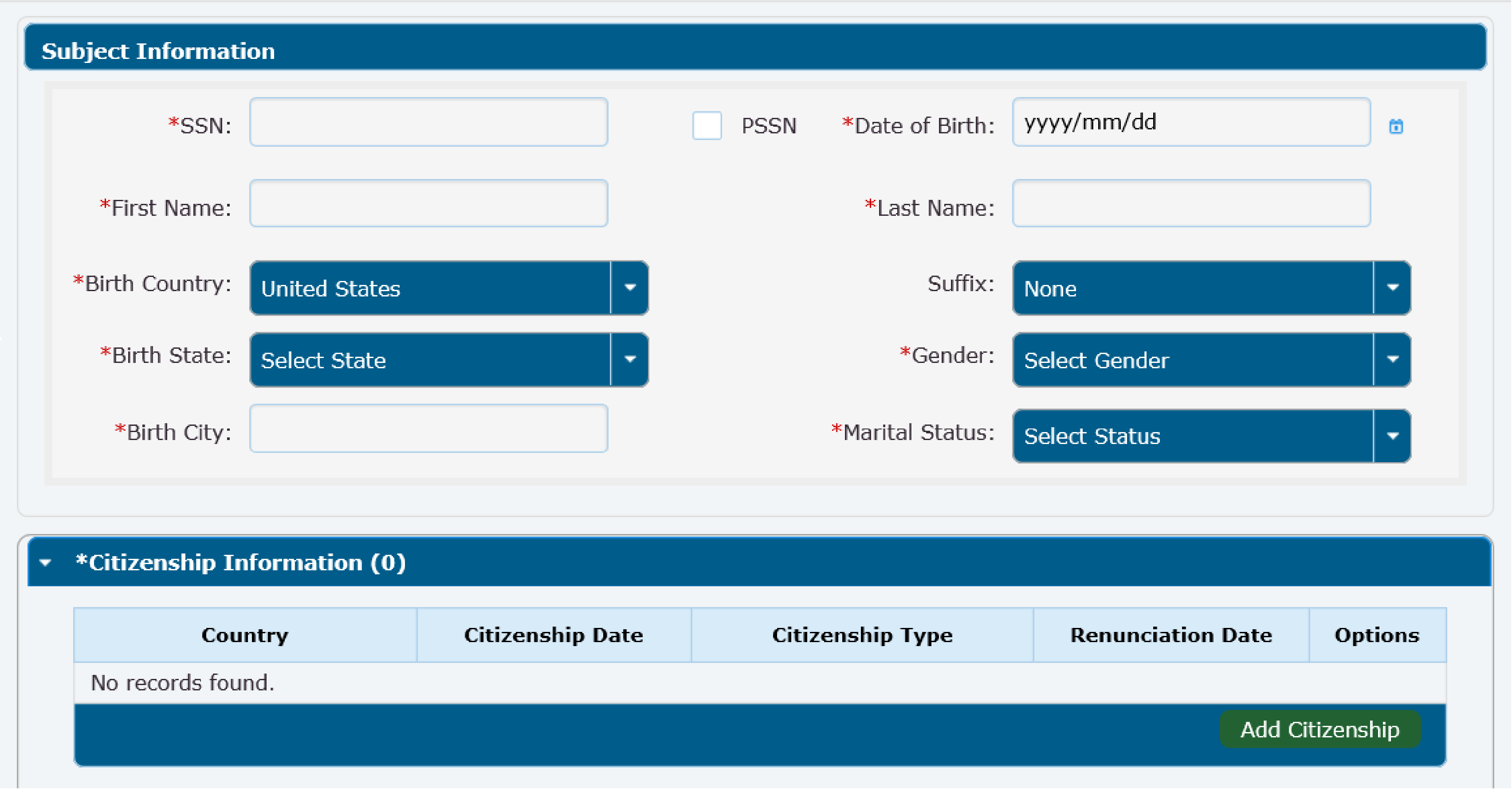
If the Subject is not in DISS or you typed in the wrong SSN you will get a **No Subject Found for SSN/PSSN.**



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

Create Subject: Required Information



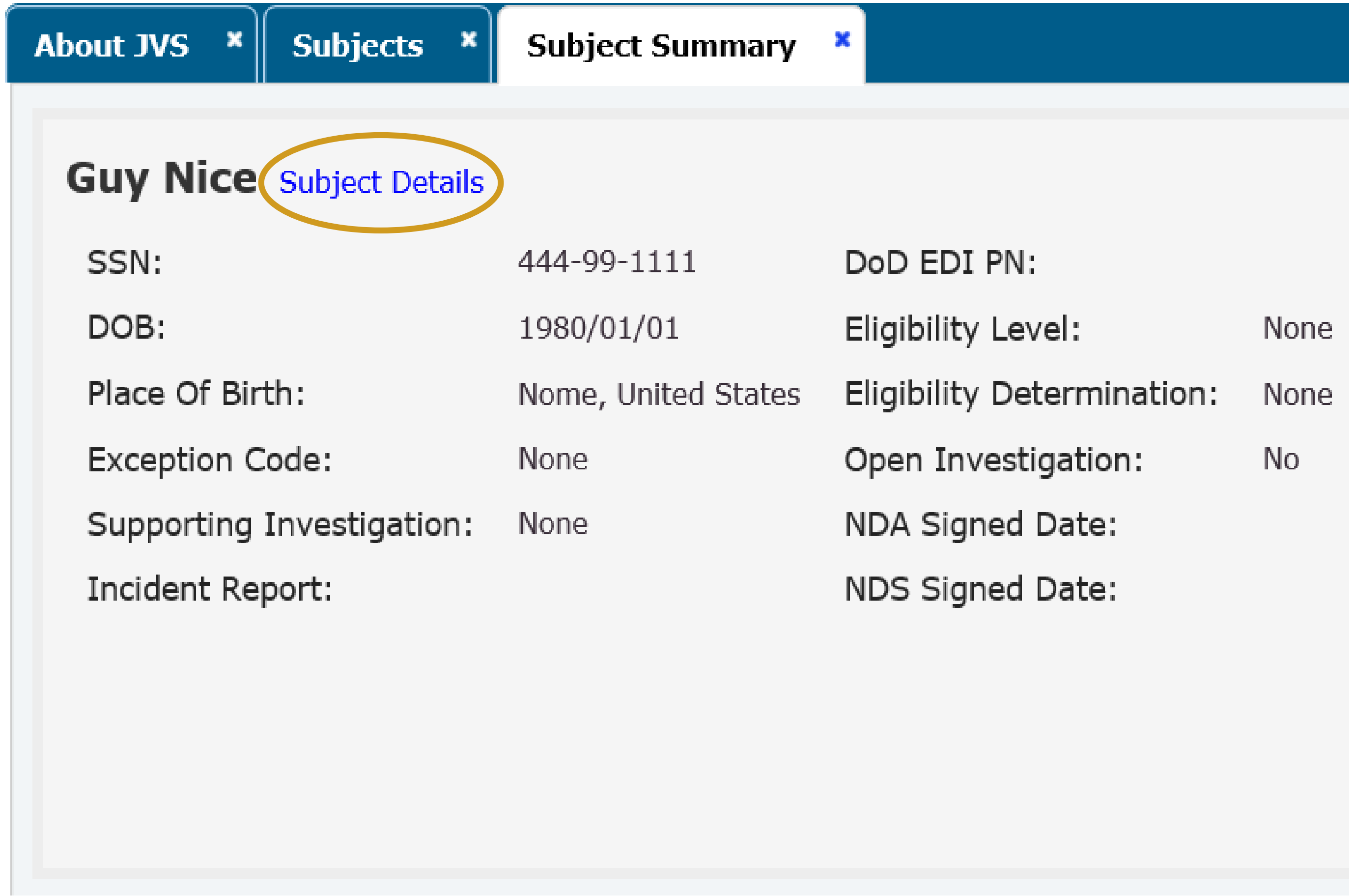


Subject Details

If you typed in the SSN correctly, the Subject Summary will show.

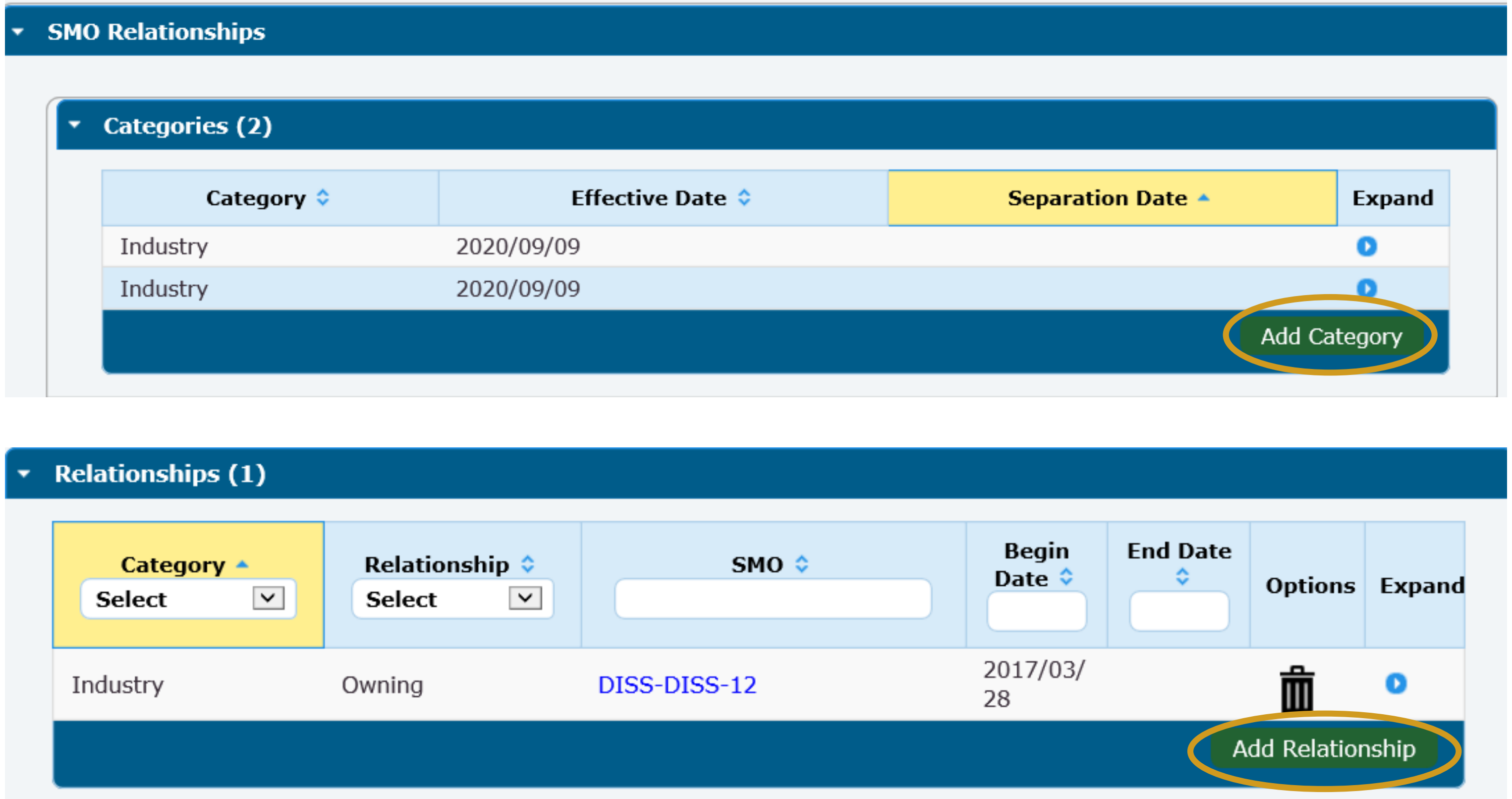
If the ***Subject Details*** hyper link is missing next to the subject name. There could be 3 possible reasons:

- Missing Relationship
- Missing Organization
- Missing Both



Subject Details

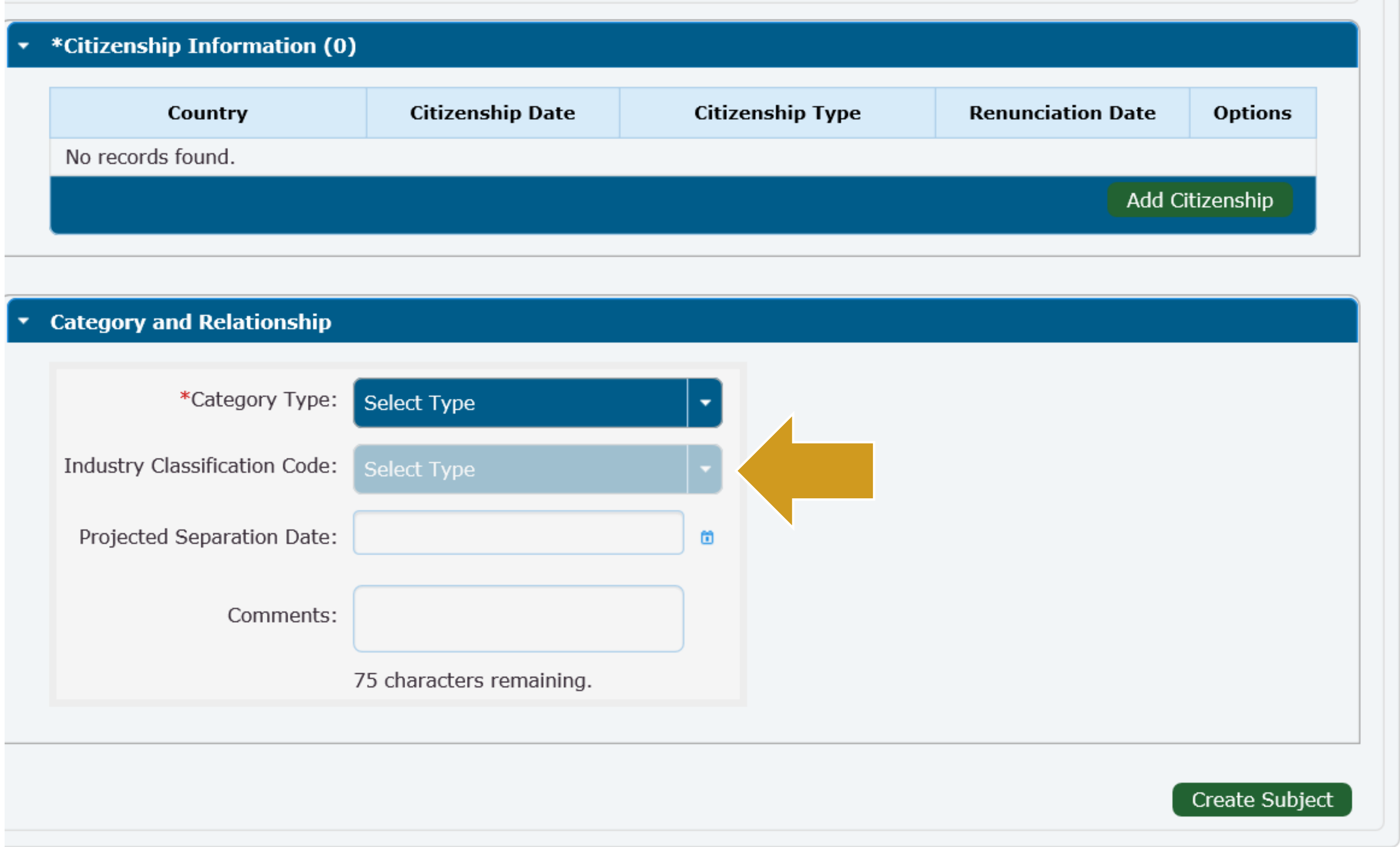
If the SMO details link is not showing in a subject record - you will need to establish a category and relationship by clicking the *Add Category* radio button and *Add Relationship*.



Once the category and relationship is established the Subject Details link will appear. Subject Details will expand the record with other tabs relating to the subject.

Category Type and Relationship

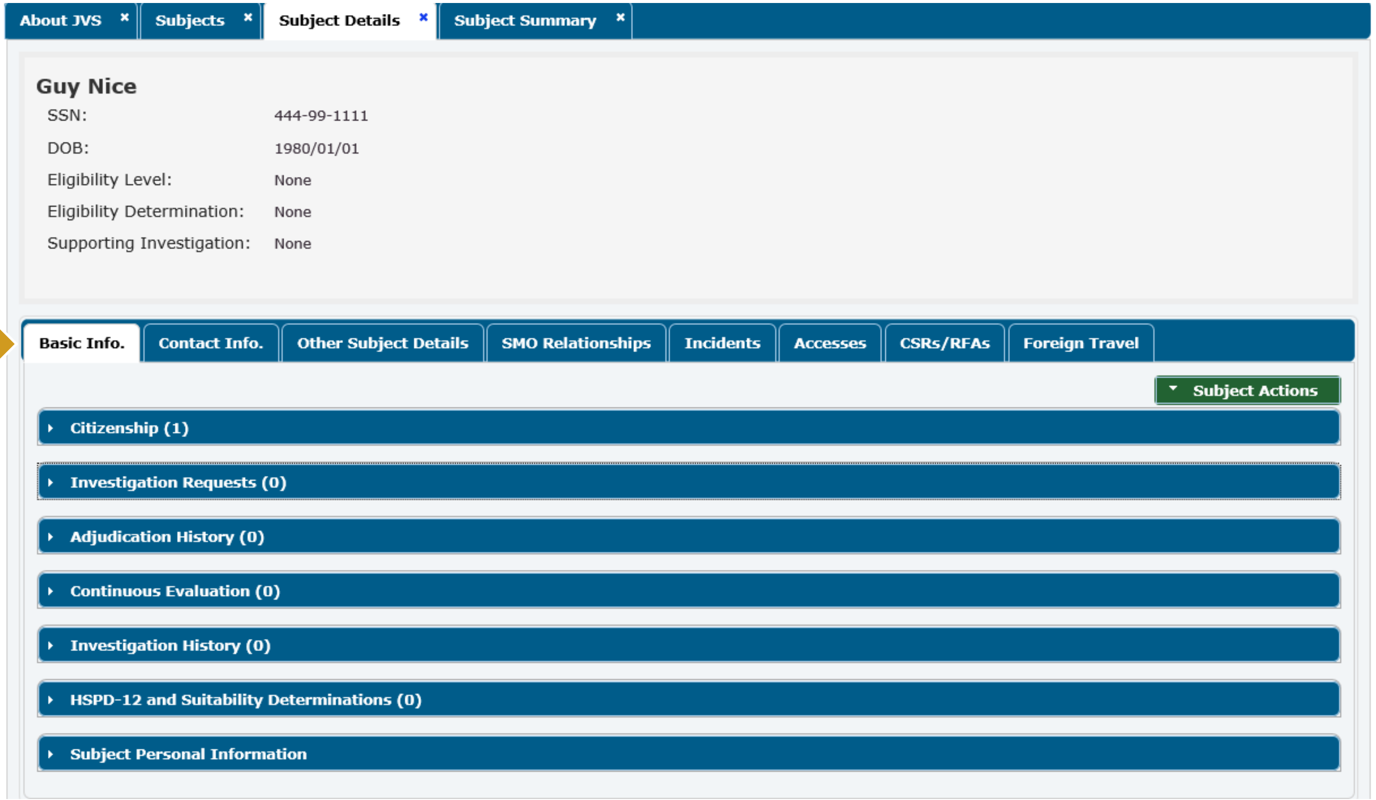
If the **Category Type** is **Industry**, use the drop-down menu to select an **Industry Classification Code**. Use the search field to find a specific **Industry Classification Code**.



Subject Details

Under the **Subject Details** tab, the header displays the subject's name, SSN, DOB, and current Eligibility Level, and Eligibility Determination.

The Basic Info. sub-tab includes Citizenship Information, Investigations, Subject's Case History, Continuous Evaluation, HSPD-12 and Suitability Determinations, and Subject Personal Information.



NDA SUBMISSION PROCESS

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Subject Details

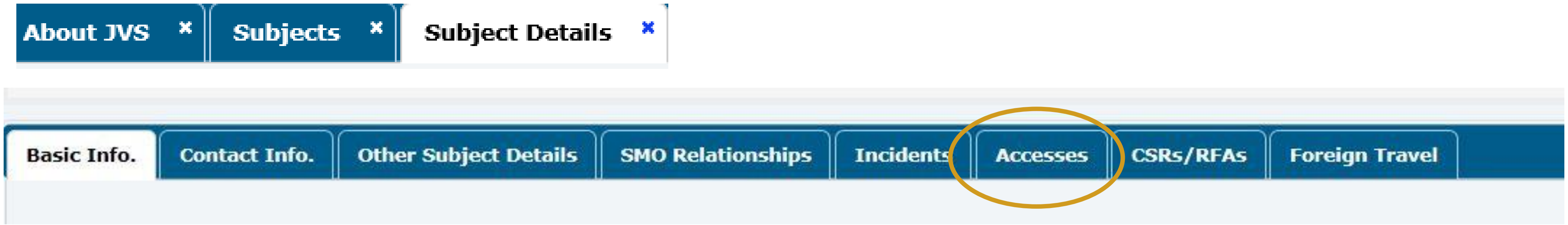
If you typed in the SSN correctly the **Subject Summary** will show.

Select ***Subject Details***.

Scenario: In this case there is an open investigation but no SF-312/Non Disclosure Agreement in the subject's record and the subject can not be granted temporary (interim) access until a SF-312 is uploaded.

Subject Details tab appears.

Subject Details: Accesses



1. Under the **Subject Details** tabs - select **Accesses.**

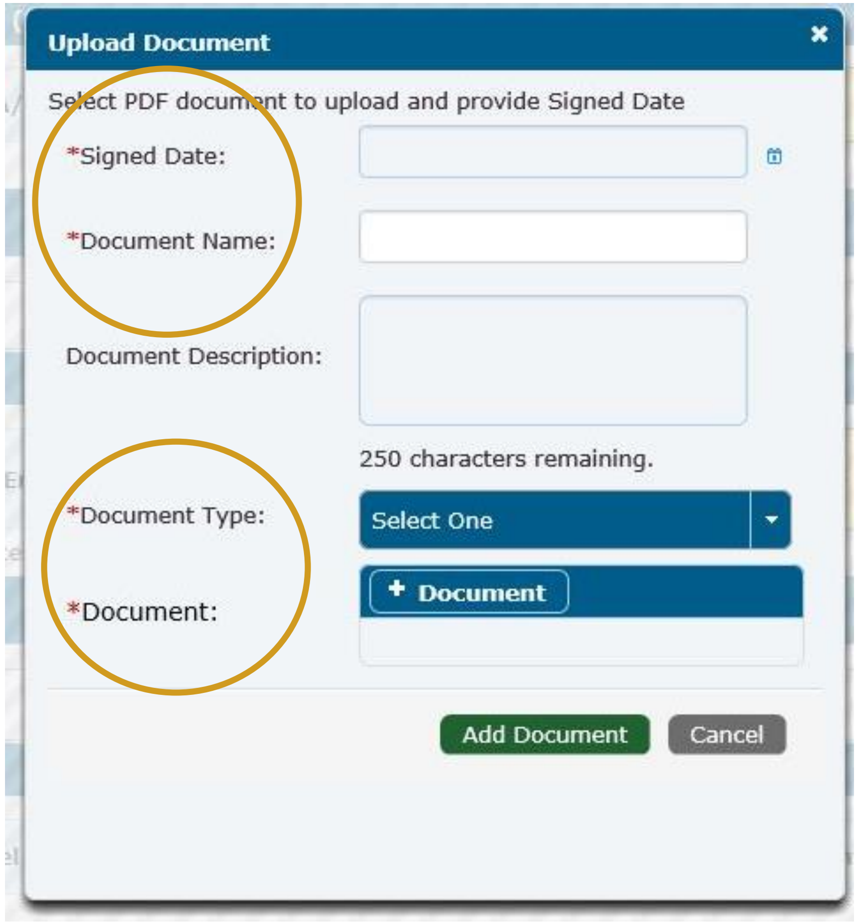
2. Select the green ***Add NDA/NDS*** link.

Add NDA/NDS Upload Document

The NDA/NDS must be a PDF file. The following are mandatory fields that must be entered.

Steps:

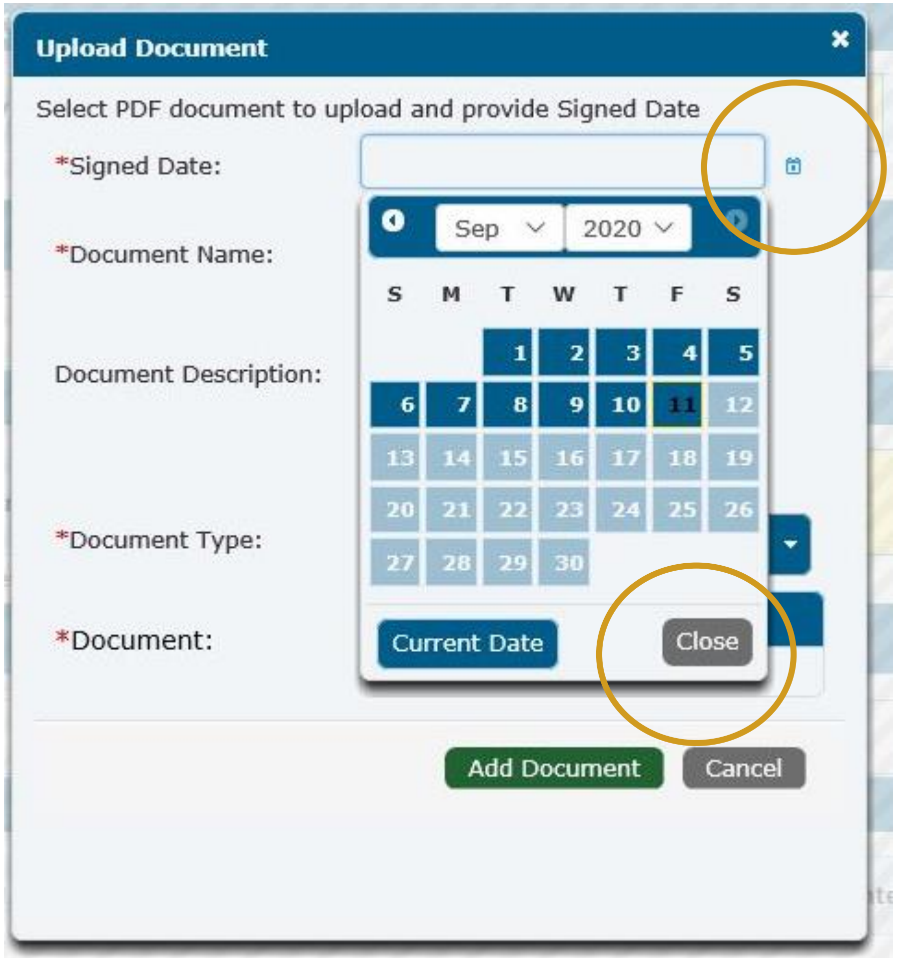
- Enter the **Signed Date** of the NDA.
- Enter the **Document Name.**
- Select the **Document Type** - click the drop down arrow and select ***NDA.***
- Select **Document** – Select PDF.



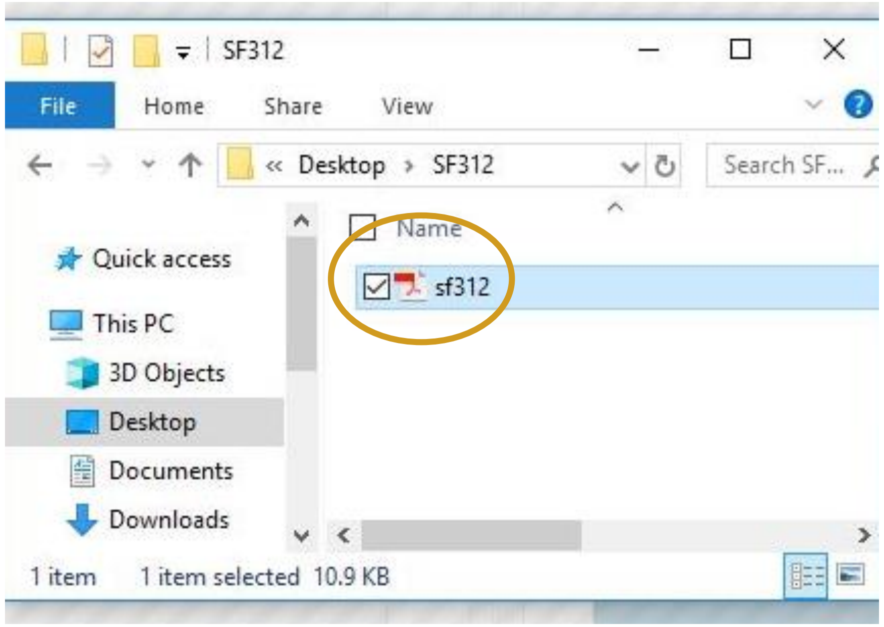
Add Signed Date

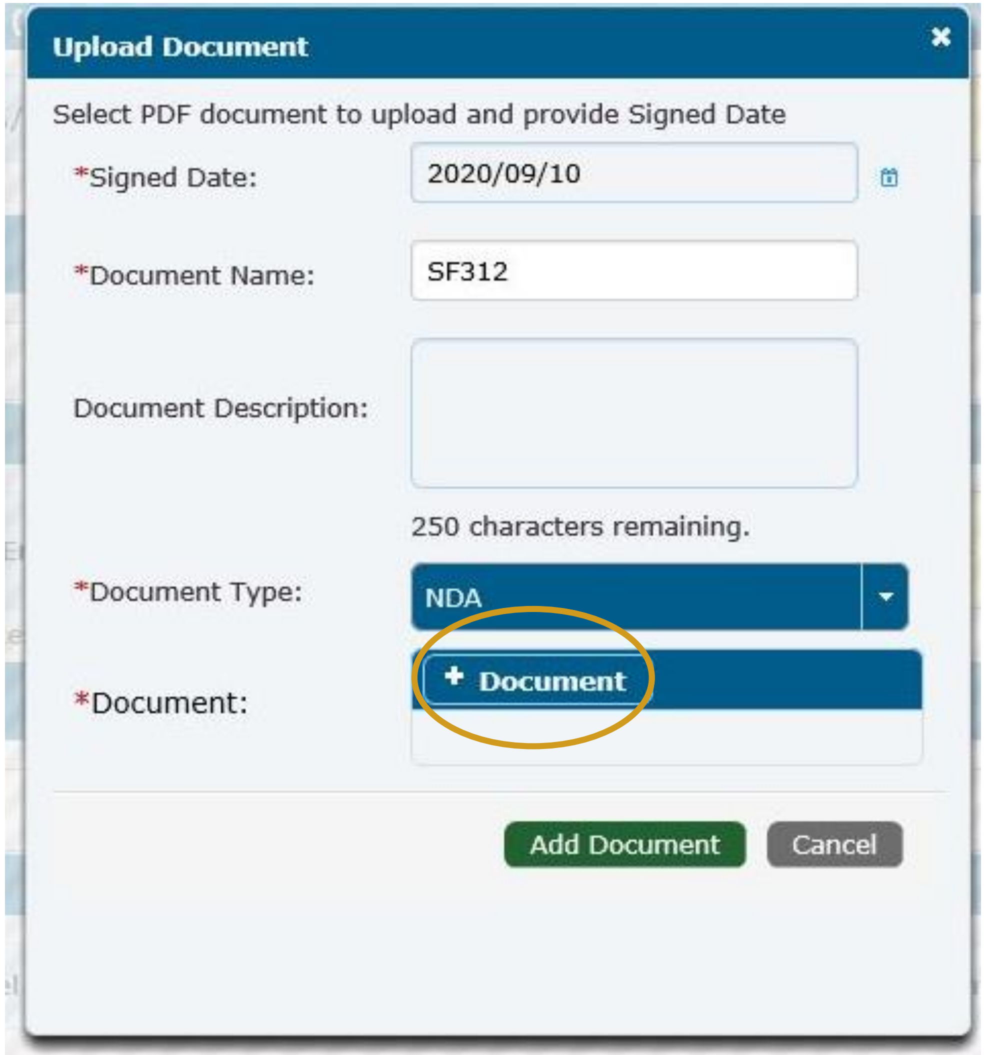
To add the **Signed Date** click on the calendar icon in the pop up **Upload Document.**

Select the **Signed Date** of the NDA and select *Close*.



Upload Document

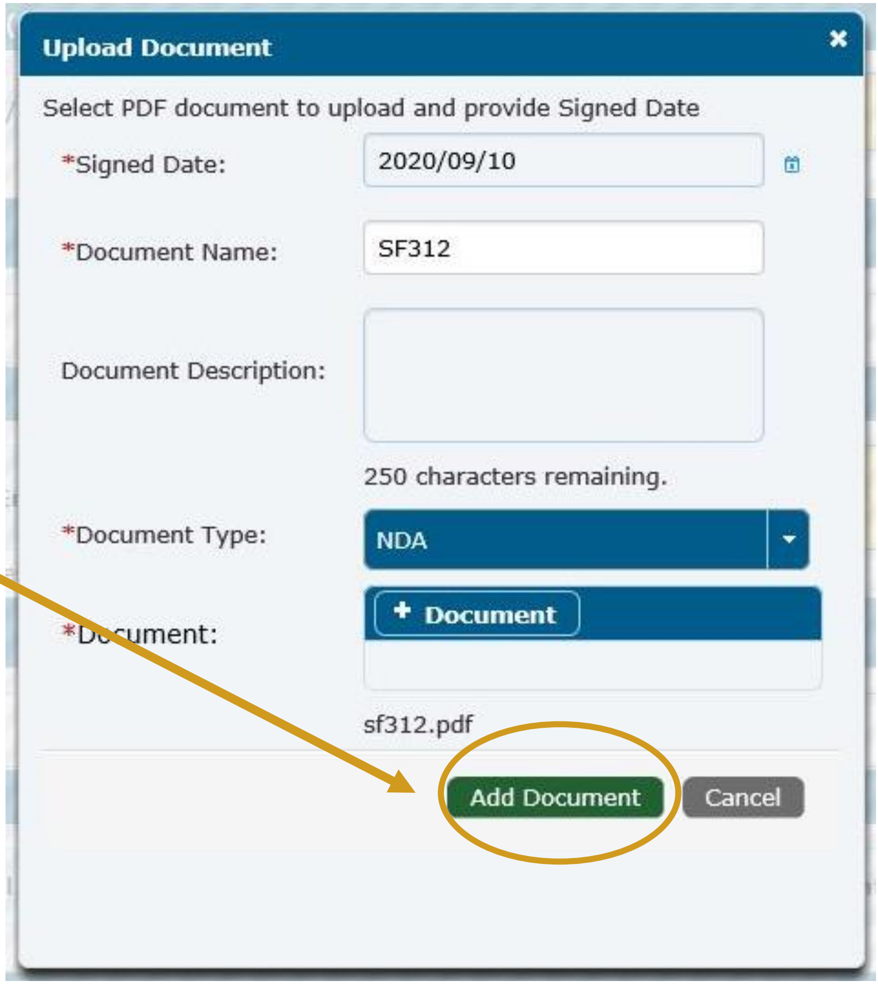




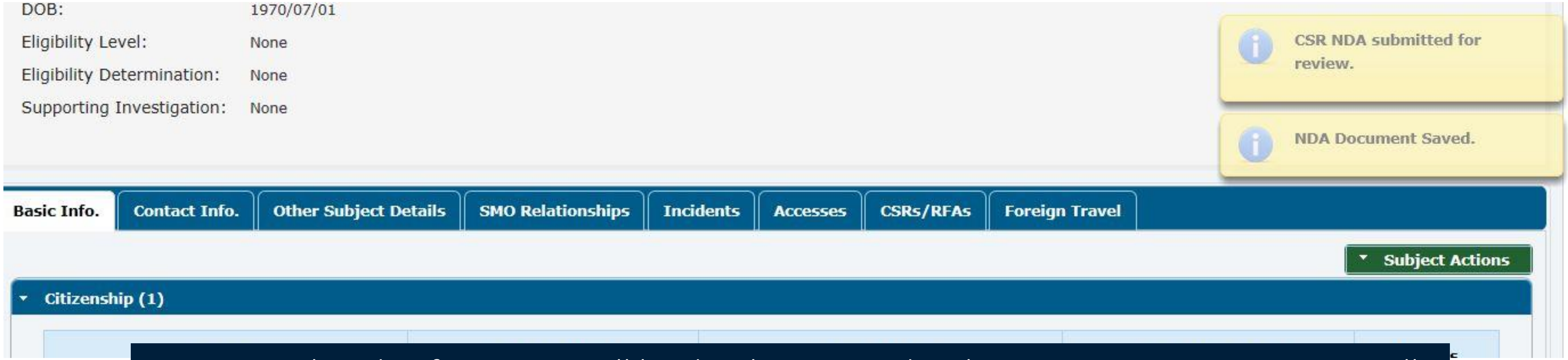
Click on **Document** and select the PDF to upload.

Add SF312

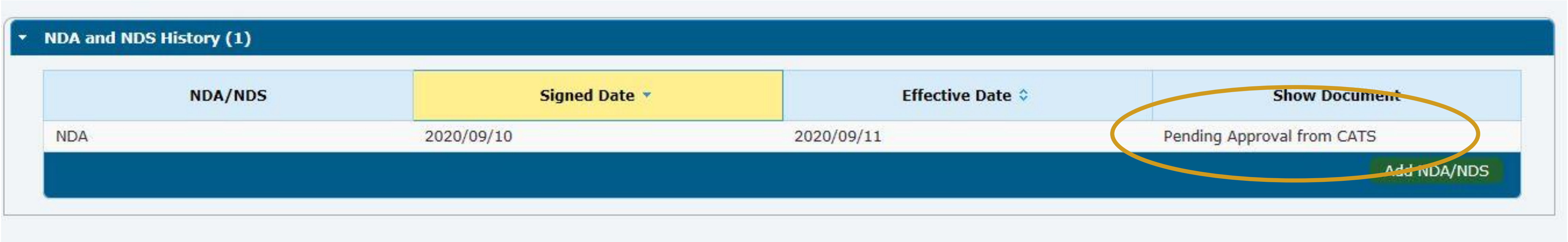
When the document is uploaded it will show in the box, then select *Add Document*.



Subject Basic Inform: NDA/NDS History



Once completed, information will load as history under this section. Status message will appear under the NDA/NDS History section - *Pending Approval from CATS*.



Approved/Reject NDA

- When a Security Officer adds an NDA or NDS document while granting a new access, JVS automatically sends an NDA/NDS Review task to CATS.
- The VROC Industry Process Team reviews the NDA/NDS and either approves or rejects, and if the NDA/NDS task is rejected/revised, the Security Officer must revise the task before resubmitting. If rejected, a message in the **Task Inbox** will appear. **Task Inbox** link is in the **Communications** control panel.
- If the NDA/NDS task is approved, the task will close and JVS users will be able to view the NDA/NDS document on the Accesses sub-tab in JVS.

ACCESS MANAGEMENT

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Subject Details

If you typed in the SSN correctly the **Subject Summary** will show.

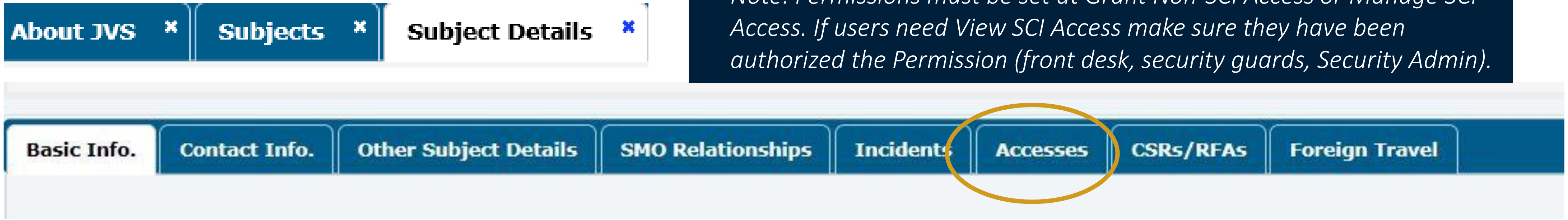
Select ***Subject Details***.

Scenario: In this case there is an open investigation but no SF-312/Non Disclosure Agreement in the subject's record and the subject can not be granted temporary (interim) access until a SF-312 is uploaded.

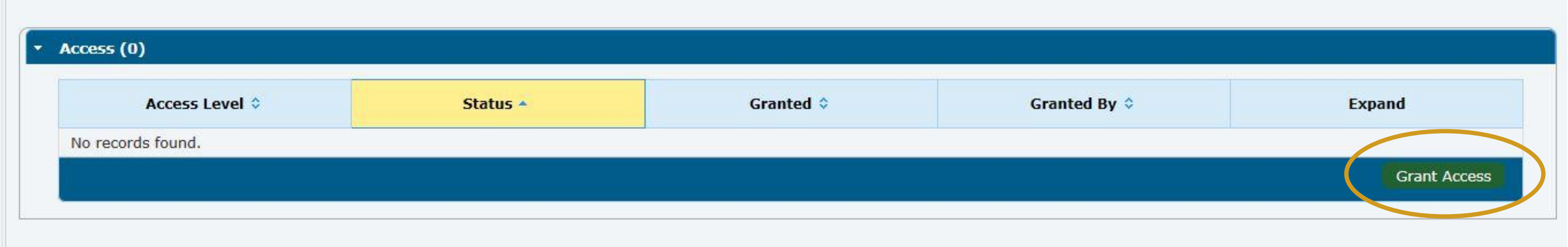
Subject Details tab appears.

Subject Details: Grant Accesses

Note: Permissions must be set at Grant Non-SCI Access or Manage SCI Access. If users need View SCI Access make sure they have been authorized the Permission (front desk, security guards, Security Admin).



1. Under the **Subject Details** tabs - select **Accesses.**

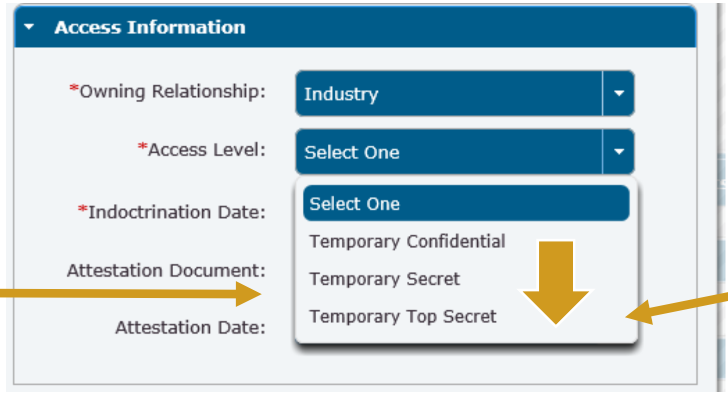


2. To grant access to a subject, click on the ***Grant Access*** button in the Accesses sub-tab. A pop-up window called **Grant New Access** opens.

Industry: If Access was granted at the Secret level based on Interim Eligibility, no action required when Final Favorable Determination made by DoD CAF.

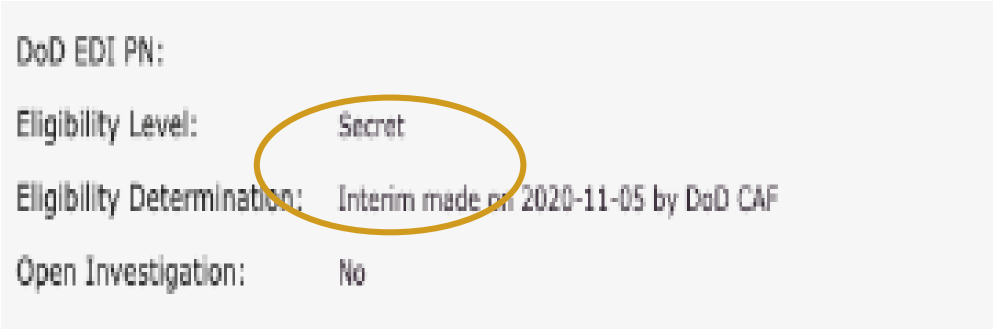
Access Information: Temporary/Industry Access

- Next, select **Access Level** – click the drop down arrow and select the applicable level:
  - Temporary Confidential
  - Temporary Secret
  - Temporary Top Secret
  - Secret
  - Top Secret…



Scroll down to find level

- **Military** and **Agencies** can grant "Temporary" access while waiting for an investigation to close and final adjudication determination.
- **Industry** – "Secret/Top Secret" access can be granted if the supporting Interim determination is posted by VROC.
- **Reminder:** Industry is authorized NATO or other special access levels (see NIPSOM) with an Interim Top Secret Eligibility determination.



Temporary Secret (Interim) Access

Once access is established, the Access subtab will show the Type (Level), Status, Granted (date), and Granted By (SMO), and Subject Category.

Military and Agencies

Accesses

Type	Status	Granted	Granted By	Subject Category	Expand
Temporary Secret	ACTIVE	2020/11/05	DISS	Academy	

To expand the Access box click on the blue arrow to see Associated Relationships

Industry

Accesses

Type	Status	Granted	Granted By	Subject Category	Expand
Secret	ACTIVE	2020/11/05	IWORKS-TEST-1	Industry	

Industry Access will be established based on **Interim/Final Eligibility** at the Secret/Top Secret Level based on Reciprocity across the National Industrial Security Program (NISP).

Access is Active and Associated Relationship

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

Access (1)

Access Level	Status	Granted	Granted By	Subject Category	Expand
Secret	ACTIVE	2019/08/05	561P94 - TEKSYNAP CORP	Industry	

Access Information

Indoctrination Date: 2019/08/05

Attestation Date:

Subject Category: Industry

Attestation Document:

Debrief Information

Debrief Date:

Debrief Type:

Access Removal Reason:

Access Removal Date:

Debriefing SMO:

Debrief Comments:

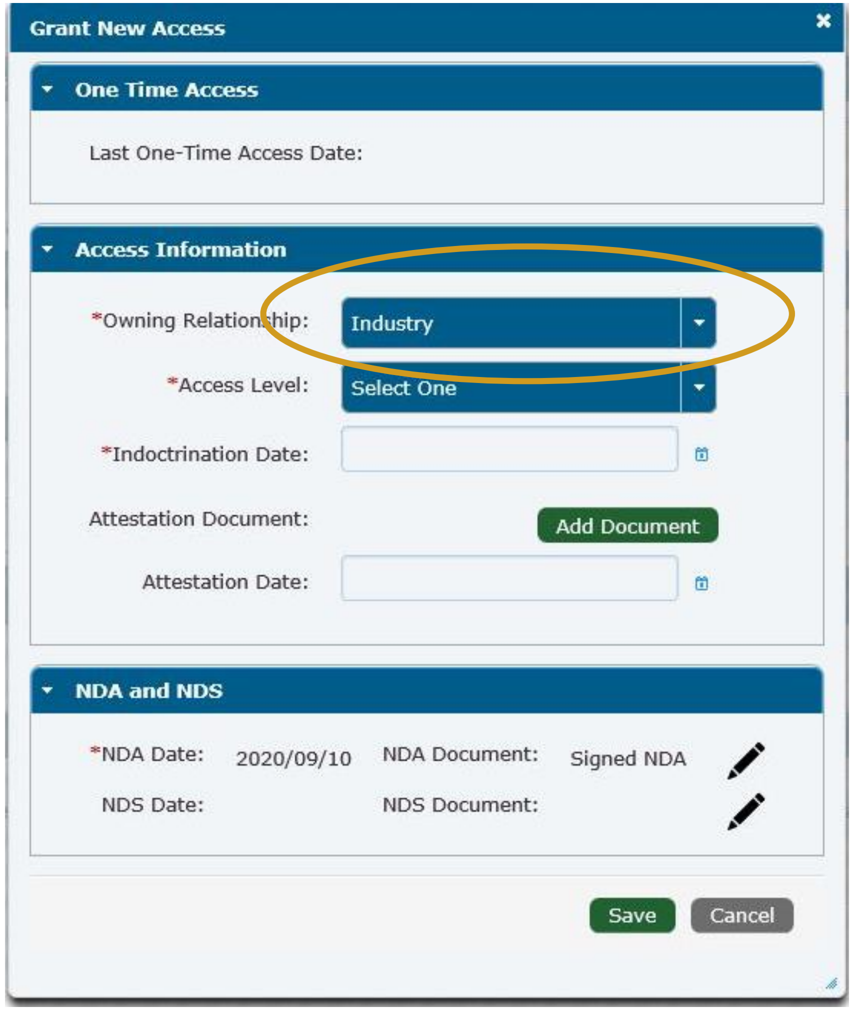
Associated Relationships

Type	SMO Name	Begin Date	ICC	End Date	Term. Reason
Owning	561P94 - TEKSYNAP CORP	2019/07/30			

Grant Access

Access Information: Owning Relationship

- If the subject has only one owning relationship, the Owning Relationship field is disabled and automatically filled.
  - Otherwise, use the drop-down menu to select an Owning Relationship.
- In this case, **Industry** is automatically displayed.



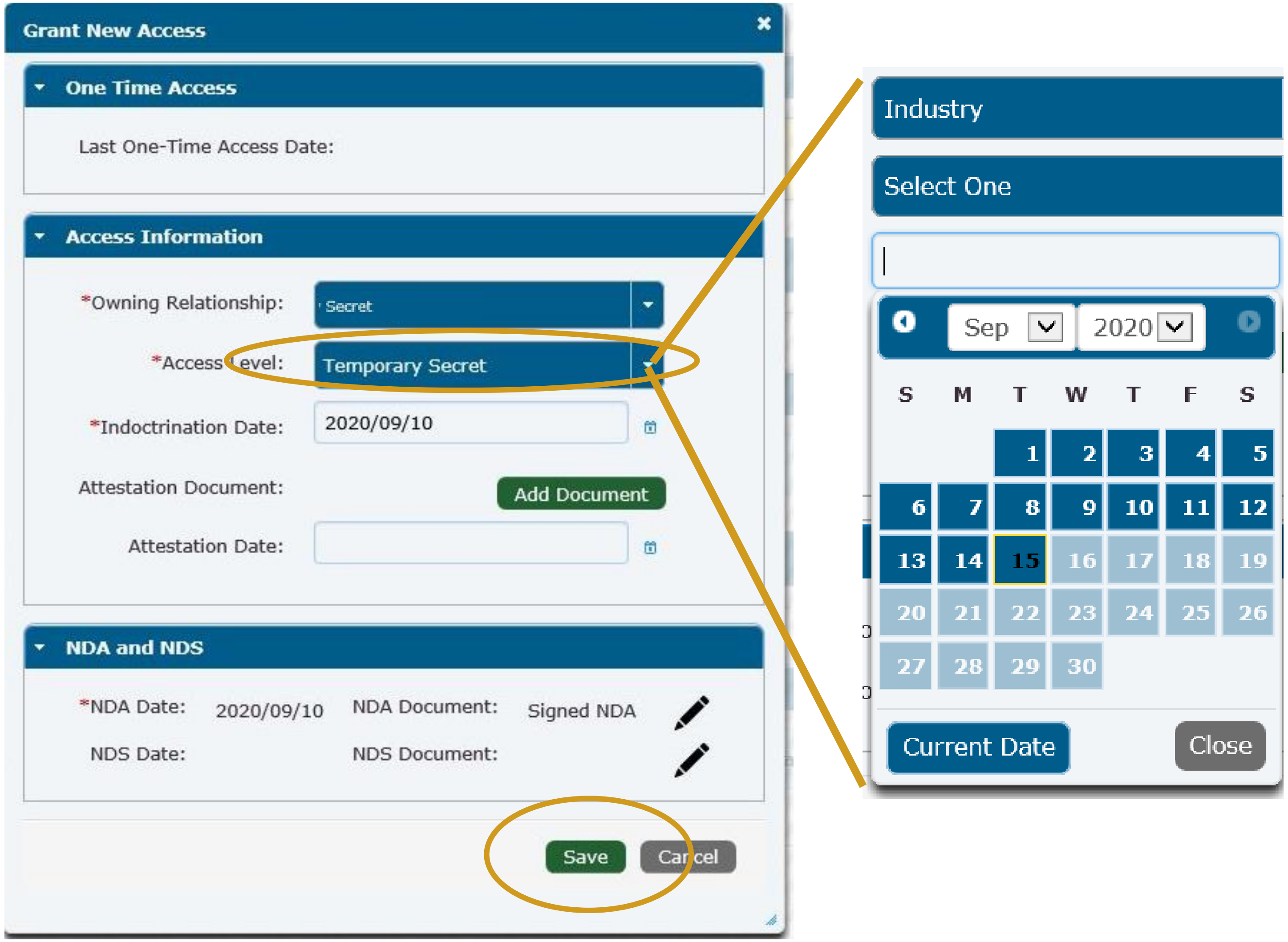
Access Information: Temporary (Interim) Access Level

Add the **Indoctrination date** using the calendar.

NDA date will show under NDA/NDS Section.

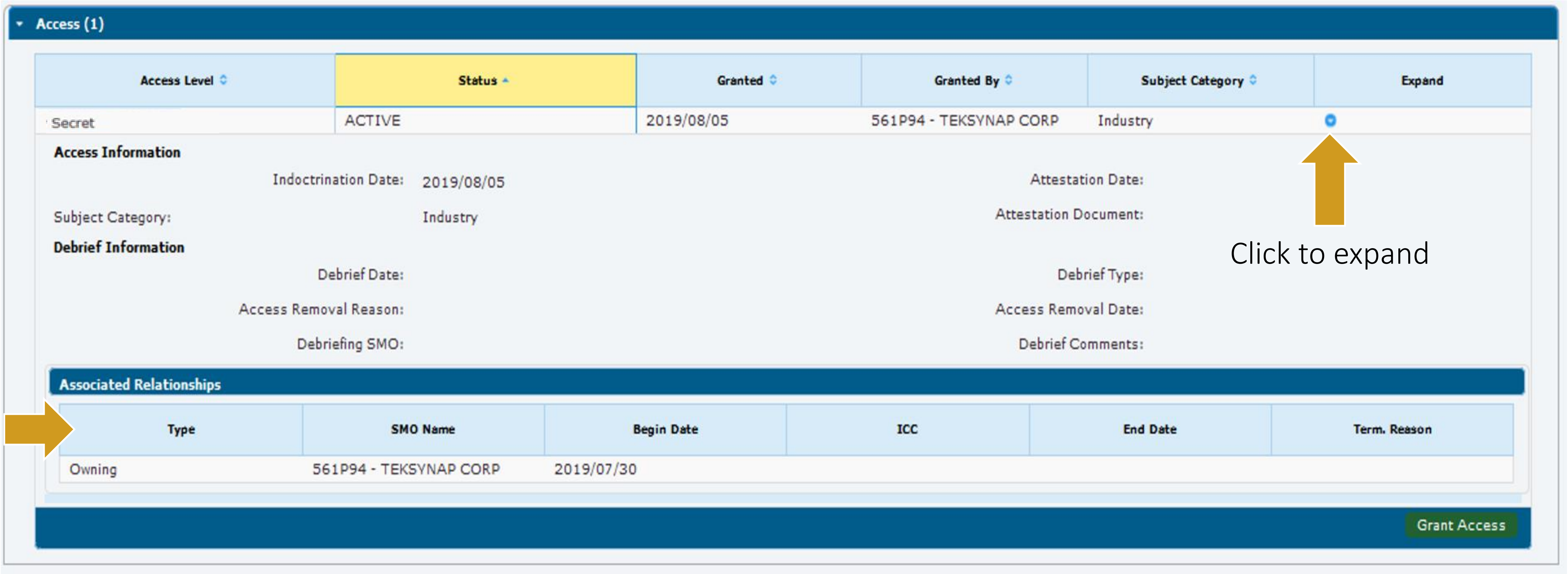
Select ***Save***.

Note: The Attestation Date is required when the Attestation Document has been uploaded, and Access Level selected is Top Secret, it is not required for SCI.



Access Tab: Associated Relationships

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

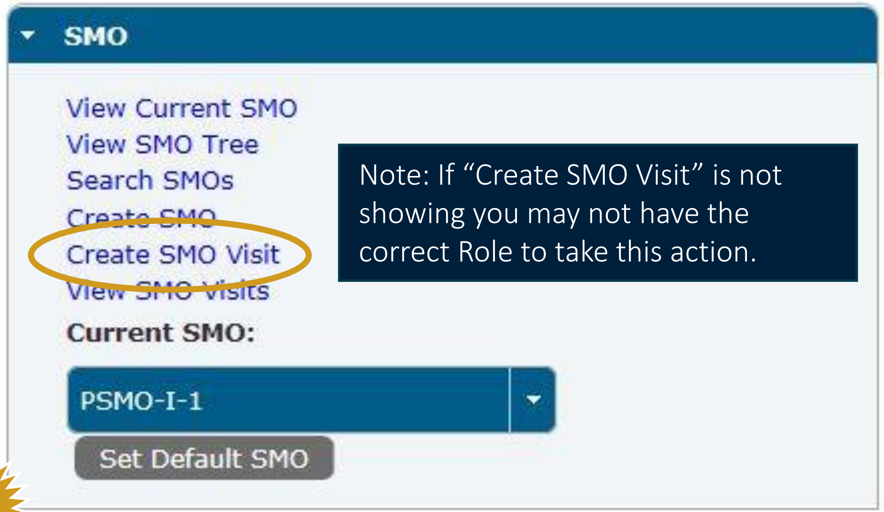


VISIT REQUESTS

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Create SMO Visit

Select Hosting SMO is a required field. Options available **are Current SMO** or **Find Hosting SMO.**



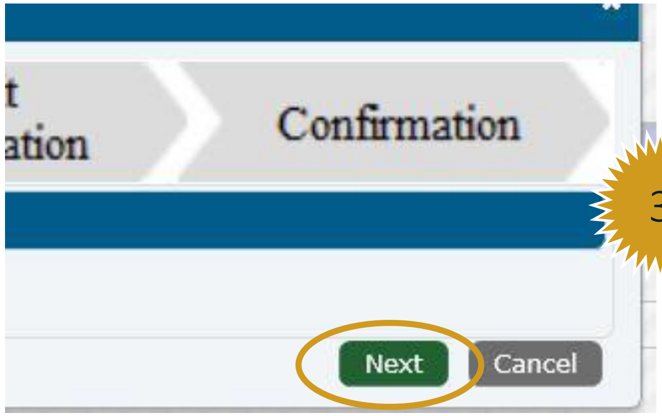
1

Click on ***Create SMO Visits.***

If you have a role for more than one SMO, ensure you are in the correct SMO to submit the visit under.

2

Select ***Current SMO or Hosting SMO.***



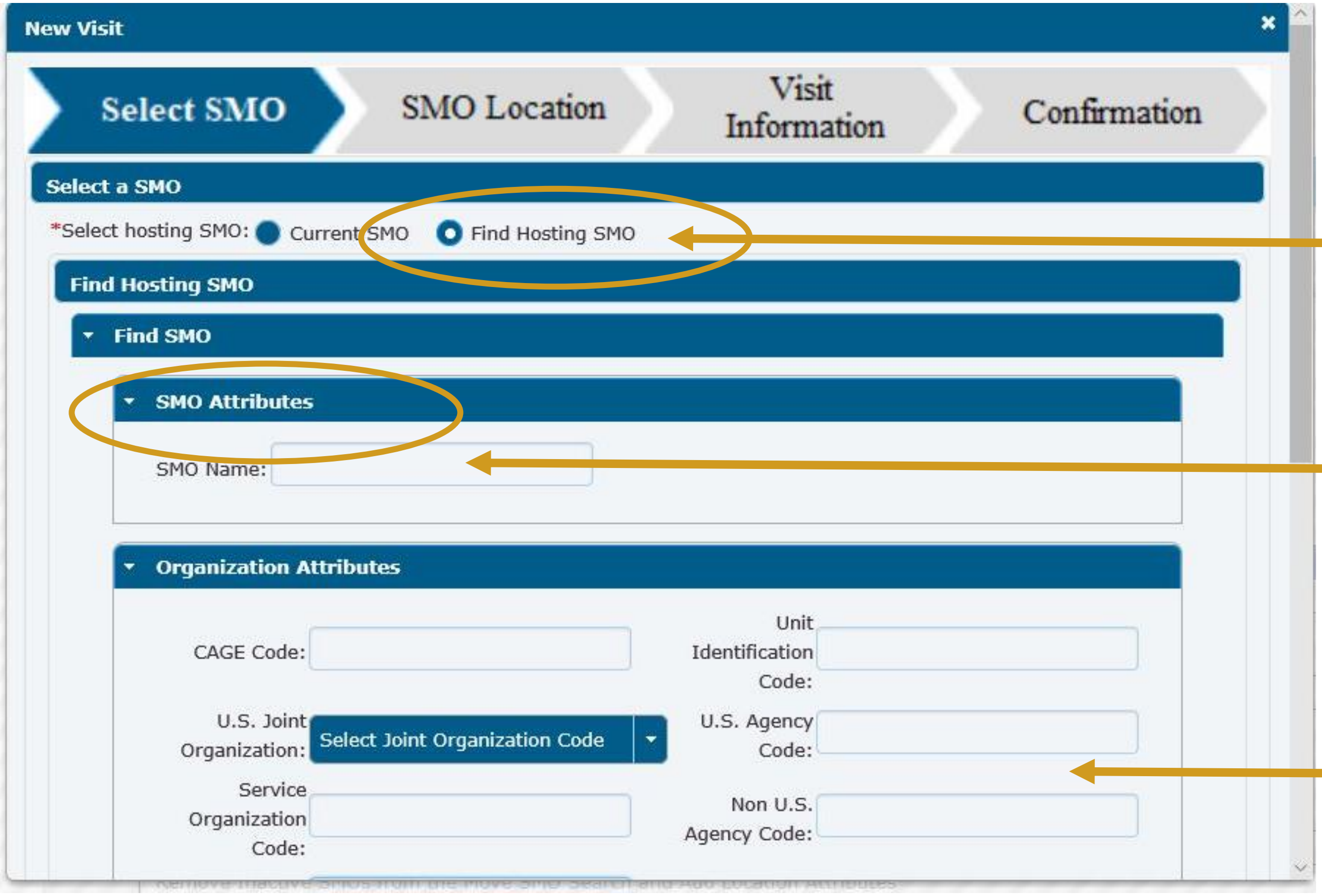
3

Select ***Next.***

SMO Location

Select **Existing SMO Location** and Select ***Next***.

Select SMO: Find Hosting SMO

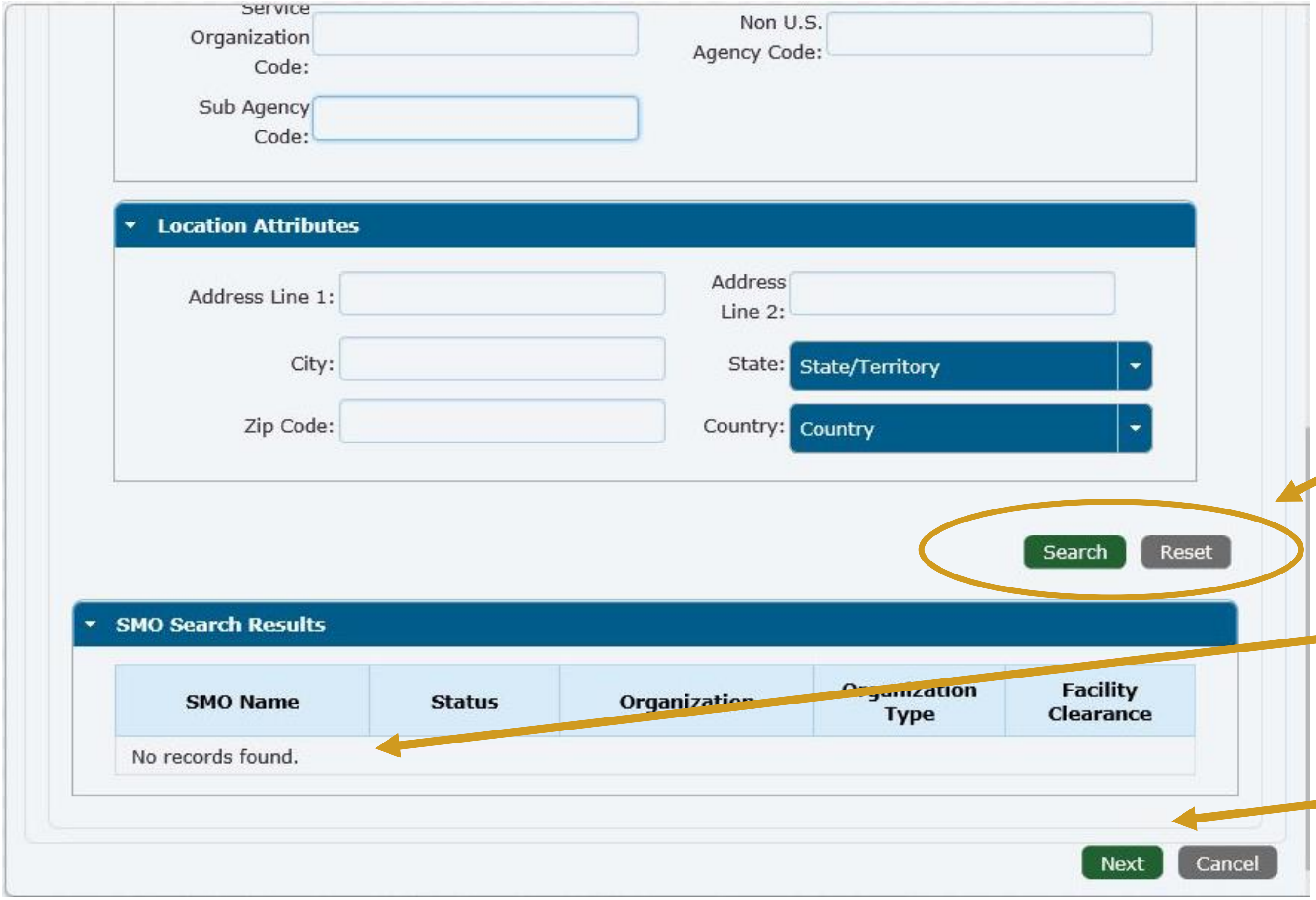


If you are not the Host then you need to find the Hosting SMO.

Select **Find Hosting SMO.**

Use the SMO Attributes to search for the SMO such as SMO Name, Cage Code, Service, Unit Identification Code, etc.

Select SMO: Finding Hosting SMO



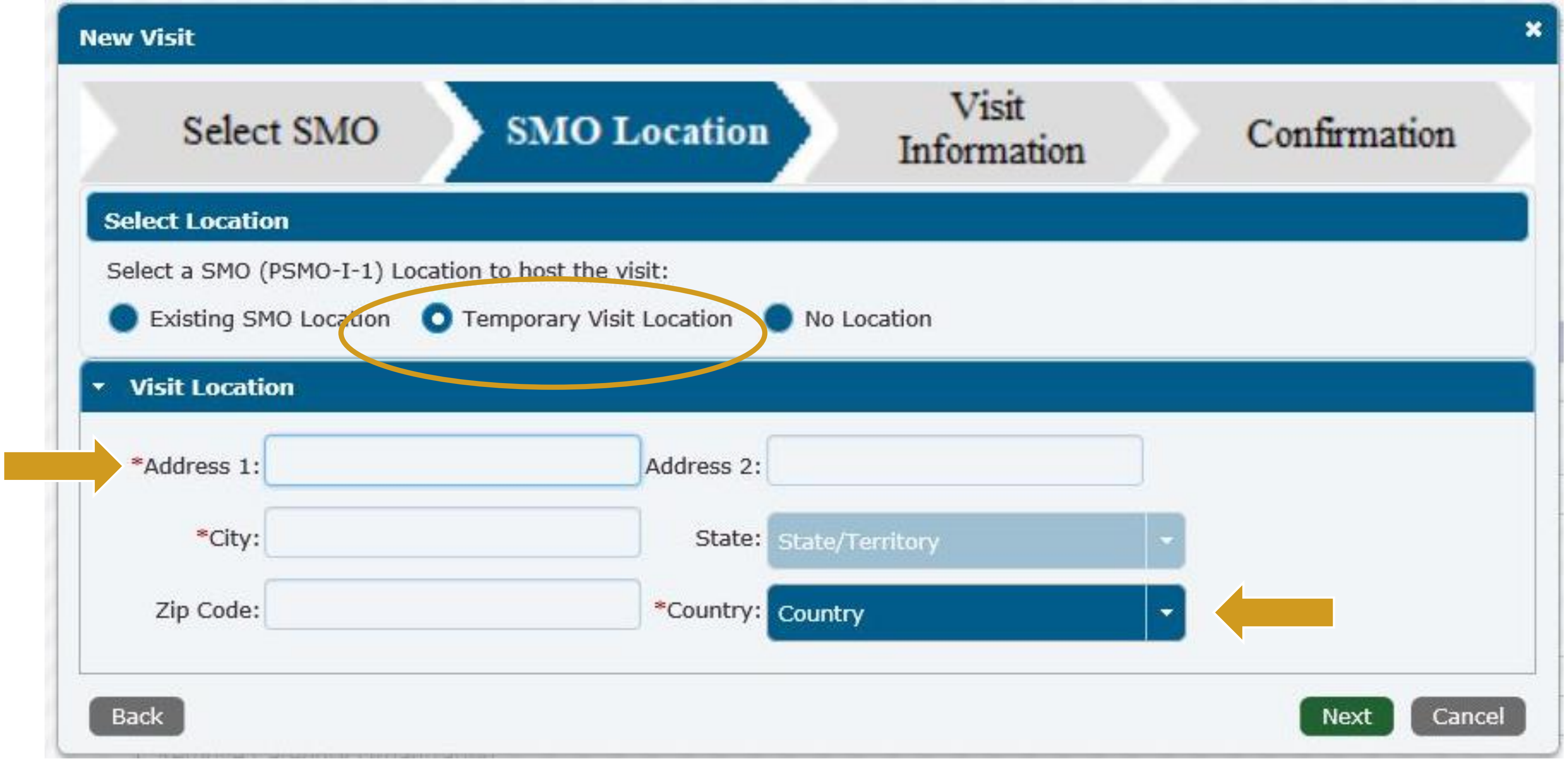
Click on ***Search*** to generate any matching results.

The results display in the SMO Search Results table.

Select the appropriate SMO and Select ***Next***.

SMO Location: Temporary Visit Location

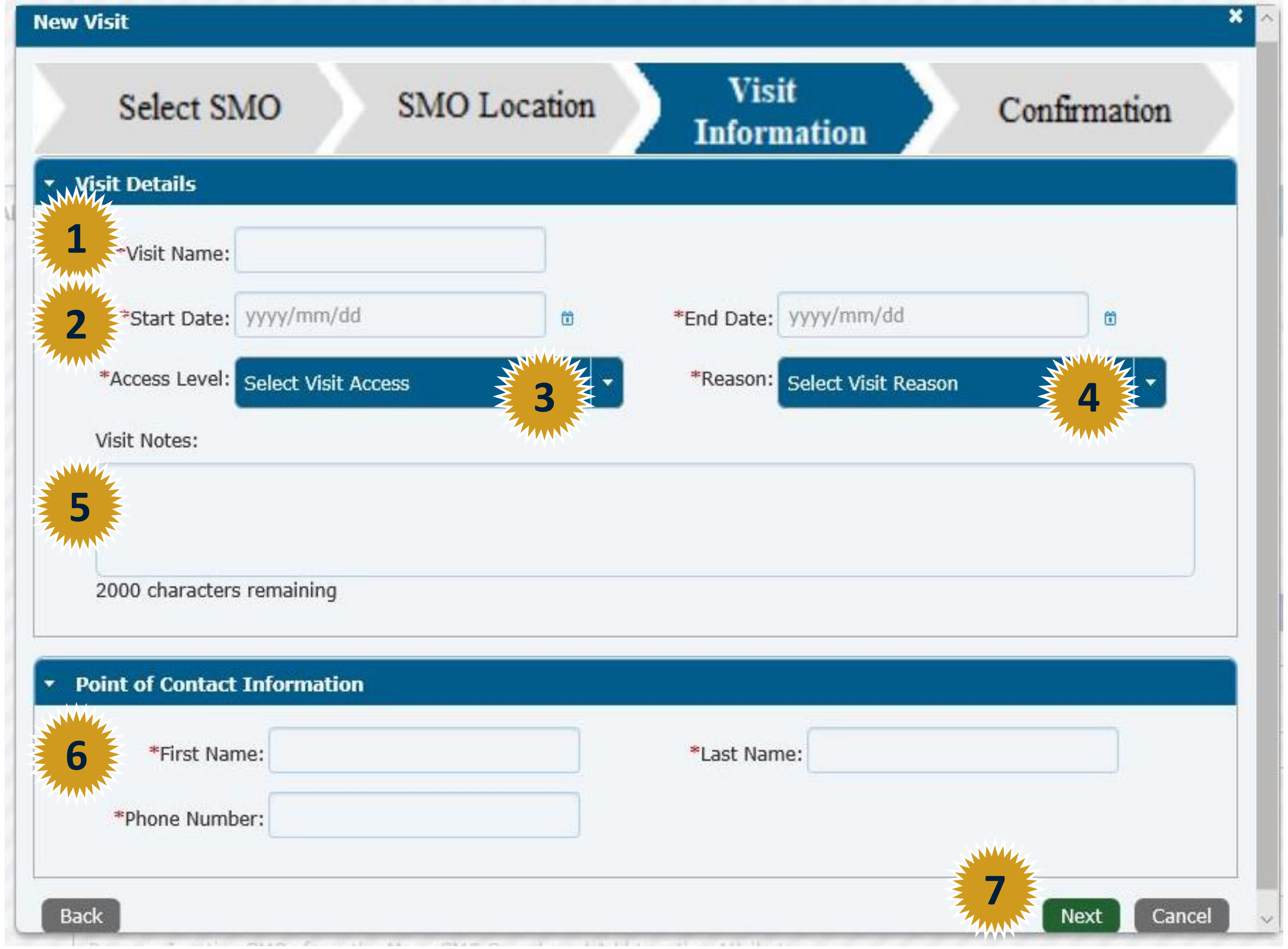
If you select **Temporary Visit Location**, you need to fill in the location fields. Use the drop-down menus to select a State and Country.



SMO Location: Select Existing SMO location

Select the correct **Existing SMO Location** from your options and select ***Next***.

Visit Information



1. Enter **Visit Name**.
   - This is a free text field.
2. Enter **Start Date** and **End Date**.
   - Use the calendar to ensure proper entry however, this information can be manually entered in the DISS approved date format.
3. Enter **Access Level**.
   - Drop-down option contains: None, Top Secret, Top Secret SCI, Secret and Confidential.
4. Enter **Visit Reason**.
   - Drop-down option contains: Inspection, Meeting, Other, Planning Conference, Seminar, Symposium, TAD/TDY, and Training.
5. Enter **Visit Notes**.
   - While this is not a required field this space could be utilized for additional information such as contract being utilized for meeting or other special instructions.
6. Enter **Point of Contact information**.
   - First Name, Last Name and Phone Number are all required fields to be completed under this section.
7. Select ***Next*** when complete.

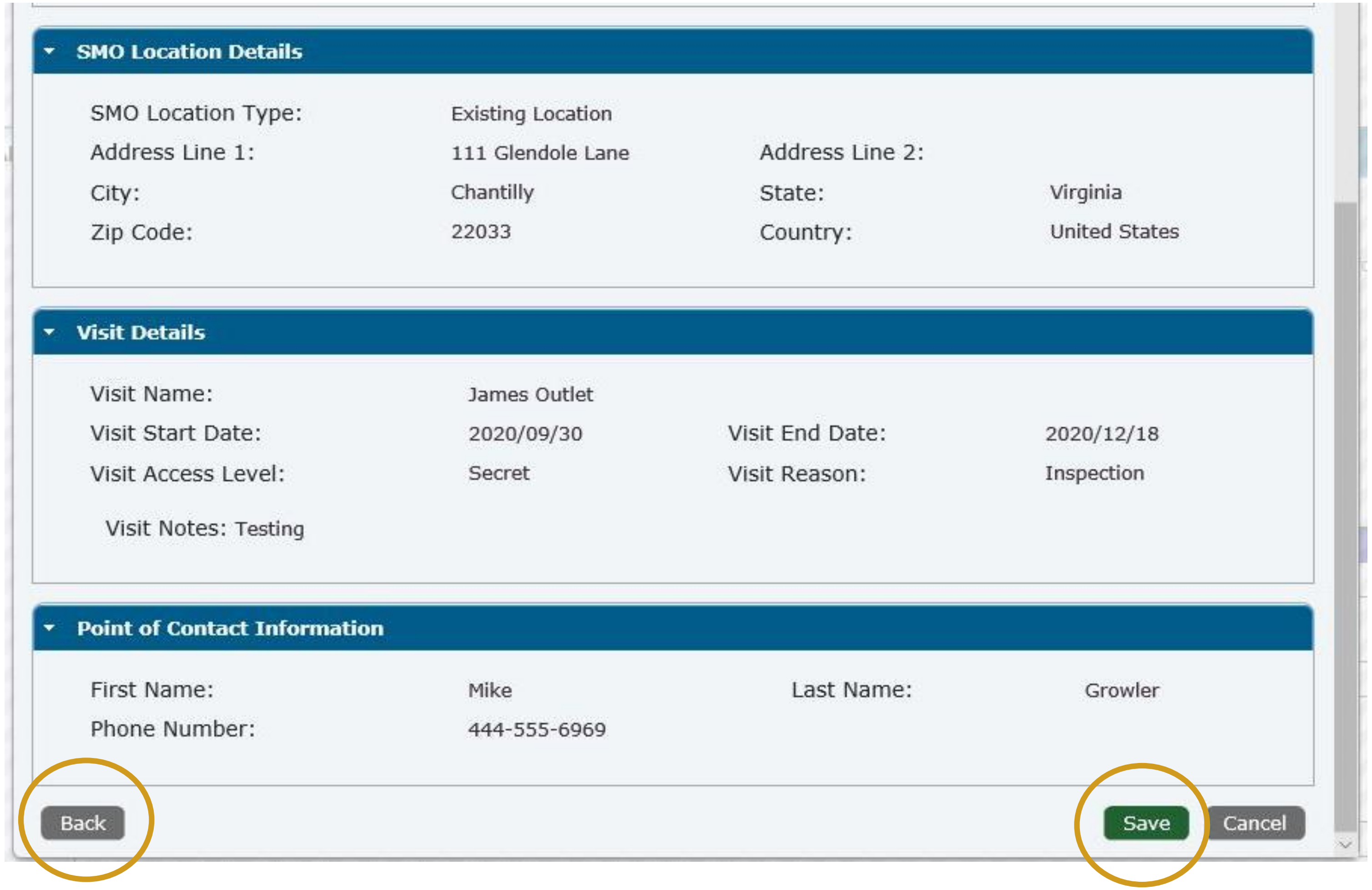
Visit Confirmation (continued)

After you selected *Next* the Visit Confirmation Details appear.

Review the **Visit Details** to confirm they are correct.

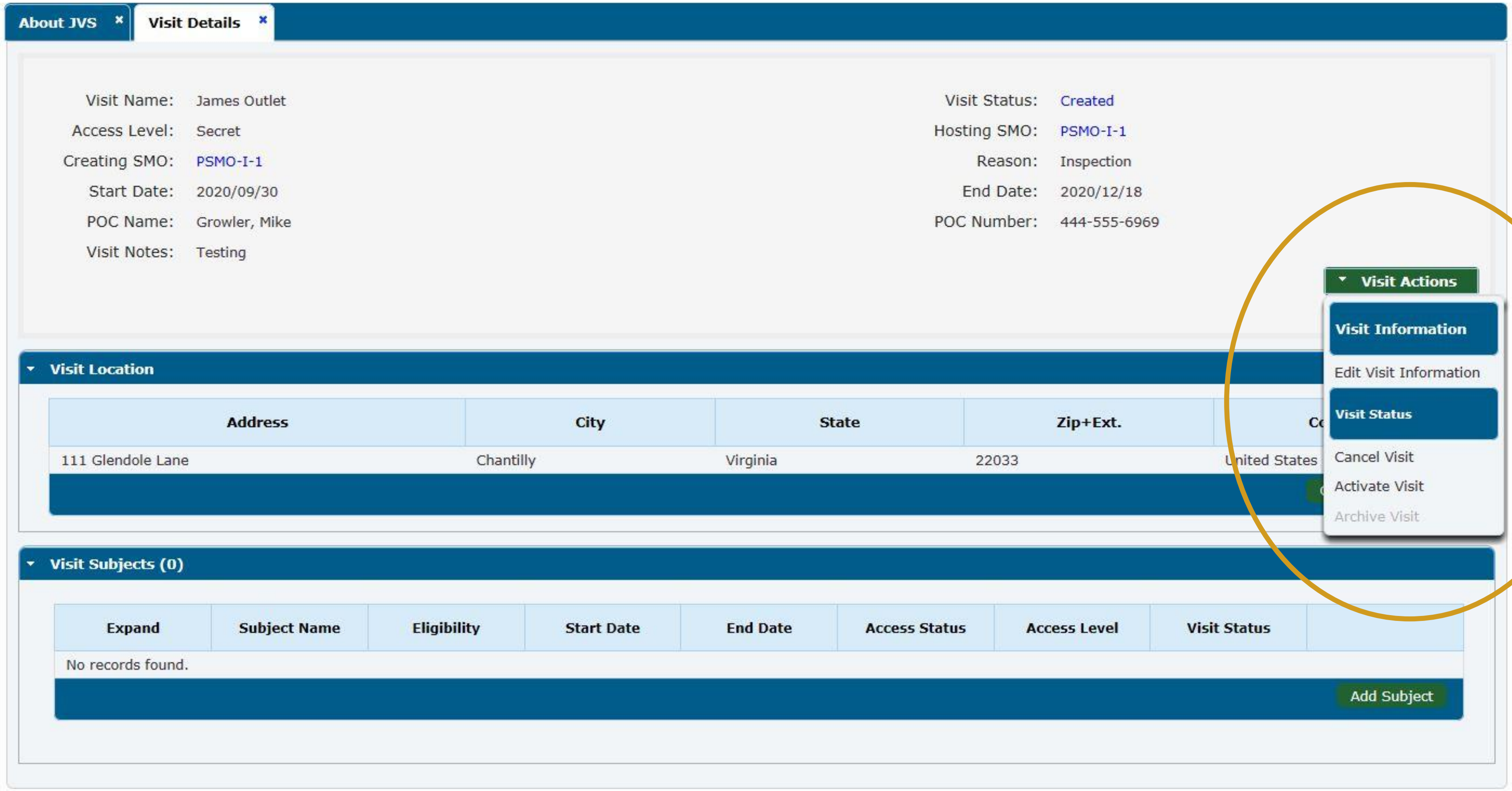
If the **Visit Details** are incorrect select ***Back*** to correct.

If the **Visit Details** are correct select ***Save***.



Visit Actions

- Once you have saved the Visit information it will appear in the **Visit Details Tab** where you are able **Activate Visit** and take other actions: **Visit Actions, Change Location** or **Add Subject.**
- Under **Visit Actions** menu you can **Edit Visit Information** or change **Visit Status** to **Cancel or Activate.**
- To activate an existing **Visit**, click on the **“Visit Actions”** drop-down menu and select **Activate Visit.**

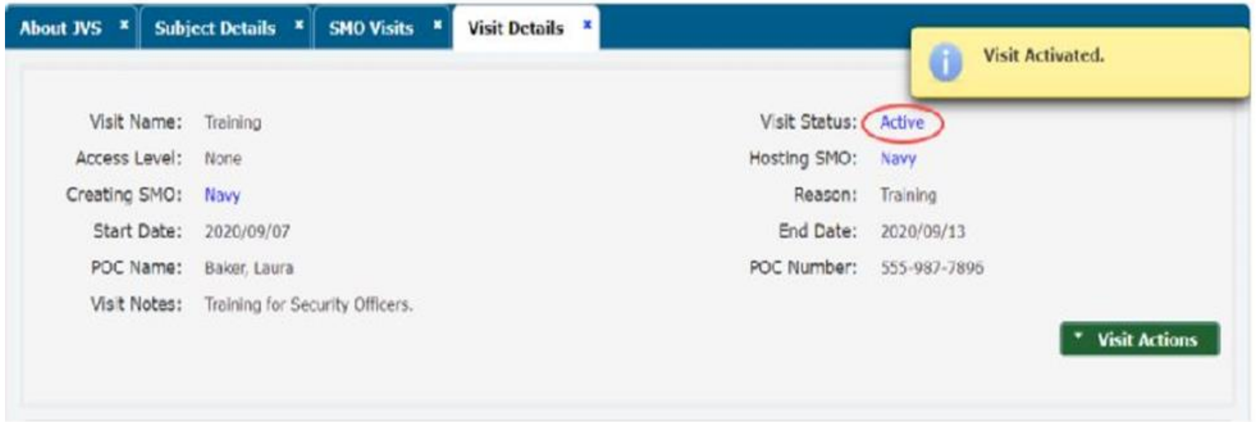


Visit Actions (Activate)

A pop-up window called **Activate Visit** opens.

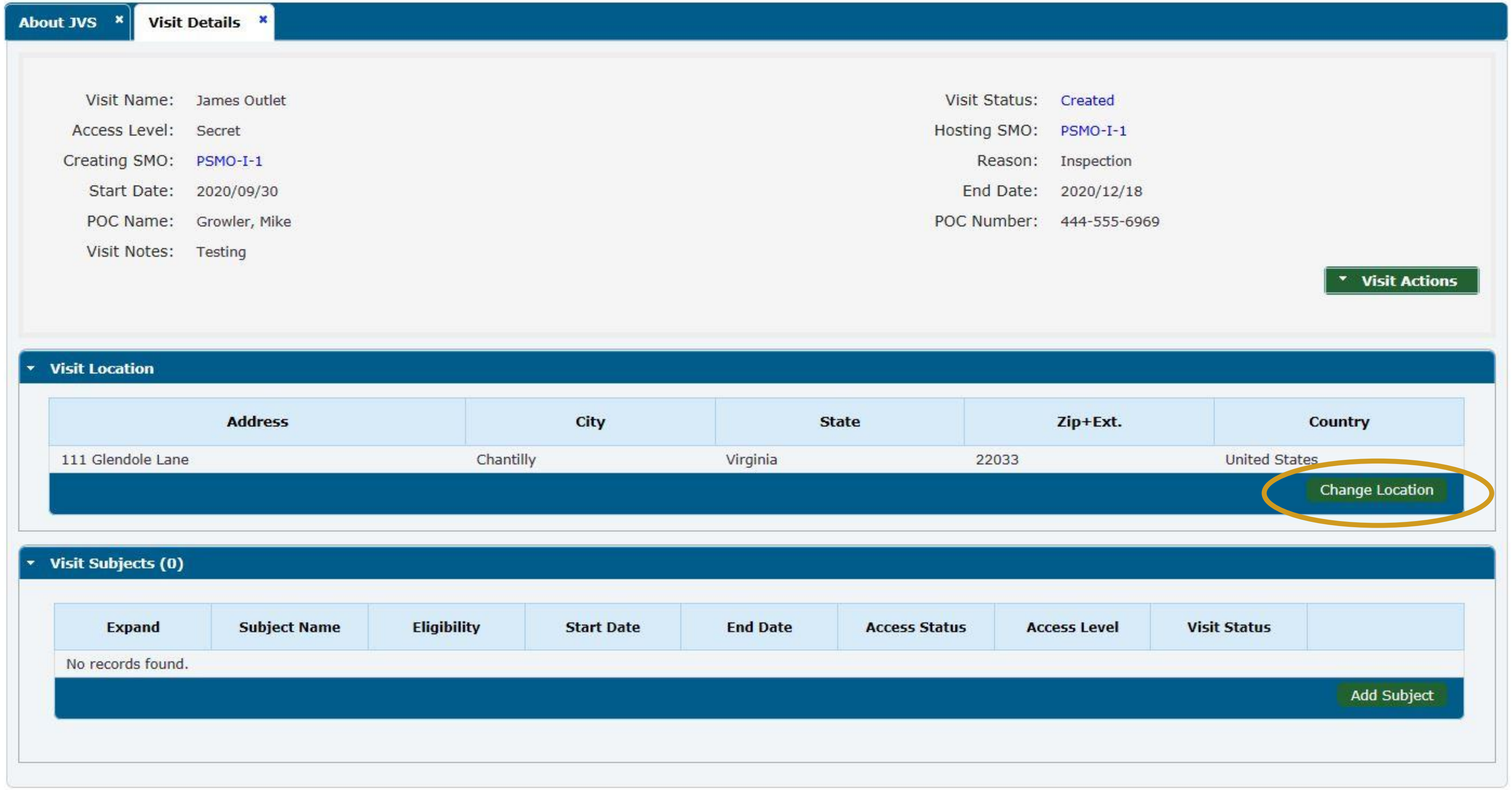
Select **Yes** to finish activating the visit, or select **No** to cancel the activation.

Once activated, the status of the visit changes to **Active** and you receive a confirmation message.



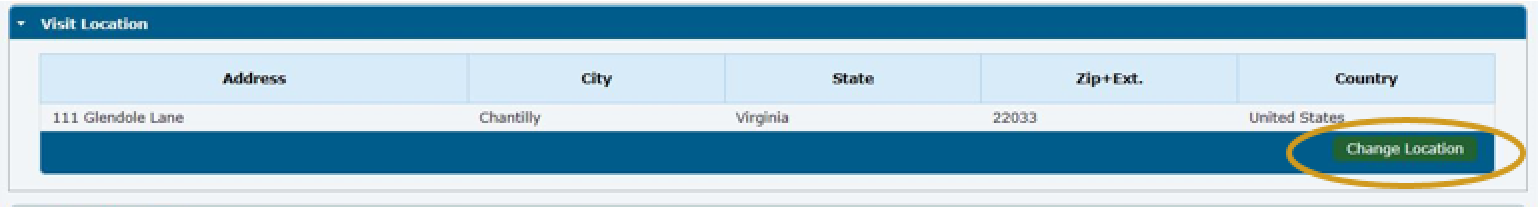
Change Visit Location

If you need to change Visit Location select *Change Location*.



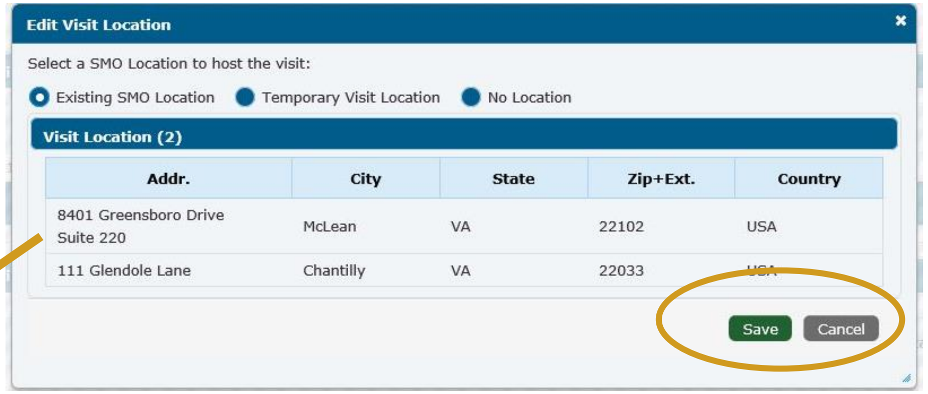
Edit Visit Location

If you need to change Visit Location select ***Change Location***.

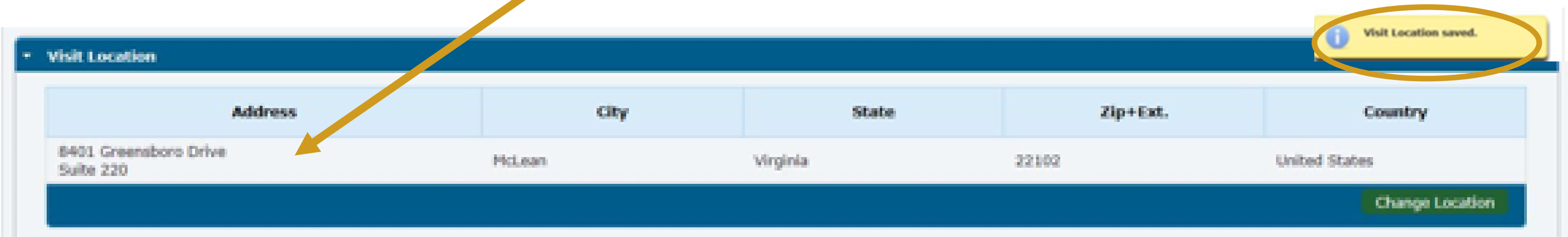


The **Visit Location** box appears with the same options you had before when you established the Visits Request.

When completed with the edits select ***Save*** or if no changes were made or you want to discard those changes select ***Cancel***.

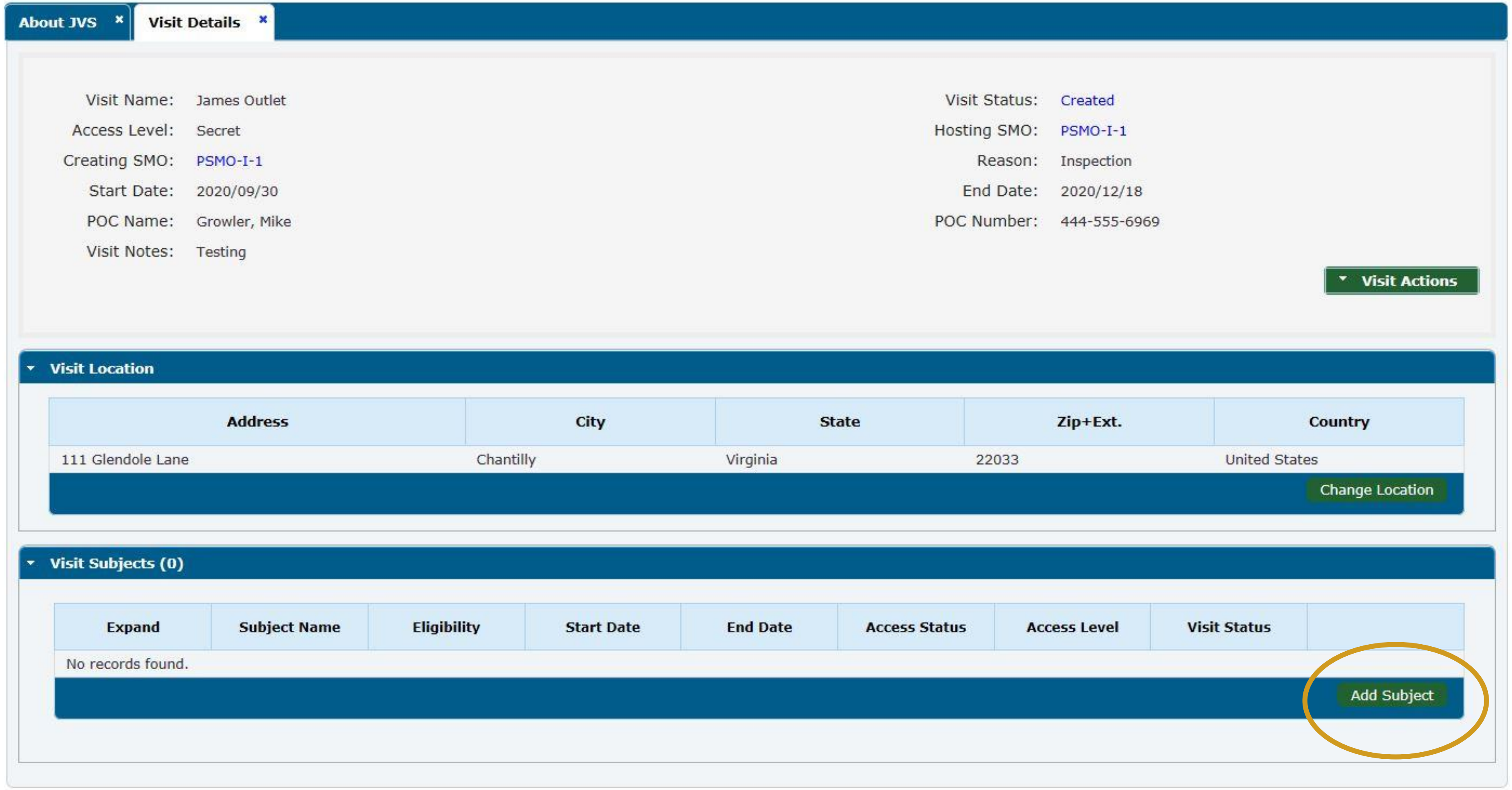


If the **Visit Location** is changed and saved a yellow box will confirm **Visit Location saved.**



Visit Details

Now you need to add visitors to the request by selecting *Add Subject*.



Add Subject to Visit

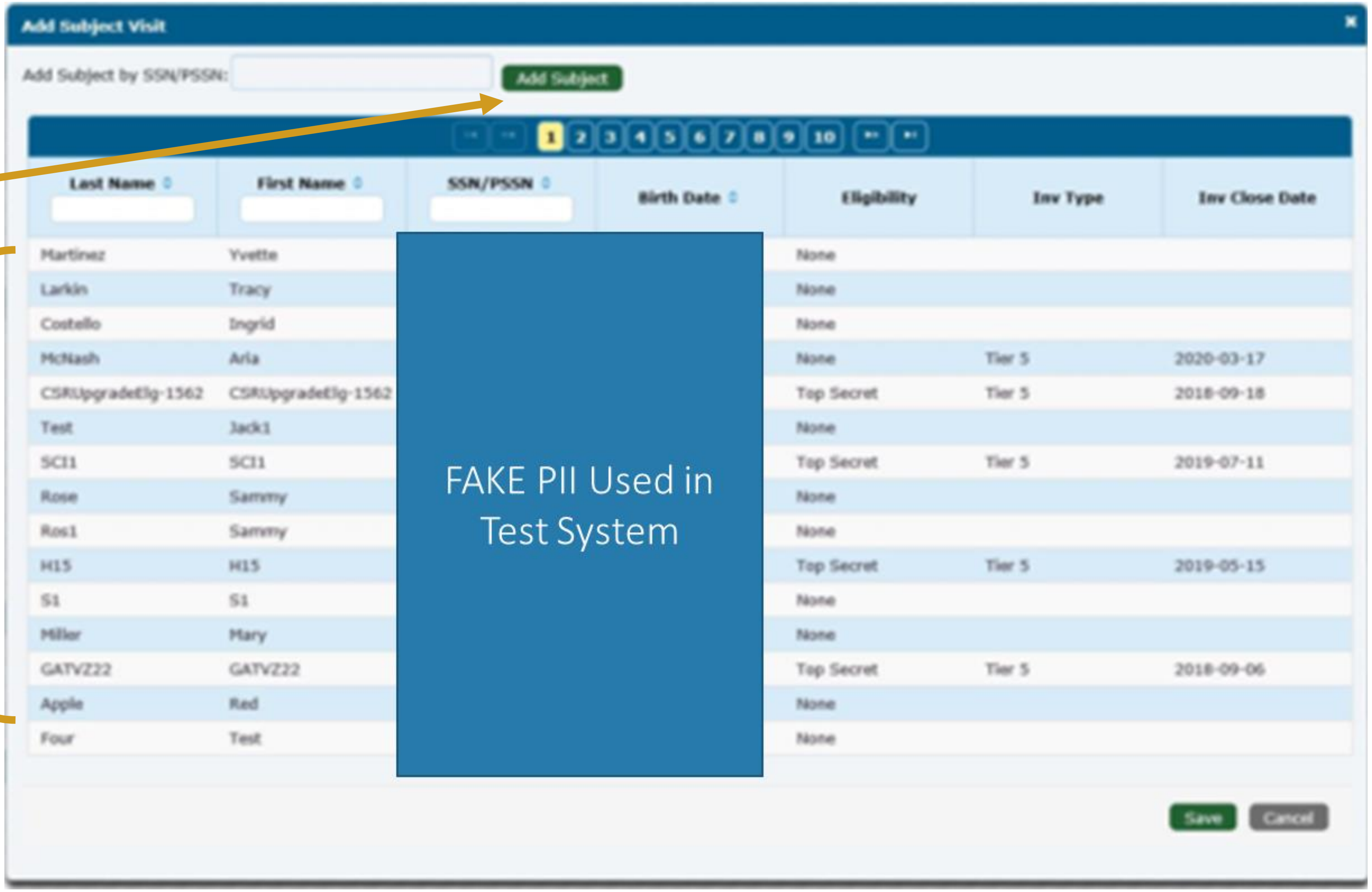
You have two options to add a Subject to the Visit.

Type in the Social Security number and Select *Add Subject.*

Or

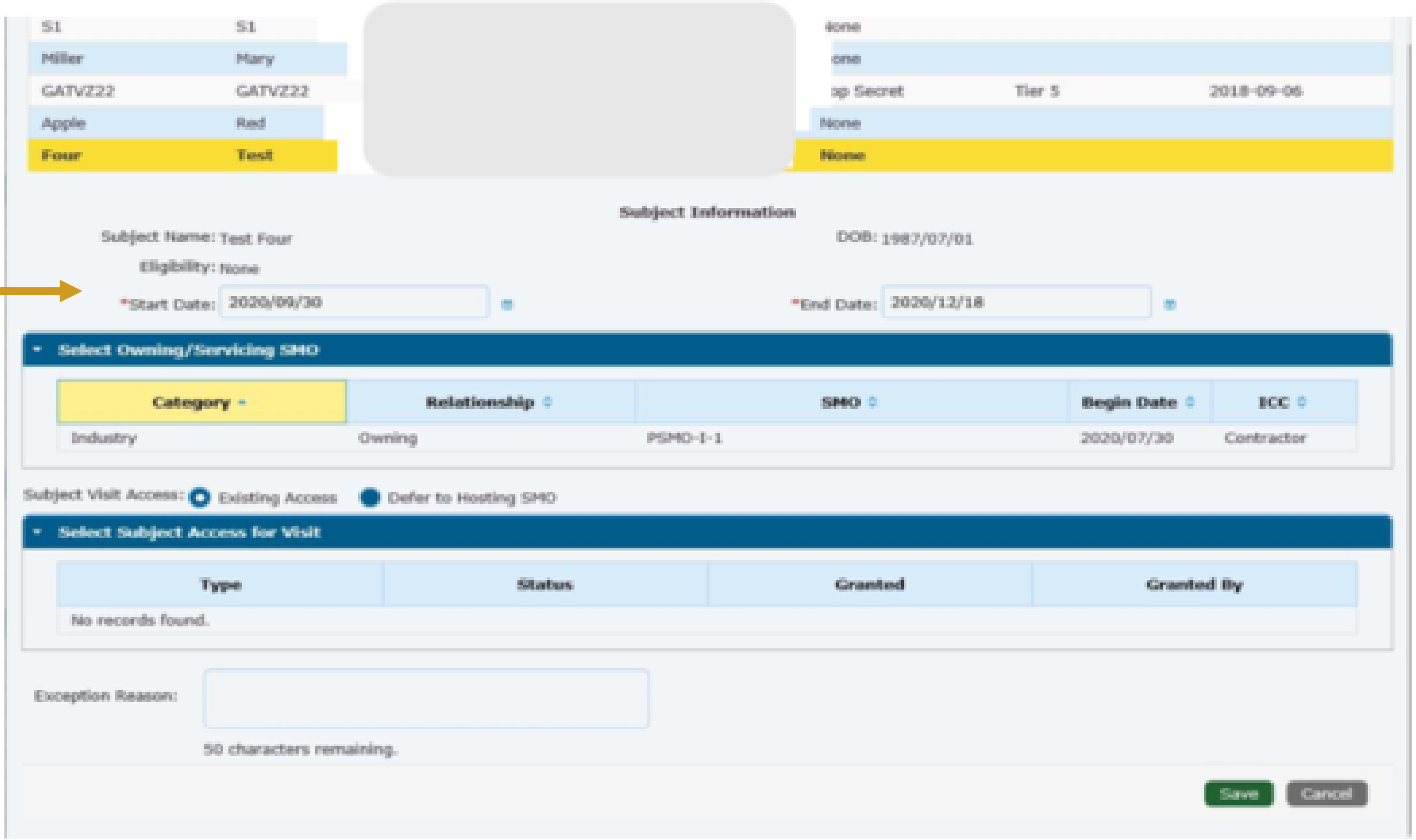
Scroll through the subject's for the Current SMO appear within the table. The entire subject list will populate.

Note: Not all subjects in the list will meet the conditions to be added to the visit.



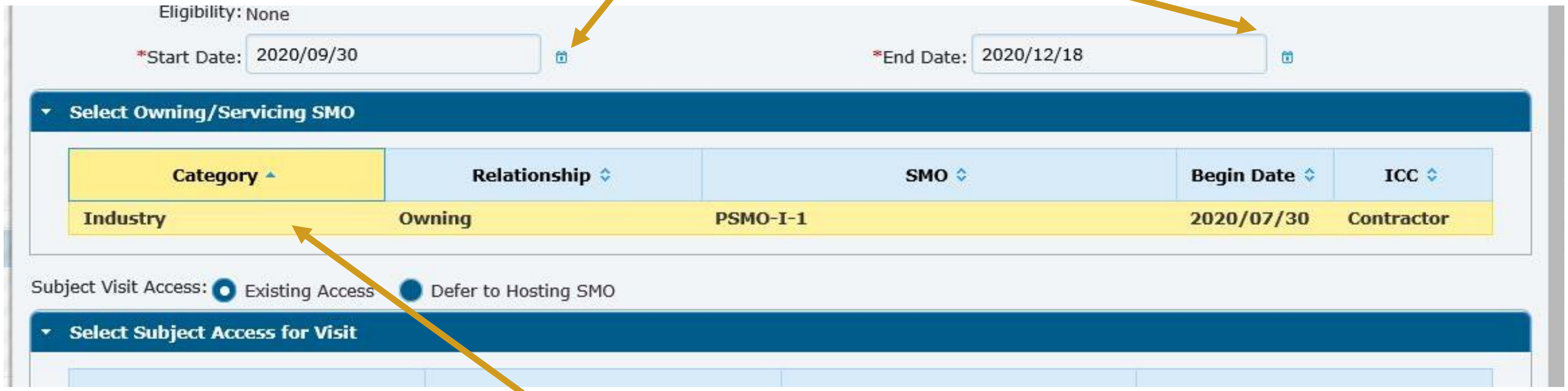
Select Subject to Visit

Selecting a subject from the table will display their information below.



Select Owning or Services

Select the calendar icon to select a **Start Date** and **End Date** The selectable dates will filter based on the dates of the visit.

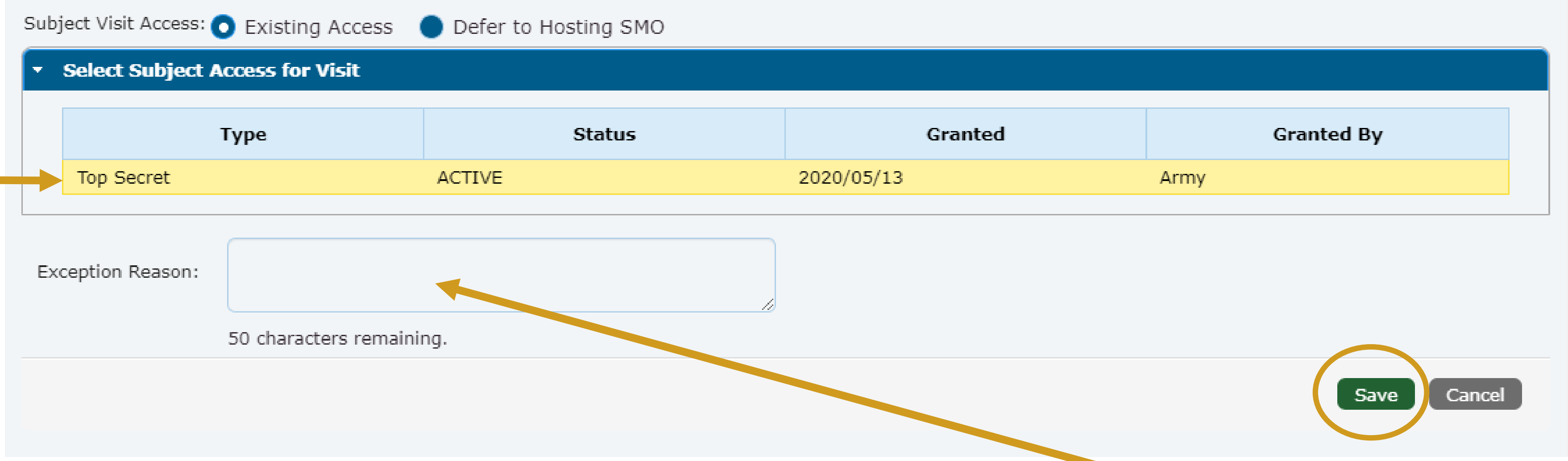


Click on a row to select an **Owning/Servicing SMO** relationship.

Use the radio buttons to select a visit access: **Existing Access,** or **Defer to Hosting SMO.** If you select **Defer to Hosting SMO**, the hosting SMO will then need to create a servicing relationship with the subject, and grant the subject the same level of access as the hosting SMO. **Use this option when the creating SMO has a lower access than the hosting SMO.**

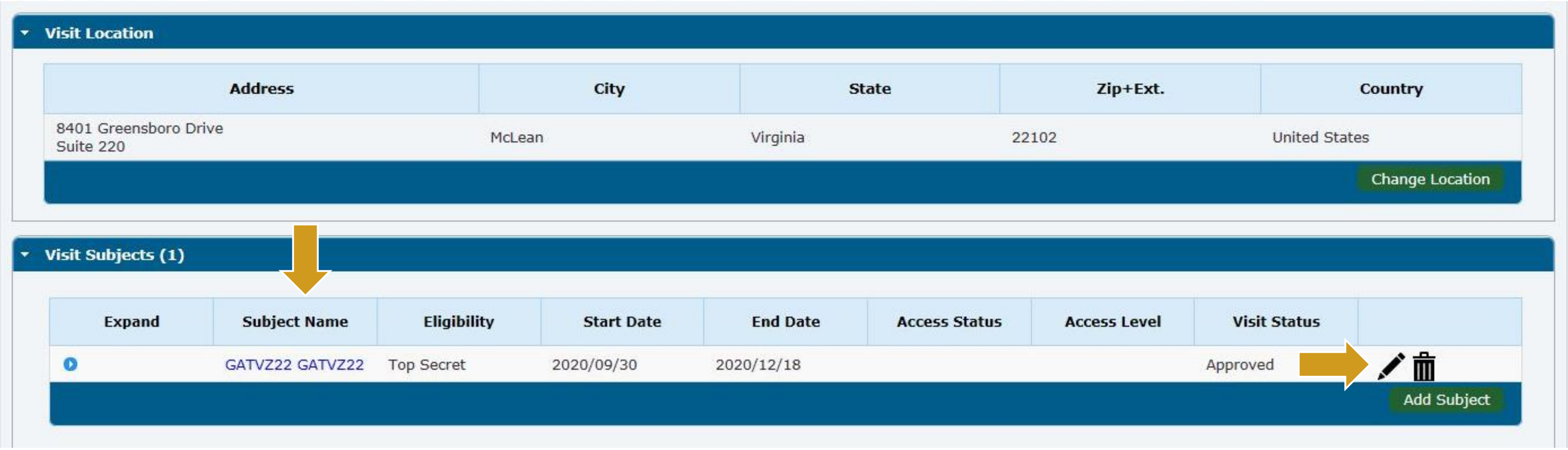
Select Subject Access for Visit

If you select **Existing Access**, click on a row to select an existing access.



If the subject's access is lower than the visit's access level, you must type an **Exception Reason** into the text box. Click ***Save***.

Selected Subject



If saved, the subject is added to the **Visit Subjects table** and the number increases by one.

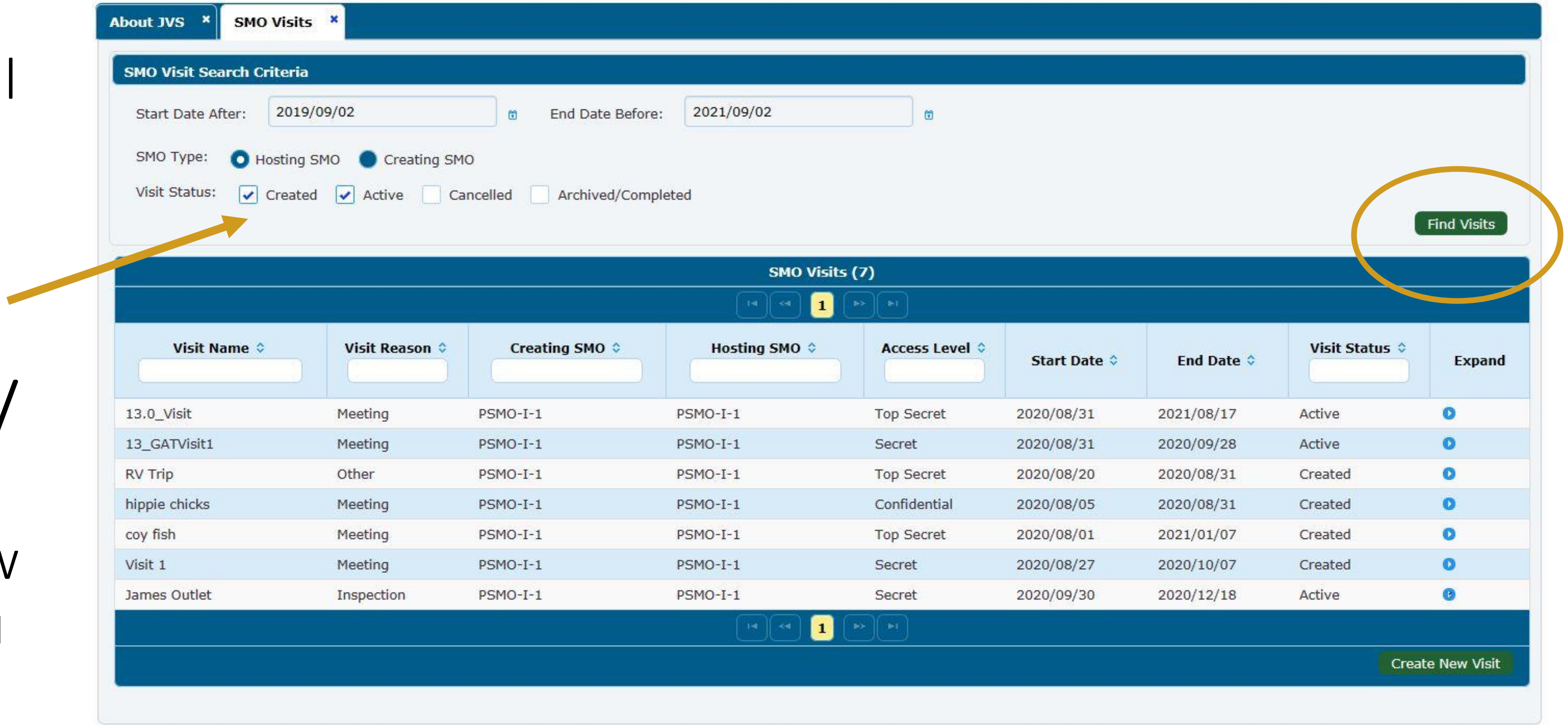
You can view the subject visit on ‘Subject details’ page under visit section in JVS, CATS and Appeals application.

To edit a subject after adding them to the visit, click on the edit icon in that row of the **Visit Subjects** table. A pop-up window called **Edit Subject Visit** opens. Edit the fields as appropriate. Click **Save** to save your edits, or click ***Cancel*** to cancel your edits. **Note:** You can only add a subject once to a visit. Otherwise, you will receive an error message.

Search SMO Visits

SMO Visits tab shows all the visits. You can filter visits by checking the boxes in **Visitor Status: Created, Active, Cancelled and Archived/ Completed.**

Select ***Find Visit*** to show only the visit status you want to see.



Visit Name	Visit Reason	Creating SMO	Hosting SMO	Access Level	Start Date	End Date	Visit Status	Expand
13.0_Visit	Meeting	PSMO-I-1	PSMO-I-1	Top Secret	2020/08/31	2021/08/17	Active	
13_GATVisit1	Meeting	PSMO-I-1	PSMO-I-1	Secret	2020/08/31	2020/09/28	Active	
RV Trip	Other	PSMO-I-1	PSMO-I-1	Top Secret	2020/08/20	2020/08/31	Created	
hippie chicks	Meeting	PSMO-I-1	PSMO-I-1	Confidential	2020/08/05	2020/08/31	Created	
coy fish	Meeting	PSMO-I-1	PSMO-I-1	Top Secret	2020/08/01	2021/01/07	Created	
Visit 1	Meeting	PSMO-I-1	PSMO-I-1	Secret	2020/08/27	2020/10/07	Created	
James Outlet	Inspection	PSMO-I-1	PSMO-I-1	Secret	2020/09/30	2020/12/18	Active	

Cancel Visit For Subject

Visit Subjects (1)

Expand	Subject Name	Eligibility	Start Date	End Date	Access Status	Access Level	Visit Status	
	Security Officer1	Secret	2020/07/24	2020/08/31			Approved	

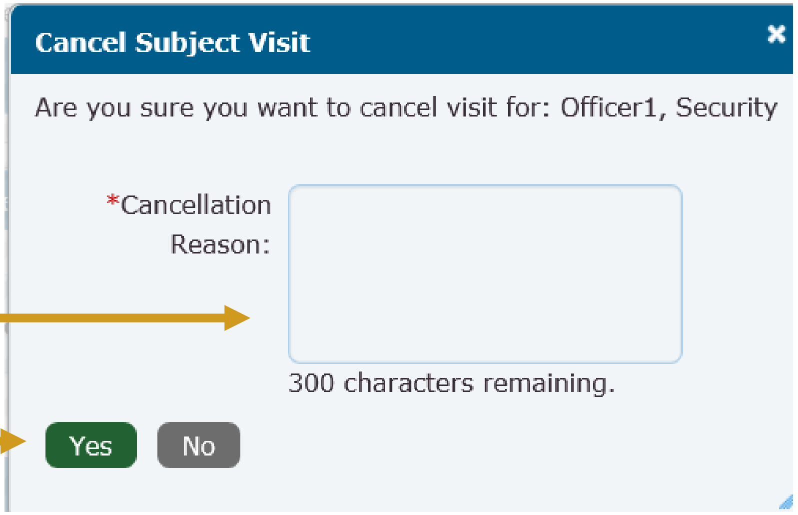
Add Subject

To cancel a visit for a subject, click on the ***Delete icon*** for that subject in the **Visit Subjects table**.

A pop-up window called **Cancel Subject Visit** opens.

Type a **Cancellation Reason** into the text box.

Select ***Yes*** to cancel the visit for the subject. Or, select ***No*** to keep the subject on the visit.



Visit for Subject Cancelled

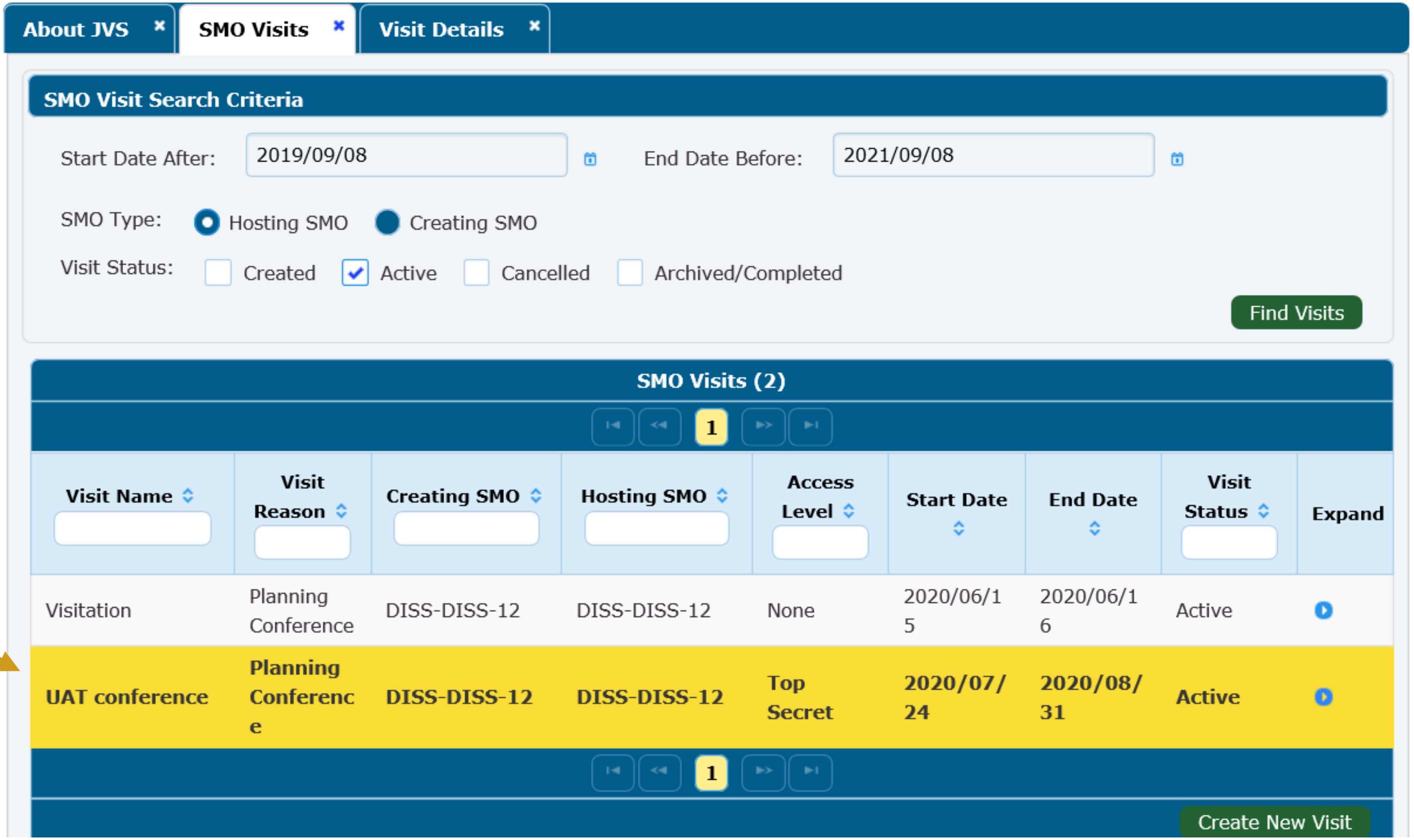
Visit Subjects (1)

Expand	Subject Name	Eligibility	Start Date	End Date	Access Status	Access Level	Visit Status
	GATVZ22 GATVZ22	Top Secret	2020/09/30	2020/12/18			Canceled

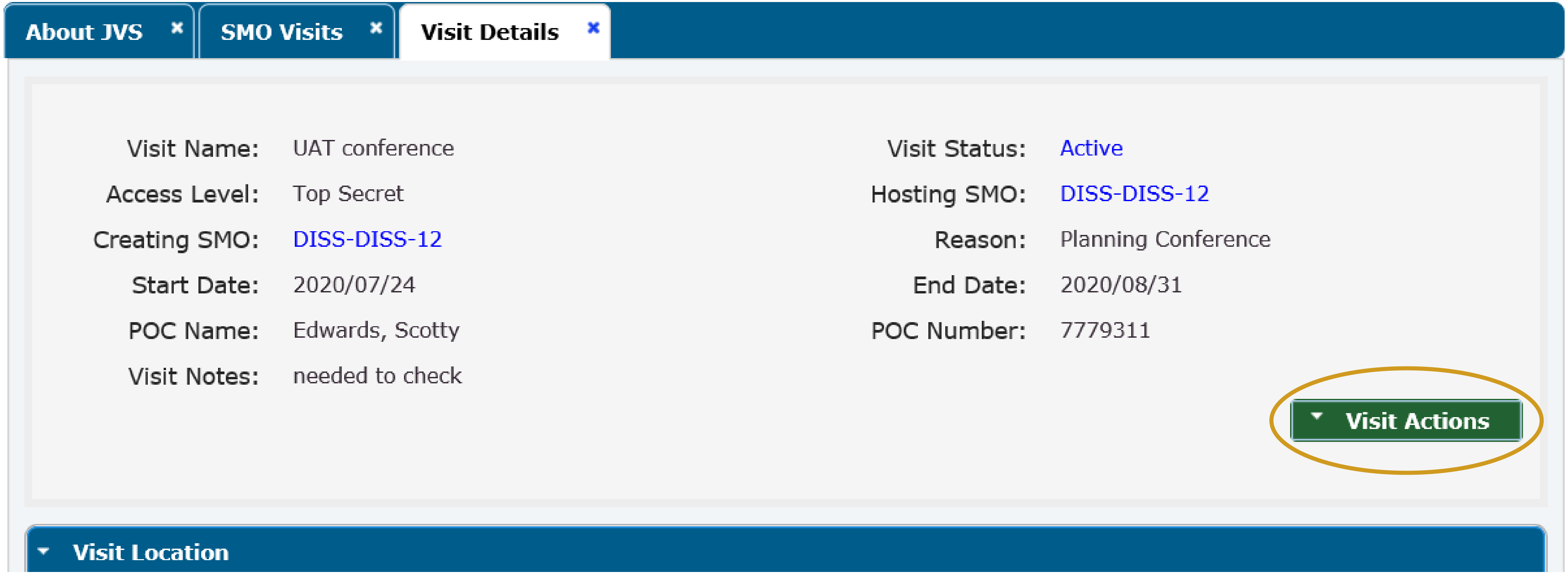
The subject remains in the **Visit Subjects** table, but their **Visit Status** changes to **Canceled**.

Changing Visit Status

To change the Visit Status to **Cancelled or Archived/ Completed** select the visit you wish to change.



Visit Actions

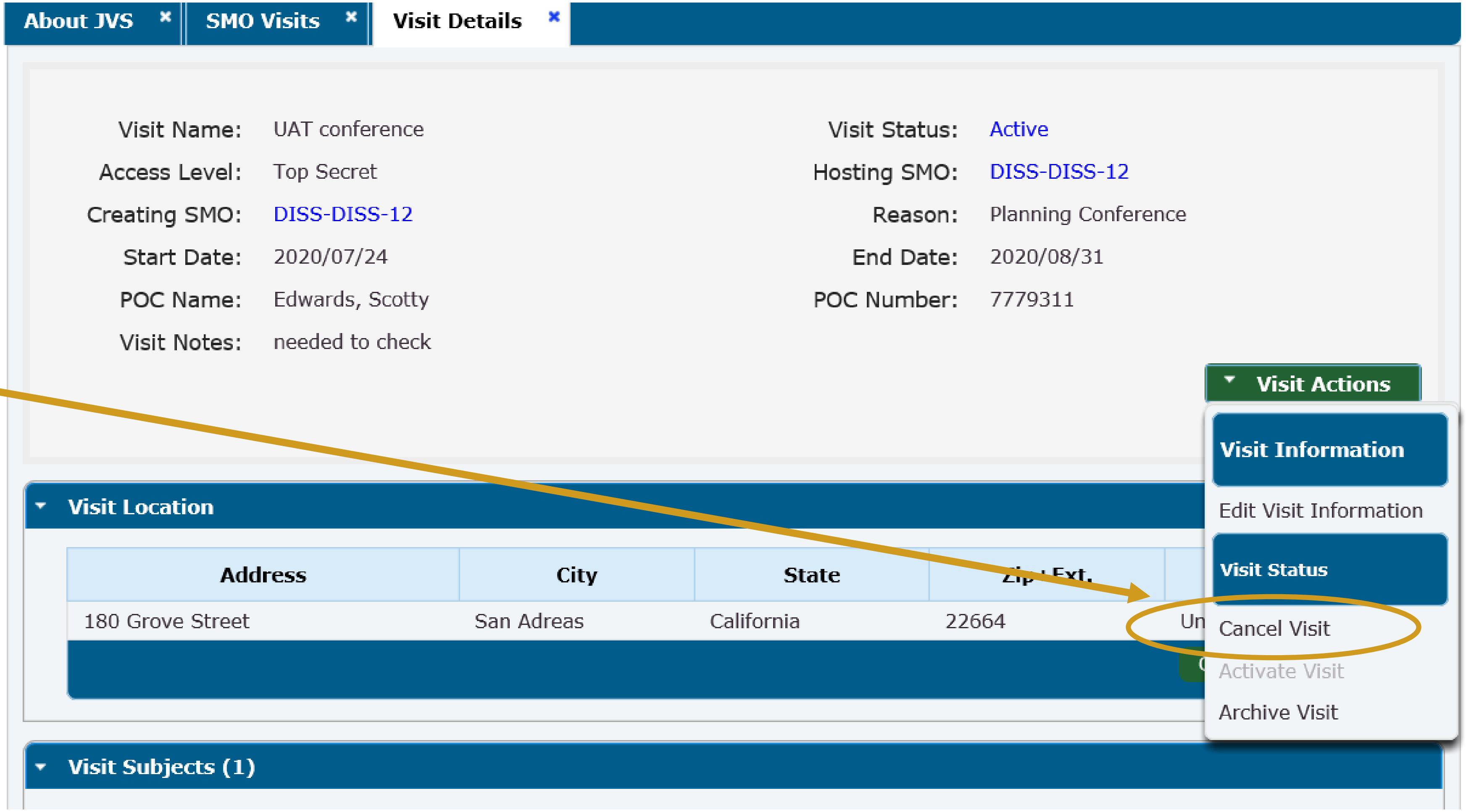


The **Visit Details** tab will open. To change Visit Status select **Visit Actions**.

Change Visit Status

Under the Visit Actions menu you can *Cancel Visit* or *Archive Visit*.

Select *Cancel Visit*.



Cancel Visit

A **Cancel Visit** box will pop up asking you to confirm you wish to cancel the meeting.

Type a **Cancellation Reason** into the text box.

Select ***Yes*** to cancel the visit, or select ***No***, which will not cancel the visit.

The status of the visit changes to Canceled and you receive a confirmation message in the upper right corner.

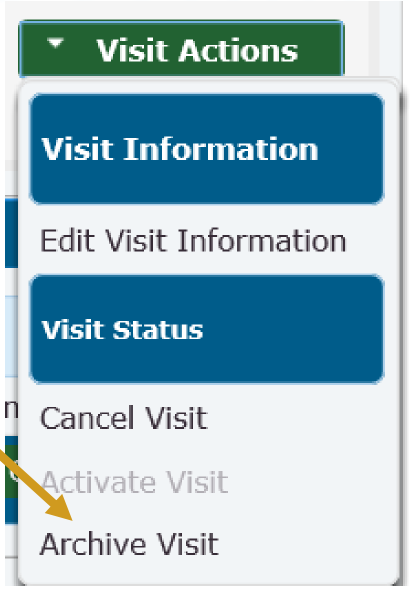
Archive Visit

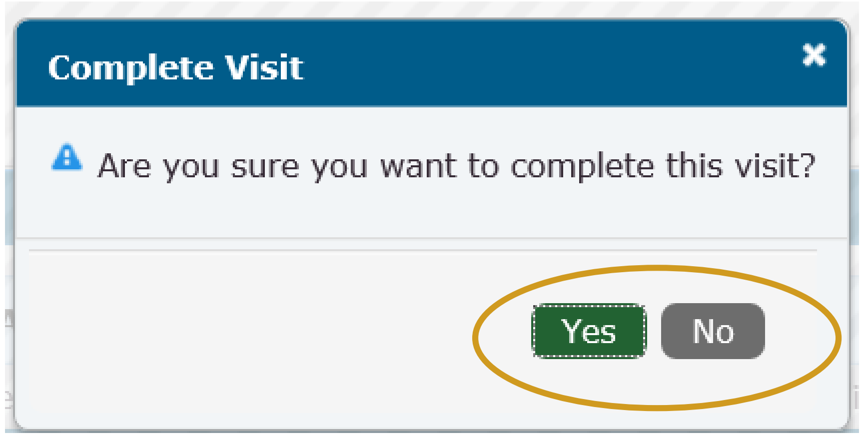
If you wish to archive the visit, select ***Archive Visit*** under the **Visit Actions** drop down menu.

A **Complete Visit** box will pop up.

Select ***Yes*** to complete the visit, or select ***No***, which will not archive the visit.

The status of the visit changes to **Archived/Completed** and you receive a confirmation message in the upper right corner.



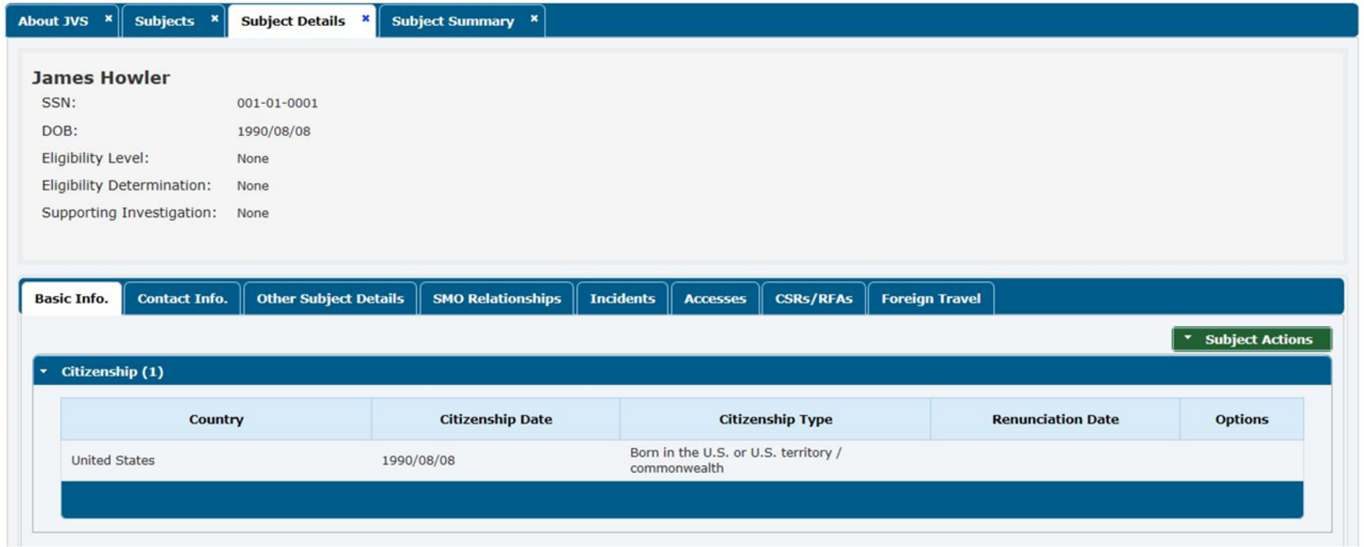


INVESTIGATION REQUESTS
(INDUSTRY ONLY)

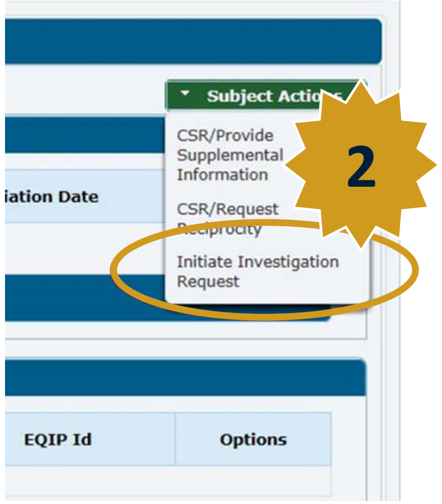
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Subject Details and Subject Actions

Within the **Subject Details** page, select the **Subject Actions** drop-down menu and select **Initiate Investigation Request**. See next slide for closer view.



1. Select **Subject Actions.**



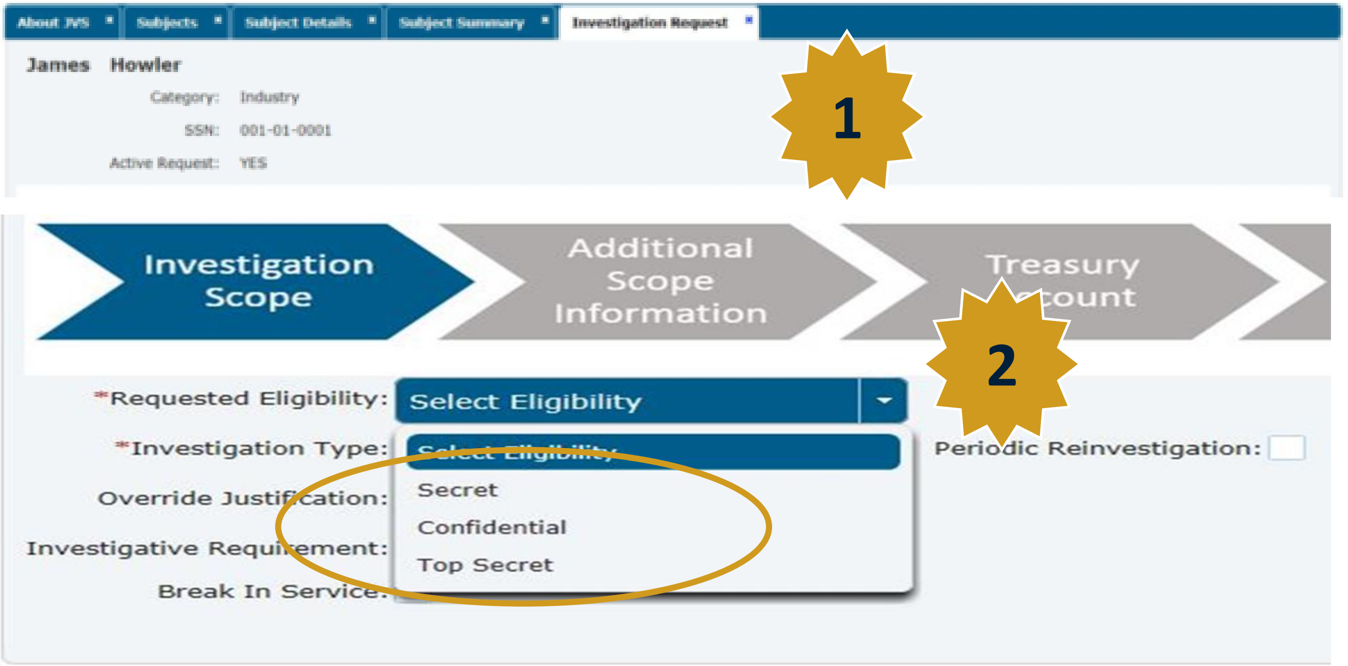
2. Select **Initiate Investigation Request.**

Owning relationship required and one of the following Industry roles:

- Security Officer
- Security Manager

Investigation Scope

1. A new tab called **Investigation Request** opens. The first step in the wizard is **Investigation Scope.**



When you select **Requested Eligibility**, the **Select Eligibility** drop down menu will give you three options: **Secret, Confidential, and Top Secret**. In this example we will select **Top Secret**.

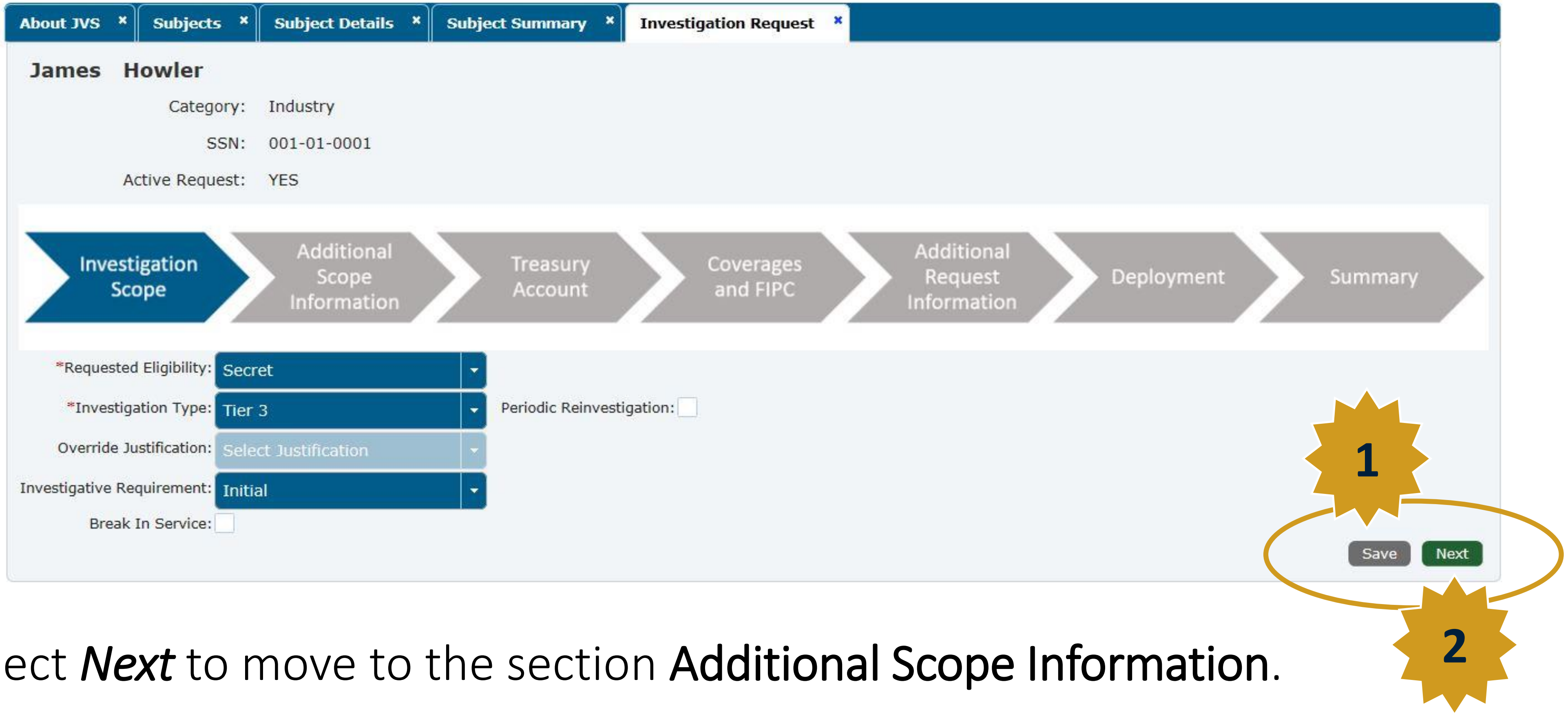
2. Use the drop-down menu to select a **Requested Eligibility.** This functionality applies only to security cases.

Tier 3R Reinvestigation Example

1. Select **Secret.**
2. **Tier 3R** will automatically populate if there is a check in the **Periodic Reinvestigation** box.
3. **Investigation Requirements** will automatically show **Reinvestigation** when **Tier 3R** is selected.

Save and Next Button

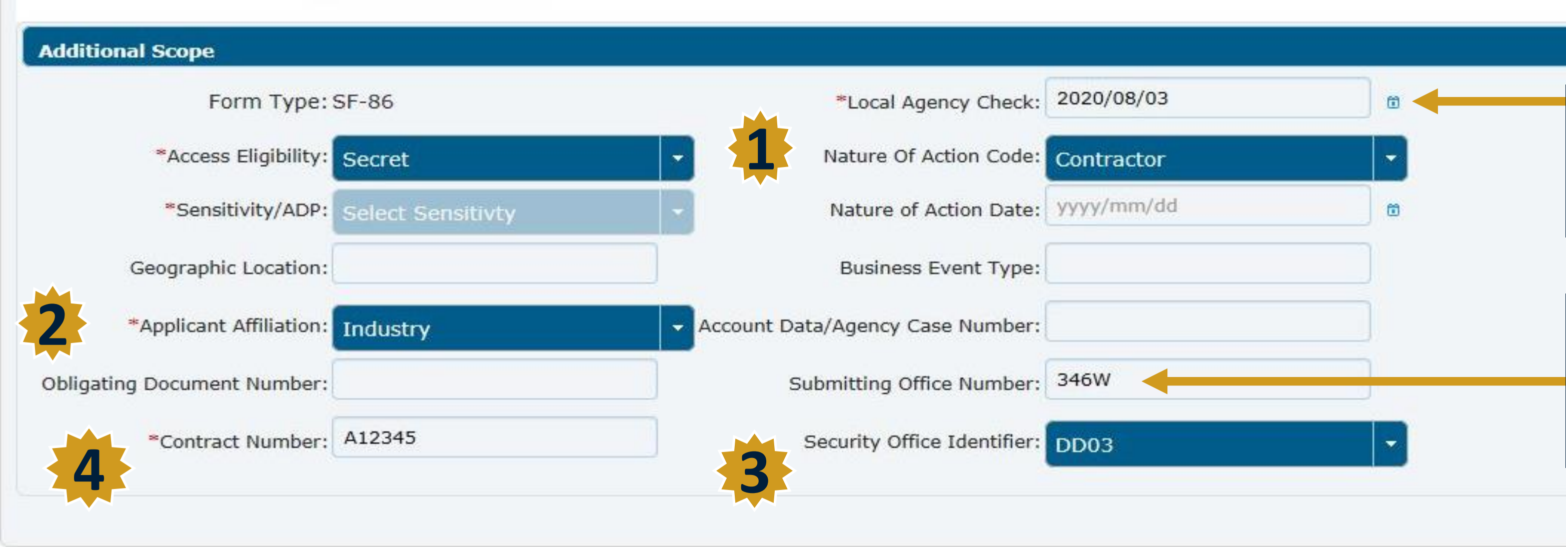
1. After you have completed the **Investigation** Scope section make sure you select ***Save*** before selecting ***Next***.



2. Select ***Next*** to move to the section **Additional Scope Information**.

Additional Scope Information

1. Use the drop-down menu to select a **Nature of Action Code**. Select from the drop-down menu **Contractor.**



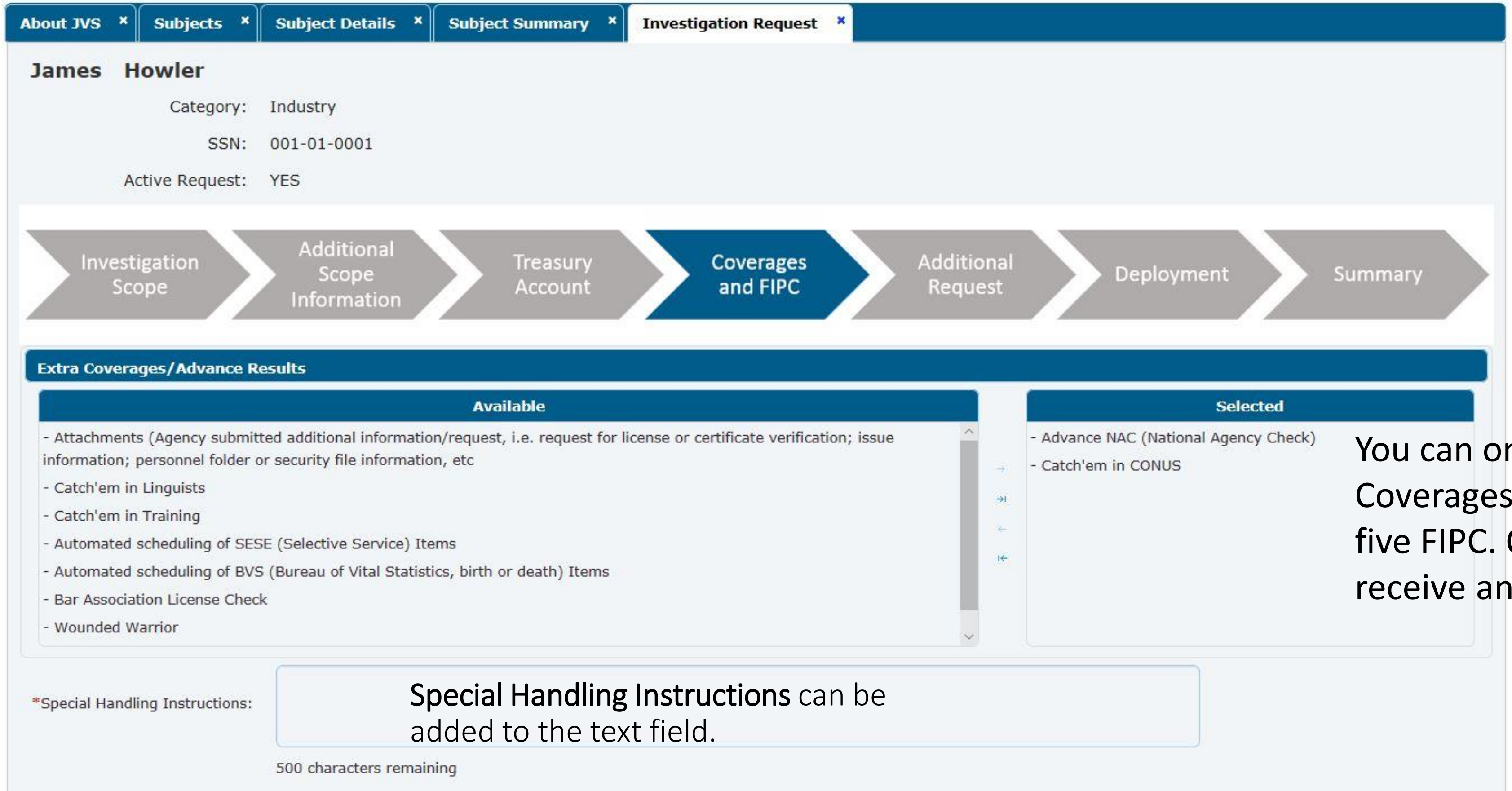
Select the Calendar icon to select a date for the Local Agency Check and the Nature of Action Date.

Note: The Submitting Office Number automatically fills in with the default SON for industry or non-industry.

2. From the drop-down menu select an **Applicant Affiliation**. Select **Industry.**
3. From the drop-down menu select the **Security Office Identifier (Select other Adjudication Offices).**
4. Include **Contract Number.**
5. Select ***Save*** and select ***Next*** to move to the section on to the **Treasury.**

Select Extra Coverage and FIPC

The fourth step is Coverages and FIPC, which is also entirely optional, and Special Handling Instructions.

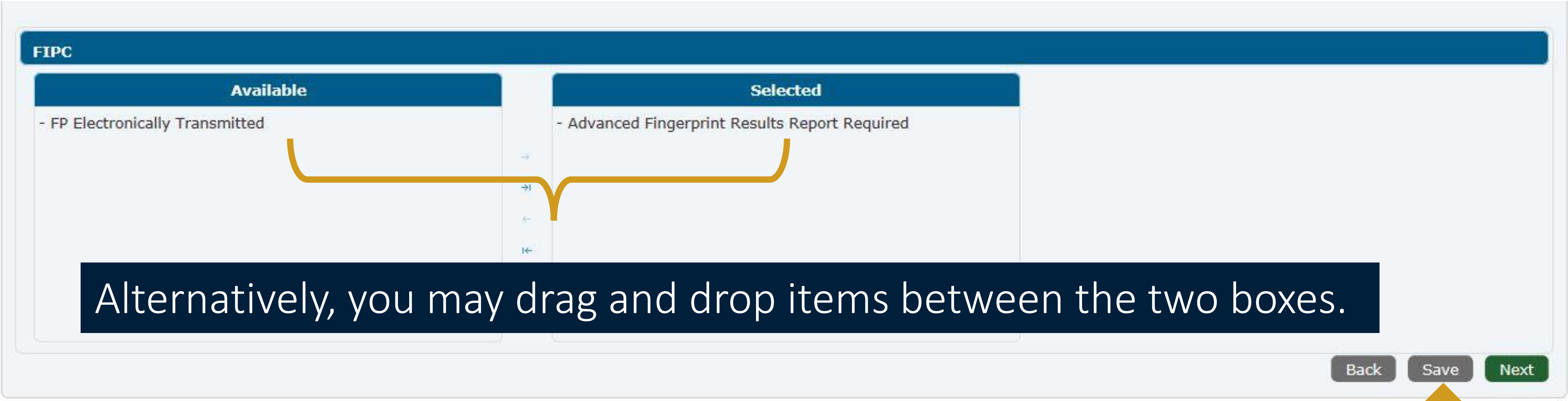


You can only add eight Extra Coverages/ Advance Results, and five FIPC. Otherwise, you will receive an error message.

Special Handling Instructions can be added to the text field.

Select FIPC

To move **Selected** items back to the **Available** box, click on the selection and then click the ***remove*** icon. To move all items from the Selected box back to the Available box, click the ***remove all*** icon.



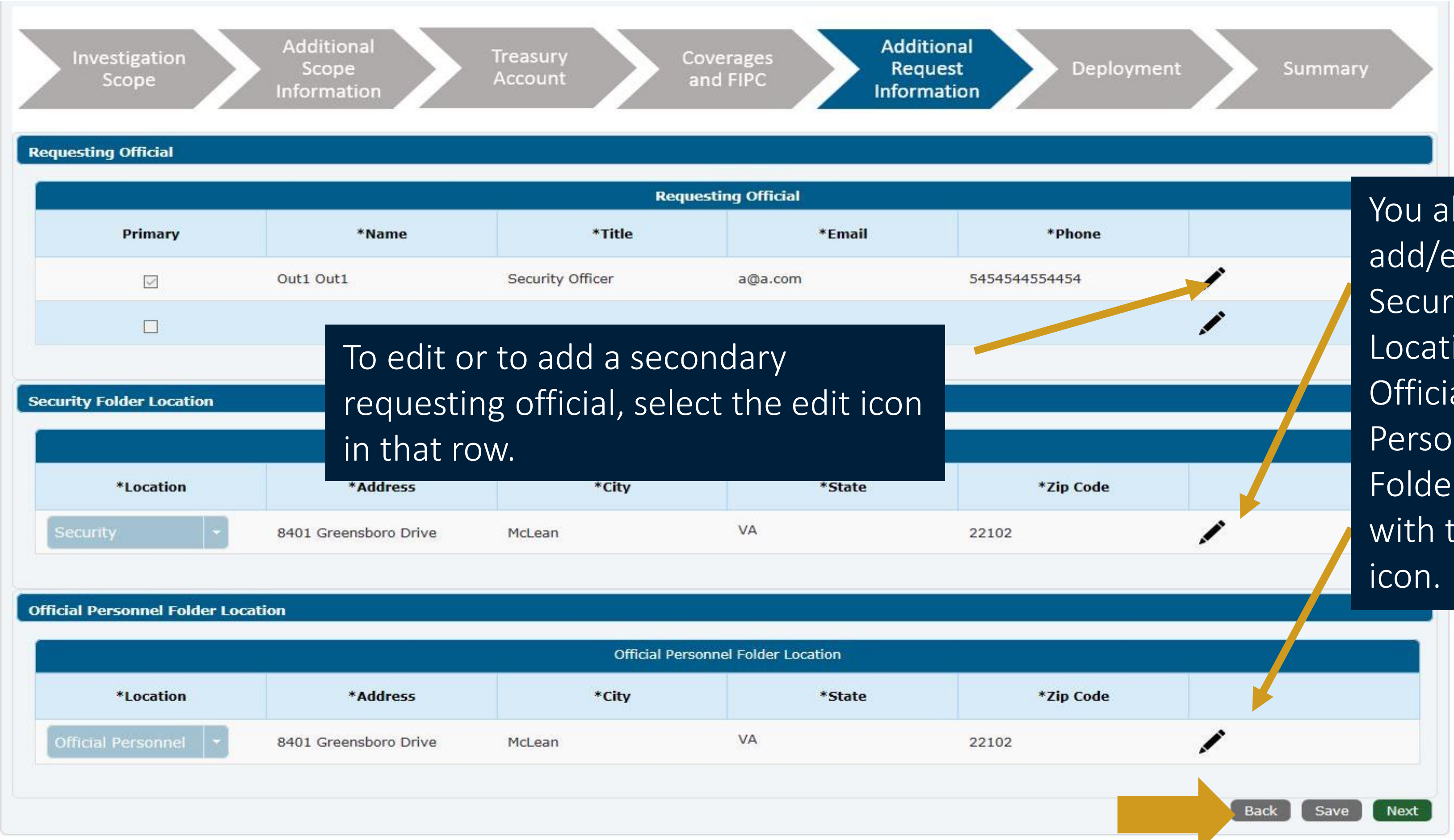
Alternatively, you may drag and drop items between the two boxes.

Select ***Save*** and ***Next*** to continue to the next step, **Add Additional Information**.

Add Additional Information

The fifth step is **Additional Request Information**. The current user will automatically fill in as the primary **Requesting Official**.

Select ***Save*** and ***Next*** to continue to the next step, **Deployment Information**.

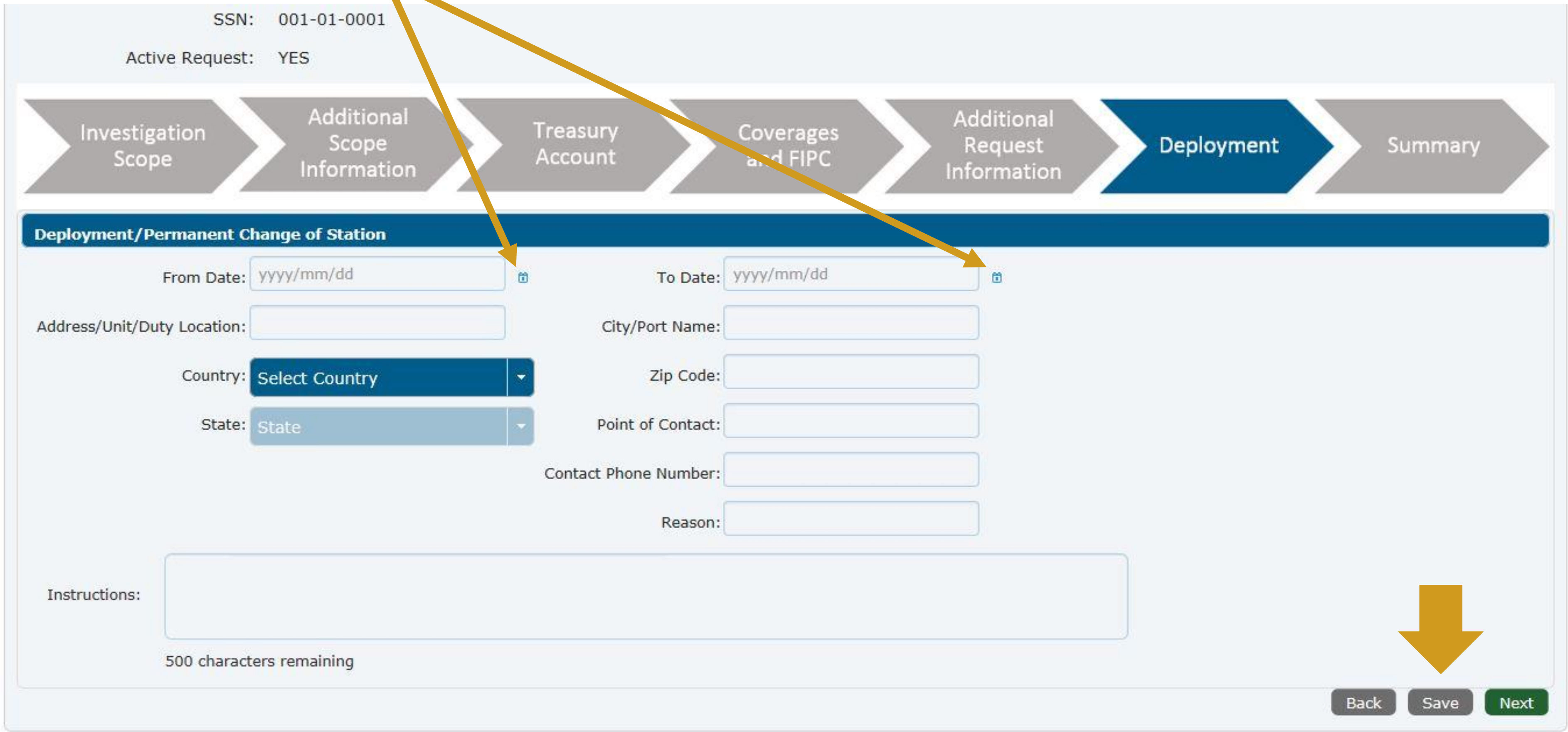


To edit or to add a secondary requesting official, select the edit icon in that row.

You also add/edit Security Folder Location and Official Personnel Folder Location with the edit icon.

Deployment Information

The sixth step is **Deployment**, which is entirely optional. Fill in the appropriate fields. Use the **calendar icon** to select a **From Date** and **To Date**.



Select ***Save*** and ***Next*** to continue to the next step, **Summary.**

Summary Screen (Continued)

Additional Request Information Summary

Requesting Official Summary

Requesting Official				
Primary	*Name	*Title	*Email	*Phone
☑	Out1 Out1	Security Officer	a@a.com	5454544554454

Security Folder Location				
*Location	*Address	*City	*State	*Zip Code
Security	8401 Greensboro Drive	McLean	VA	22102

Official Personnel Folder Location				
*Location	*Address	*City	*State	*Zip Code
Official Personnel	8401 Greensboro Drive	McLean	VA	22102

Deployment/Permanent Change of Station Summary

From Date:	To Date:
Duty Location:	City/Port Name:
State:	Zip Code:
Country:	Point of Contact:
Contact Phone Number:	Reason:

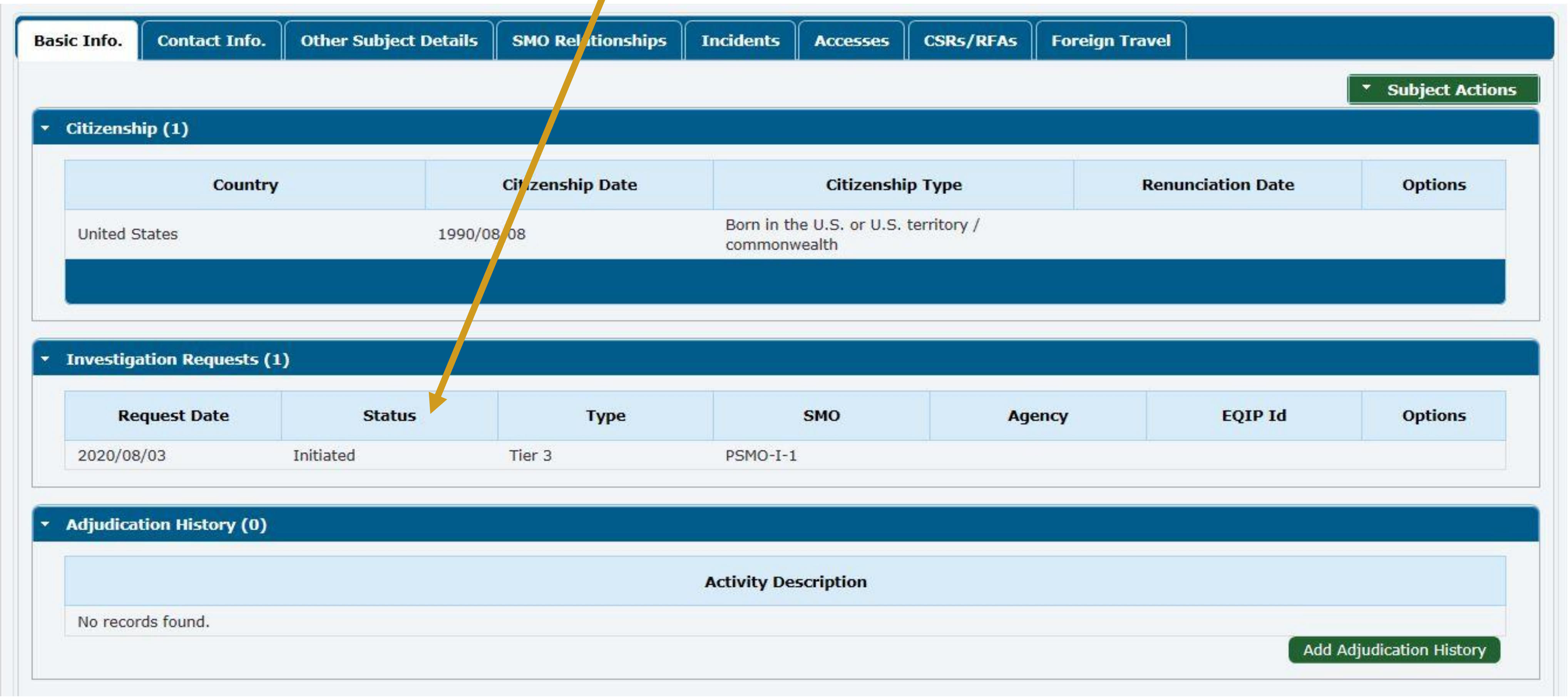
Special Handling Instructions

Back | Save | Create

Select ***Create*** to send the investigation request.

Investigation Initiation

The **Investigation Requests** table on the **Subject Details** tab now has a new entry, and the status is **Initiated**.



Initiate Request Grayed Out

After an **Investigation Request** has been submitted the **Initiate Request** is grayed out under **Subject Actions.** This prevents another investigation from being initiated.

JPAS to DISS timelines

Total Days to Submit an Investigation Request via JPAS to VROC: 37

Feb 16	Communicate	DCSA issues guidance "Important Dates for JPAS/DISS"
Mar 1	Initiate in DISS	Industry may use DISS to initiate investigation requests
Mar 14	Deadline!	Last day to initiate investigation requests in JPAS
Mar 31	Deadline!	Last day to submit investigation requests previously initiated via JPAS
Apr 1	Full DISS Deployment	VROC will not be able to access JPAS to process investigation requests. All investigation requests will process via DISS.

Total Days to Submit an Investigation Request via DISS = 120 days

FSO initiates investigation request → *30 days* → Subject accesses, completes e-QIP and sends to FSO → *30 days* → FSO completes review for accuracy/ completeness and sends to VROC → *60 days (shared with FSO/VROC)* → VROC reviews and conduct interim determination

If there are any investigation requests initiated in JPAS, they must be:

1. Filled out by the Subject
2. Reviewed for accuracy and completeness by the FSO
3. Submitted to VROC NLT March 31st, 2021.

TIPS AND TRICKS

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY

Validation of Records

It is important to validate the accuracy of all your records, particularly while you still have access to JPAS. The following are some of the discrepancies reported.

- Active employees (employees in JPAS PSMnet and Not in DISS).
- Current eligibility that is reflected.
- Investigation not matching up to JPAS.
- If placed in Continuous Evaluation – date is not reflected.
- Access (In access in JPAS not in DISS).

Quick Tips – JVS

- **Tip 1:** When searching SMOs in DISS the asterisk (*) is not required for a "wild card" search.
- **Tip 2:** The IE browser "Back and Forward" icons do not work within DISS. It will cause an error and require you to log-in again. Use only the tabs and buttons within DISS to navigate.
- **Tip 3:** Inactivity in DISS for more than 10 minutes, DISS will log you out. You will get a warning at 8 minutes.
- **Tip 4:** 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.
- **Tip 5:** If your hierarchy is inaccurate (missing SMOs, incorrect parent to child relationships, etc.) you will need to complete a Hierarchy Change Request (HCR) form.
- **Tip 6:** Failure to login within 30 days will lock your account, 45 days the account will be deactivated.

Troubleshooting

- **What if my person is not listed in my subject list to be picked?**
  - Most likely, the relationship did not flow over correctly from JPAS. You will need to search for the person by SSN and then add the relationship to the subject.
- **What if I don’t have the blue “Subject Details” link after their name?**
  - This means you do not have a relationship with the person, you will need to establish a relationship for that link to show up.
- **What if I don’t see any of my people in the subject list?**
  - You may have been provisioned under the wrong SMO, look up a record of a person that should be in your subject list, compare the SMO that has the relationship with the record to the SMO you have an account under. If they are different, then reach out to your account manager to be added to the SMO with the correct role needed.

DISS Recent Releases

- Mass Indoctrinate, Transfer, and/or Debrief subjects
  - Added the ability to indoctrinate, transfer, and/or debrief all subject's en masse with one-click.
- Report Schedule and Pickup
  - Added the ability for reports to run in the background to be retrieved at a later time, so as to not impact system performance especially with large organizations and reports.
- Enhanced Reports (7 Jan 2021)
  - Pre-Case Status Report: Assists in the management of Investigation Requests in a Users Hierarchy.
  - One-Time Access Report: Non-Industry Report for "One-Time Access."
  - Notifications Report: Assists in the management of Notifications in a Users Hierarchy.
  - Task Inbox Report: Assists in the management of Tasks in a Users Hierarchy.
  - Non-SCI Access Report: Provides Non-SCI Access information on subjects in a Users Hierarchy.
  - Subject Report: CE Information included in Subject Report.

Personnel Security Support

Knowledge Center Inquiries

In an effort to continue to protect our workforce during the COVID-19 pandemic, Personnel Security Inquiries (option 1/option 2) of the DCSA Knowledge Center has been suspended until further notice. We will continue to provide status updates via DISS Customer Service Requests and VROC email dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil. When calling (888) 282-7682, customers will have the following menu options:

- Personnel Security Clearance Inquiries (e-QIP PIN Resets, Golden Questions & VROC)
- For Industry PIN Resets: **HANG UP** and **Call** the Applicant Knowledge Center at 724-738-5090, or;
- Email DCSApplicantSupport@nbib.gov, or;
- For all other PCL related inquiries email dcsa.ncr.dcsa-dvd.mbx.askvroc@mail.mil
- Industry PSAARs should be sent to: dcsa.dcsa-northern.dcsa-dvd.mbx.diss-provisioning@mail.mil

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@osdgc.osd.mil

DMDC Contact Center

Phone	1-800-467-5526
Email.	dmdc.contactcenter@mail.mil
Menu Options	1 – DISS 3 – JPAS 4 – e-QIP 5 – SWFT 6 – DCII 7 – PerSec/ General Questions 8 – STEPP/ISFD/FCL