DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

JOB AID

NBIS CONSOLIDATED JOB AIDS

Volume 2 v1

Abstract

This is a compilation of the NBIS application job aids.

DCSA

dcsa.quantico.nbis.mbx.training@mail.mil

Table of Contents

VERSION CONTROL/CHANGE LOG

Version 1	Jan 10, 2022	Created	SAB

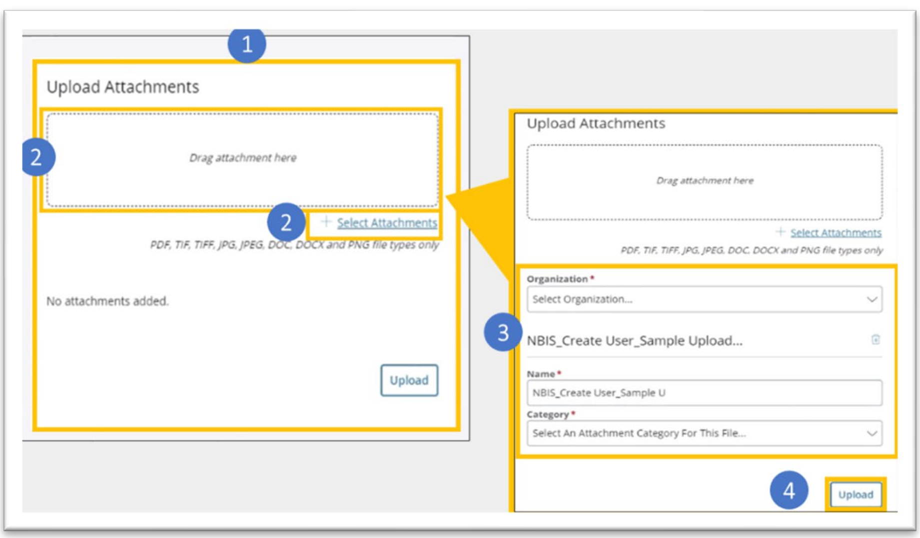
SUBJECT MANGEMENT

HOW TO ADD ATTACHMENTS TO A SUBJECT'S PROFILE

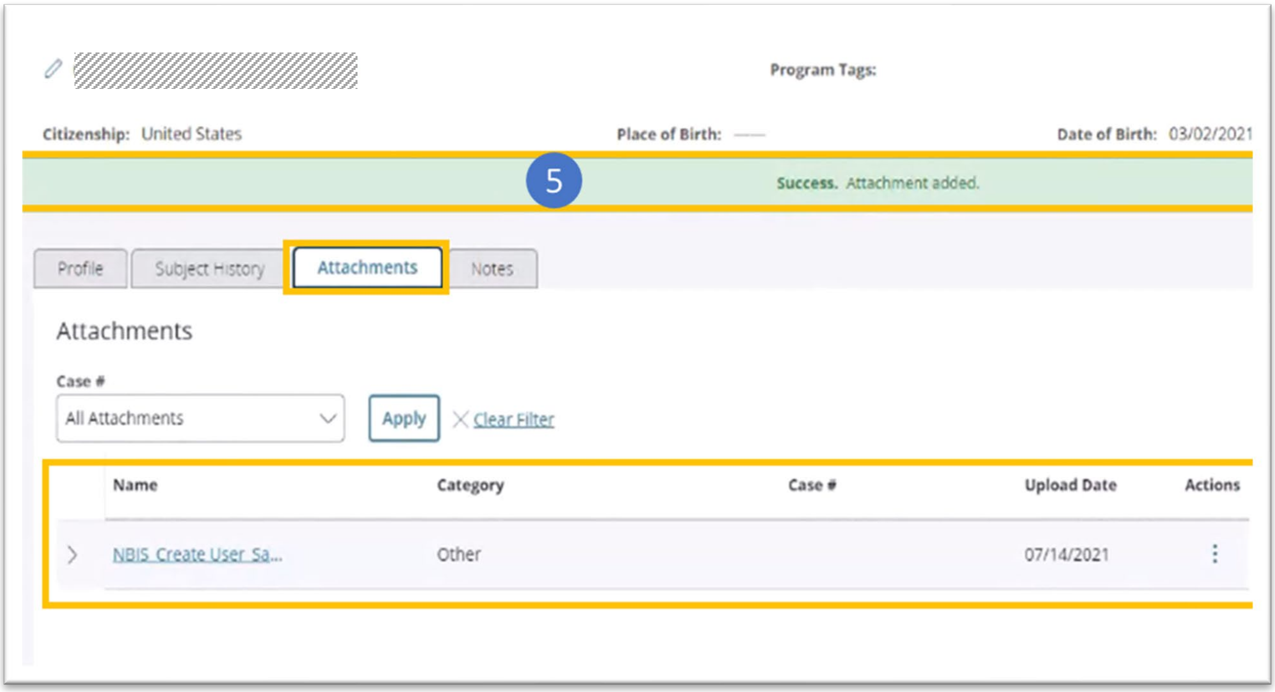
Users with the Subject Manager, Authorizer, Reviewer, Initiator, Mass Initiator, Screener, Subject Profile Editor, Subject Viewer and Facility Security Officer (FSO) roles can access the Attachments section in a Subject's case. Users can add, manage, and upload attachments associated with the Subject's profile. New attachments will appear near the top of the Attachments tab list in the Subject's Worksheet.

1. From the Subject Management tab, search for the Subject's SSN and open the Subject's Worksheet. Locate the "**Upload Attachments**" box on the right-hand side of the screen.
2. Drag an attachment into the "Drag Attachment Here" box or select the "Select Attachments" hyperlink below the "Upload Attachments" box.
3. Browse for and add the attachment. Enter the Organization, document name, and category for the document.
4. Select **Upload**.
5. A green success banner will appear when the attachment has been uploaded. To view the new attachment, navigate to the Attachment tab in the Subject Worksheet. Select the "**Attachment Name**" hyperlink. Note: If the attachment does not immediately appear in the list, select "Clear Filter."

Steps 1-4



Step 5


Program Tags:
Citizenship: United States
Place of Birth: —
Date of Birth: 03/02/2021
5
Success. Attachment added.
Profile
Subject History
Attachments
Notes
Attachments
Case #
All Attachments
Apply
Clear Filter
Name
Category
Case #
Upload Date
Actions
NBIS Create User Sa...
Other
07/14/2021

HOW TO LOCATE AN EXISTING SUBJECT

There are two ways to locate an existing subject in NBIS. First is searching for an existing subject using the Global Search Bar and second is via the Advanced Search Hyperlink.

GLOBAL SEARCH BAR

Users with the Subject Manager, Authorizer, Reviewer, Initiator, Mass Initiator, Screener, Subject Profile Editor, Subject Viewer, and Facility Security Officer (FSO) roles can access Subject Profiles in their organization. Prior to initiating a case request requires searching for a Subject using their SSN. Below is the 5-step process to locate an existing Subject using the Global Search Bar.

1. From initial login, select **Subject Management** to see a list of all existing Subjects.

a. To modify the data fields that populate for all existing subjects, click Table Settings on the upper right-hand side of the table. Select **Fields** from the drop-down menu and check the boxes for the data fields you wish to display (e.g., Place of Birth, Email, Organization, etc.).

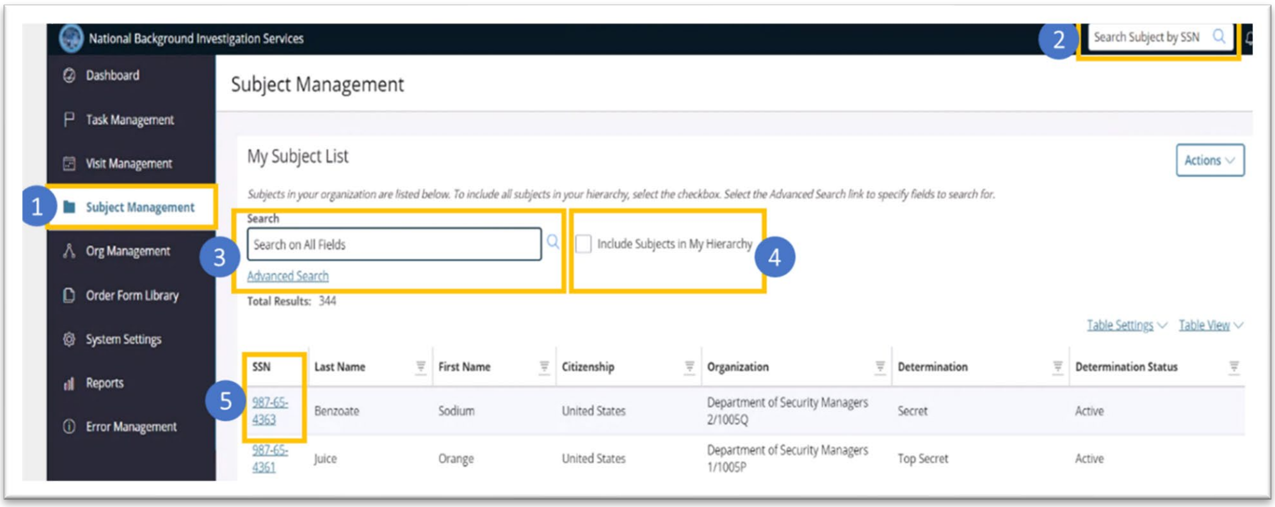
2. (Option 1) In the upper right-hand corner of the Dashboard, type the Subject's SSN into the **Global Search Bar** and select the magnifying glass to search for the Subject.
3. (Option 2) On the left-hand side of the Subject Management screen, type in the "**Search on All Fields**" text box to search for existing Subjects by SSN, email, first/last name, organization, or other value.
4. (Option 2) Select the box "**Include Subjects in My Hierarchy**" to search Subjects in your specific organization.
5. If a Subject exists search results appear in **My Subject List**. Select the Subject's SSN hyperlink to open the Subject's profile.

ADVANCED SUBJECT SEARCH

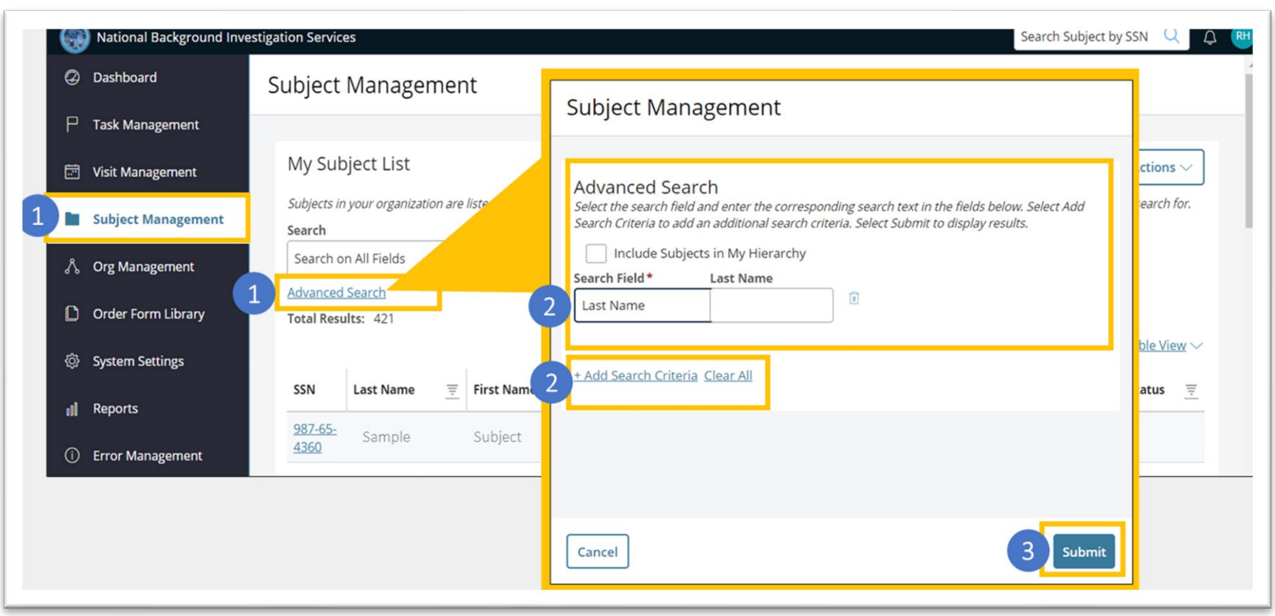
Below is the 4-step process to search for a Subject using the Advanced Search hyperlink. If a Subject does not yet exist, users will need to follow the steps to create the Subject before initiating a case request. Some of the Advanced Search Field options include SSN, email, first or last name, and organization.

1. From initial login, select **Subject Management** and navigate to and select the Advanced Search hyperlink located below "Search on All Fields."
2. Select the specific **Search Field** from the drop-down menu to choose the field. Enter the information for the search field.
3. Select **Submit**.
4. If a Subject exists search results appear in **My Subject List**. Select the Subject's SSN hyperlink to open the Subject's profile.

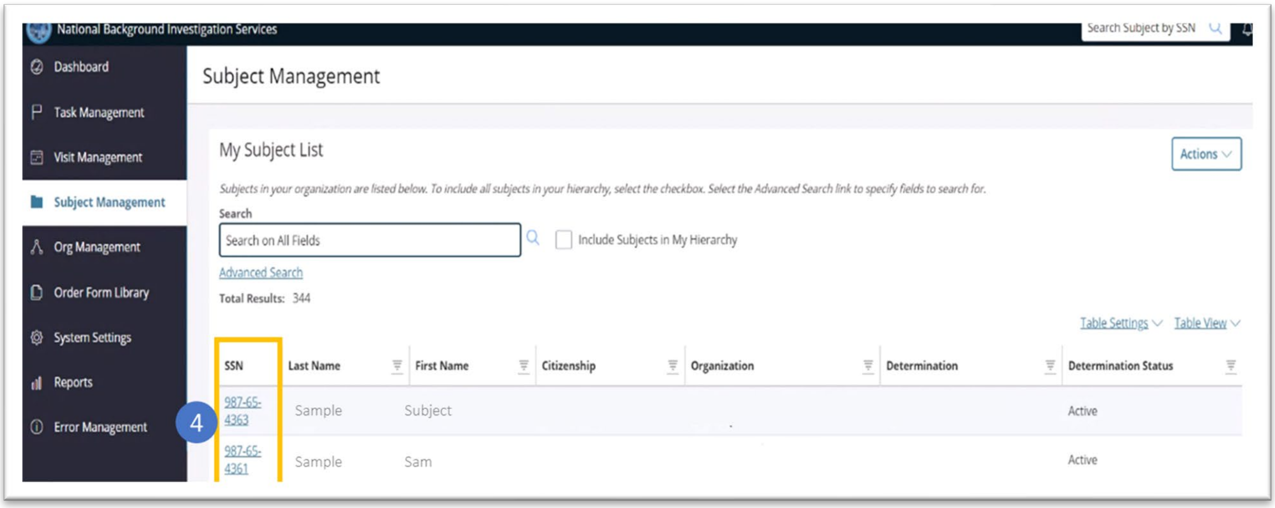
Global Search Bar (Steps 1-5)



Advanced Subject Search (Steps 1-3)



Advanced Subject Search (Step 4)

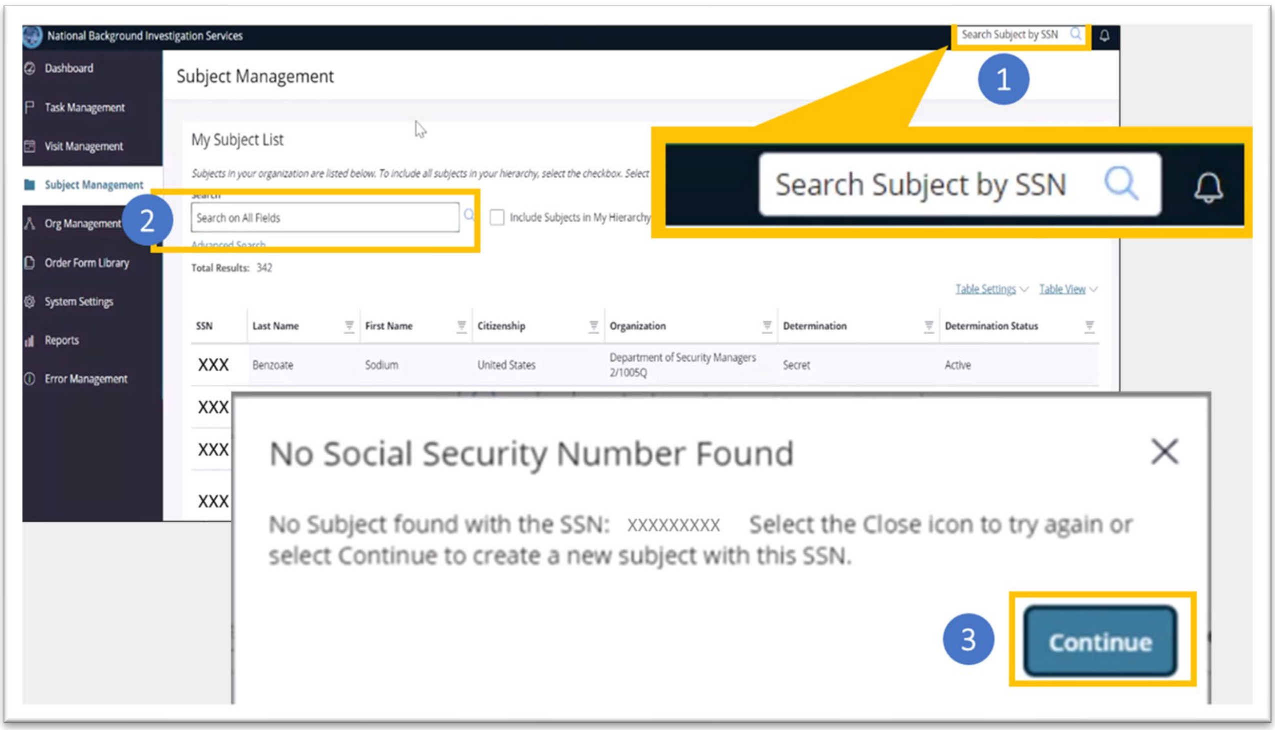


HOW TO CREATE A NEW SUBJECT

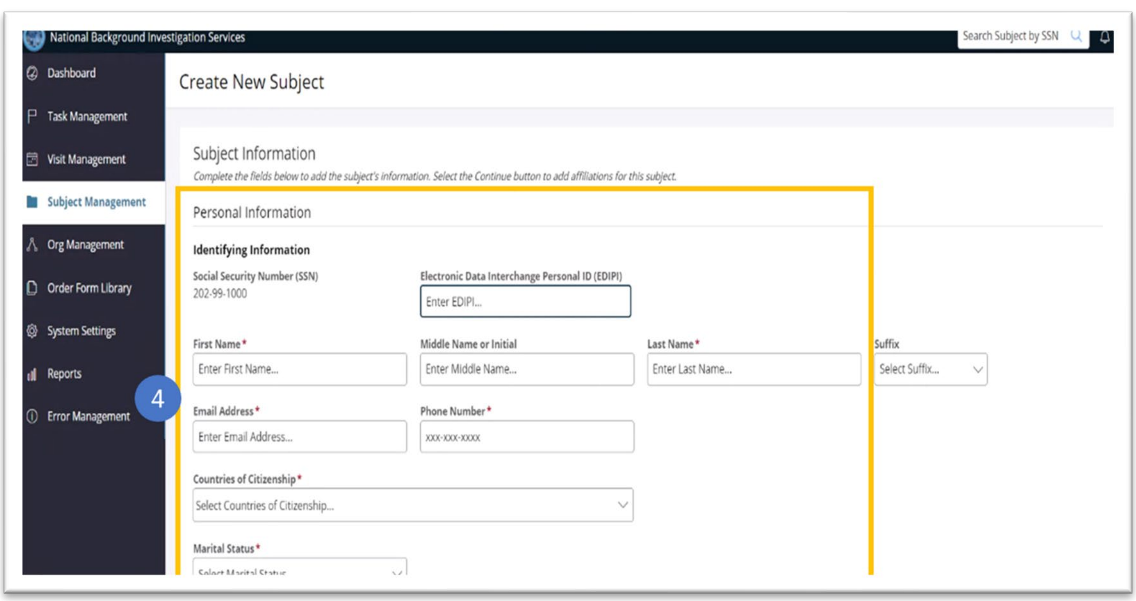
If a Subject does not appear in the existing search results, users with the Subject Manager, Authorizer, Reviewer, Initiator, Mass Initiator, Screener, Subject Profile Editor, Subject Viewer and Facility Security Officer (FSO) roles can create a new Subject. Required Subject fields vary based on a user's role. Users with the Subject Manager role are required to add an affiliation. Only users with the Subject Profile Editor role can edit the SSN field. To avoid creating a glut of Subjects unnecessarily, users should simultaneously create a Subject and initiate a case. Below is the 5-step process to Create a New Subject.

1. Select the "Search Subject by SSN" box in the **Global Subject Search Bar** located in the top right-hand corner. Type in the Subject's SSN and select Enter or the magnifying glass icon.
2. If you do not know the Subject's SSN, select the "**Search on All Fields**" search bar for the Subject List to search. If the Subject exists, follow the steps to initiate a case request.
3. If either search option does not yield a Subject, a pop-up window will indicate that no SSN was found and close to try again. Select "**Continue**" to create a new Subject with the SSN.
4. **Enter Subject data** into the required and optional fields. Required fields will be found under the personal and birth Information sections. Press "Continue."
5. Add the Affiliation to include the "Owning Organization" and "Category" from the drop-down options. If needed, select "Add Servicing Organization" hyperlink. Select "**Submit**." A green success banner will appear indicating the new subject was created.

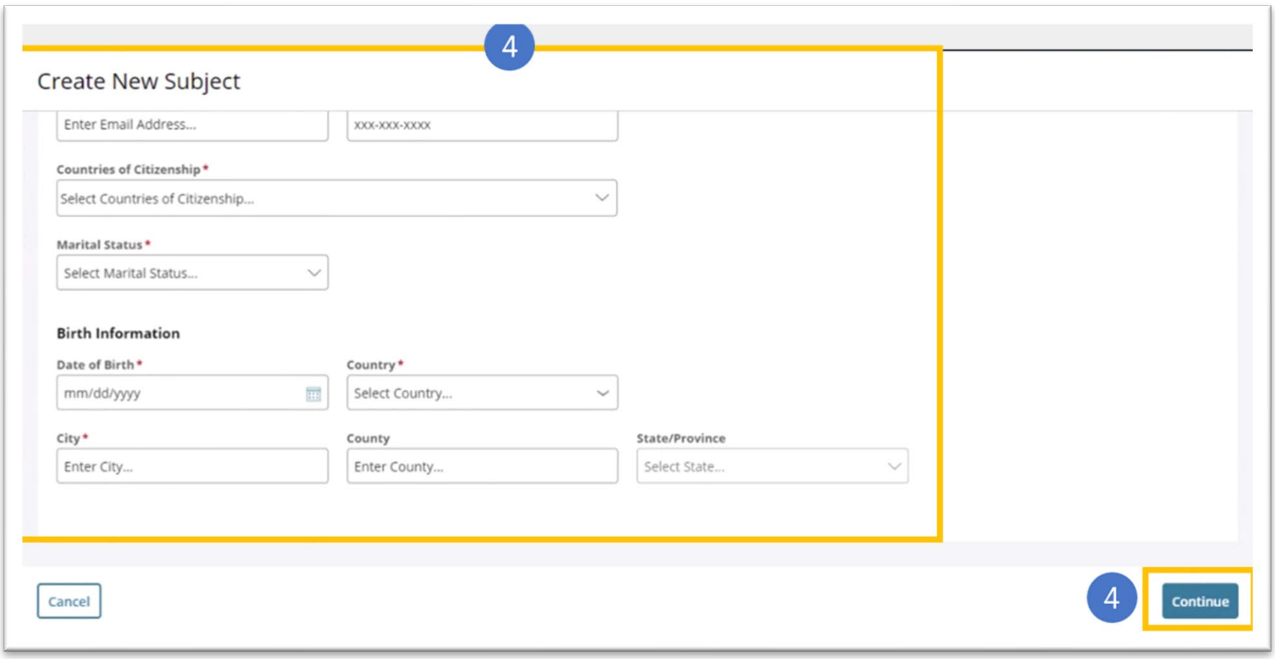
Steps 1-3



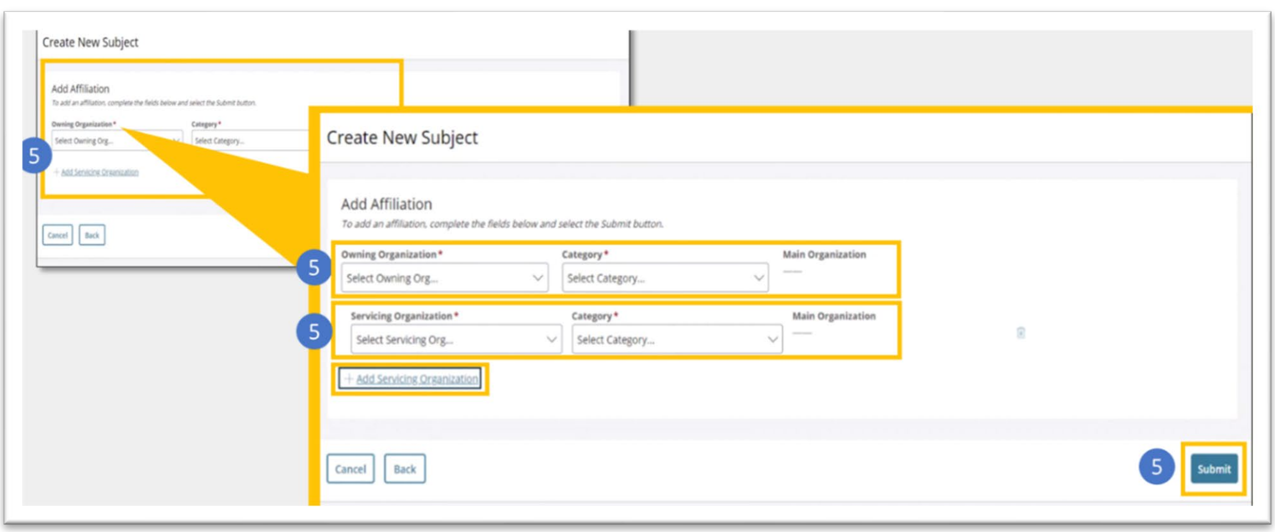
Step 4



Step 4 (Continued)



Step 5



HOW TO REVIEW A SUBJECT'S WORKSHEET

NAVIGATE TO THE SUBJECT'S WORKSHEET

1. Select **Subject Management** from the **Left Navigation.**
2. Search for the subject by typing the subject's first or last name, or SSN, in the **Search on All Fields** text box and select the **Magnifying Glass** to execute the search.
3. Select the **SSN** link corresponding with the subject to view the **Subject Worksheet**.
4. The user will be directed to the **Subject's Worksheet**. The components of **Subject's Worksheet** include:
    a. Subject Banner
    b. Subject Worksheet Tabs
    c. Action Cards

ACCESS THE SUBJECT BANNER

1. The **Subject Banner** provides high level information about the subject including SSN, EDIPI, Program Tags, Citizenship, DOB, POB, and Contact Information. The banner also includes the **Actions** drop-down.
2. Select the **Pencil** icon to make changes to the high-level information.
3. Select the **Actions** drop-down to take actions on the subject such as **Create Request**, **Start Initiation,** and **Reset eApp Password** (only available when subject is in the Initiation phase).
4. When working in the context of a case, the **Case Banner** will display beneath the **Subject Banner** and also be visible to the user. The **Case Banner** includes information regarding the **Case Type, Phase, date of last Phase update, External Status, date of last Status Update**, and **Case ID.**
5. Select **Collapse** or **Expand** to view more or less information within the **Case Banner**.

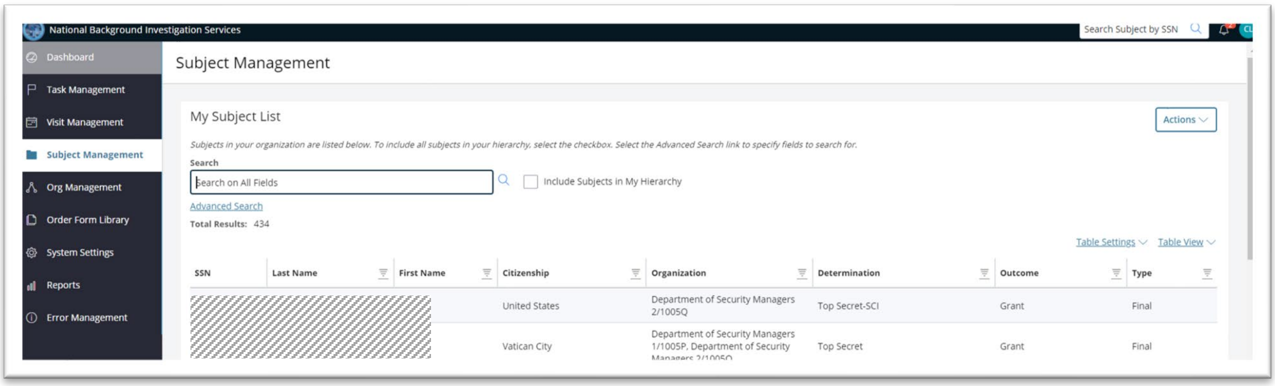
ACCESS SUBJECT WORKSHEET TABS

1. Within the **Subject Worksheet** there are multiple tabs visible to the user, including **Profile, Subject History, Attachments,** and **Notes.**
2. Select the **Profile** tab to view **Subject Profile** information.
3. Select the **Subject History** tab to view the **Subject History Summary** and sub-tabs for **Adjudications & CV, Requests & Cases,** and **Vetting Data.**
4. Select the **Attachments** tab to view documents uploaded by the user's organization. Select the **Notes** tab to view notes added by the user's organization.

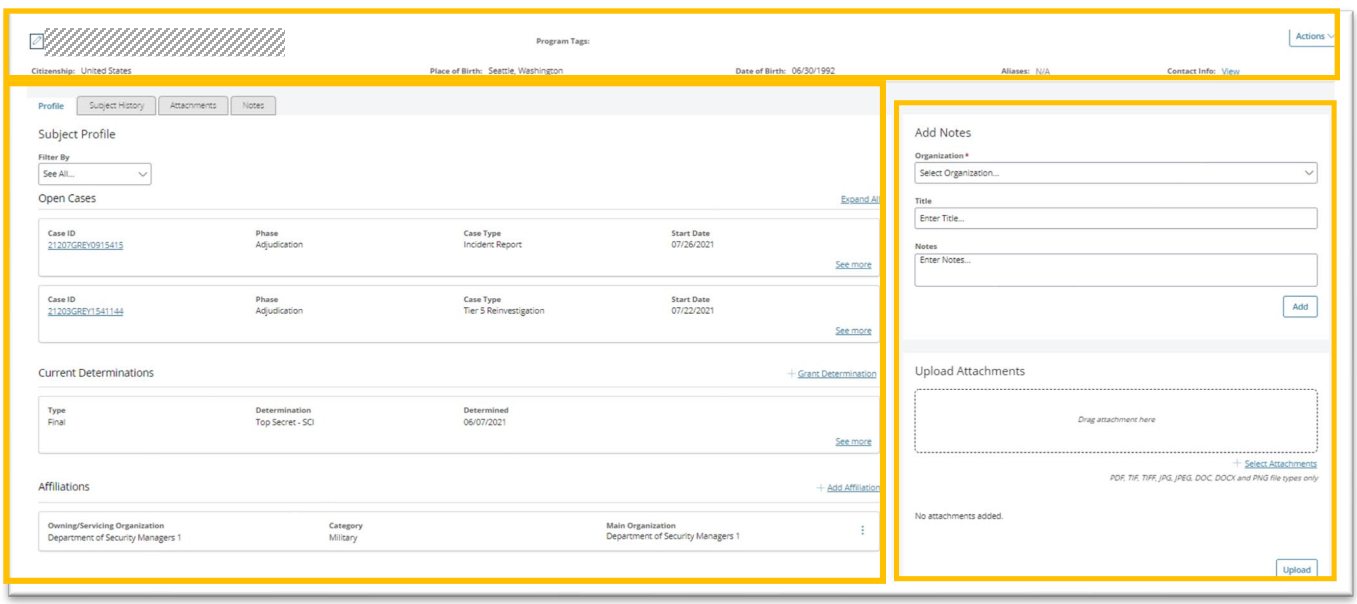
ACCESS ACTION CARDS

1. On the right, use the **Add Notes** card or the **Upload Attachments** card to add notes or documents to the **Subject Worksheet**.

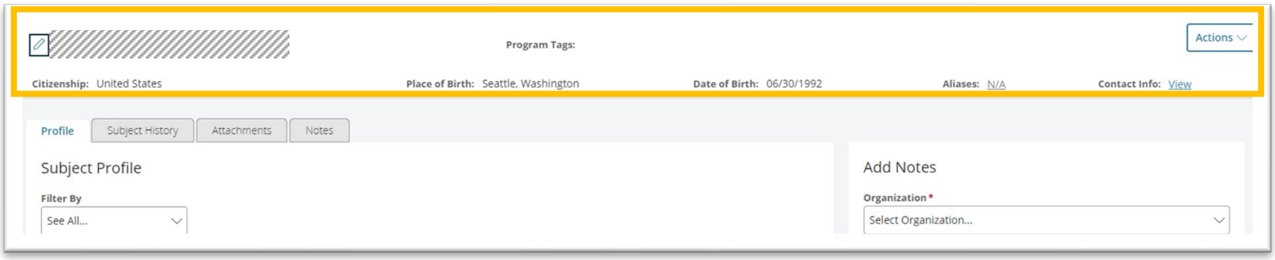
Navigate to the Subject's Worksheet (Steps 1-3)



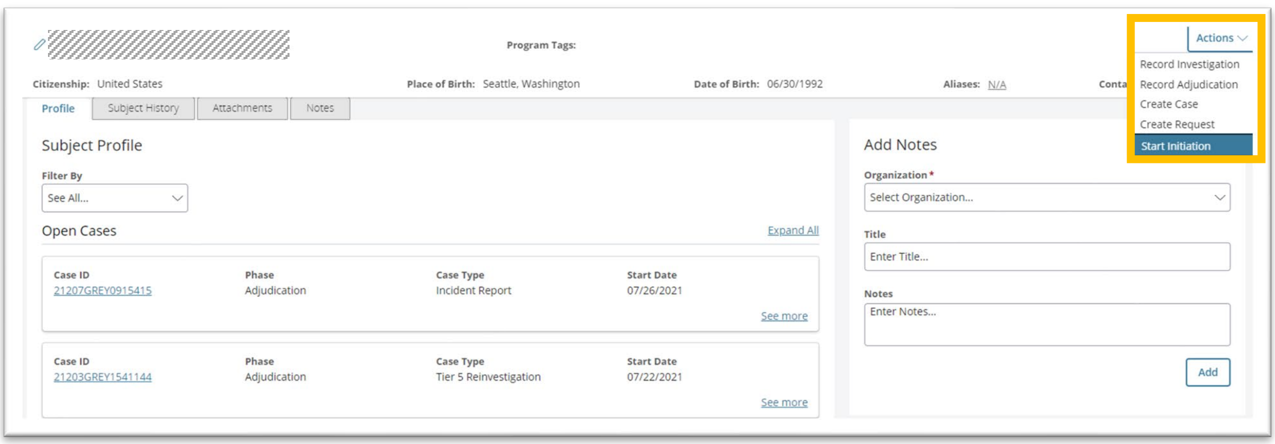
Navigate to the Subject's Worksheet (Step 4)



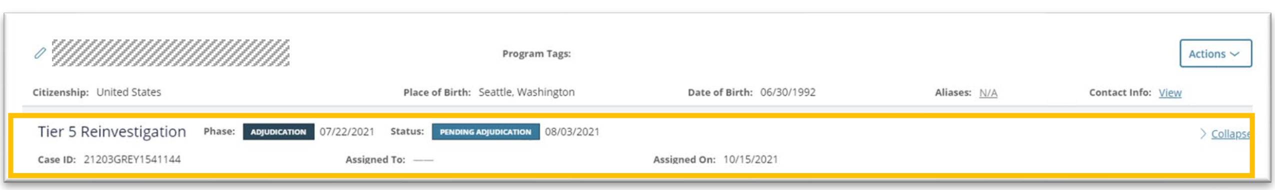
Access the Subject Banner (Steps 1-2)



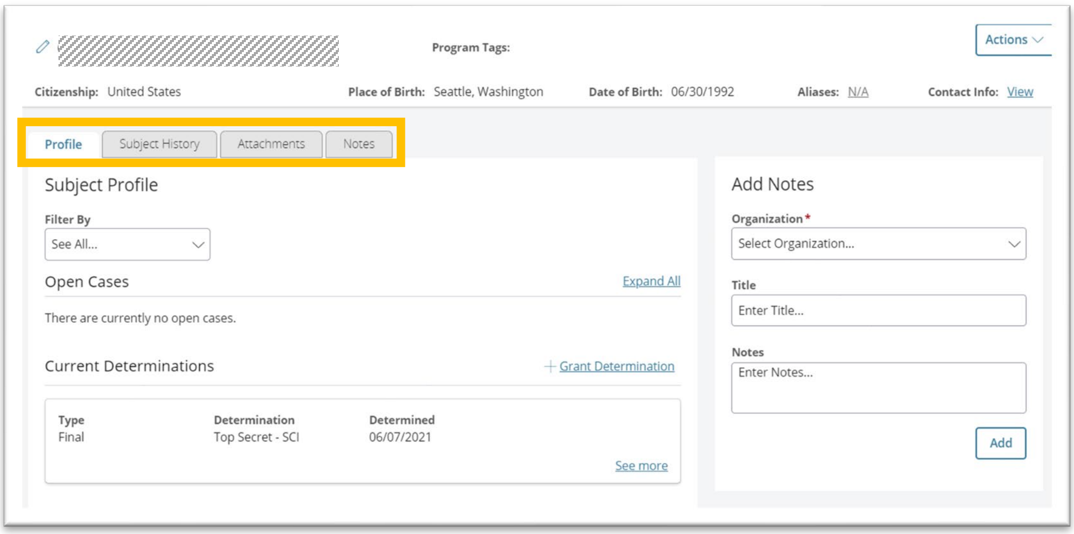
Access the Subject Banner (Step 3)



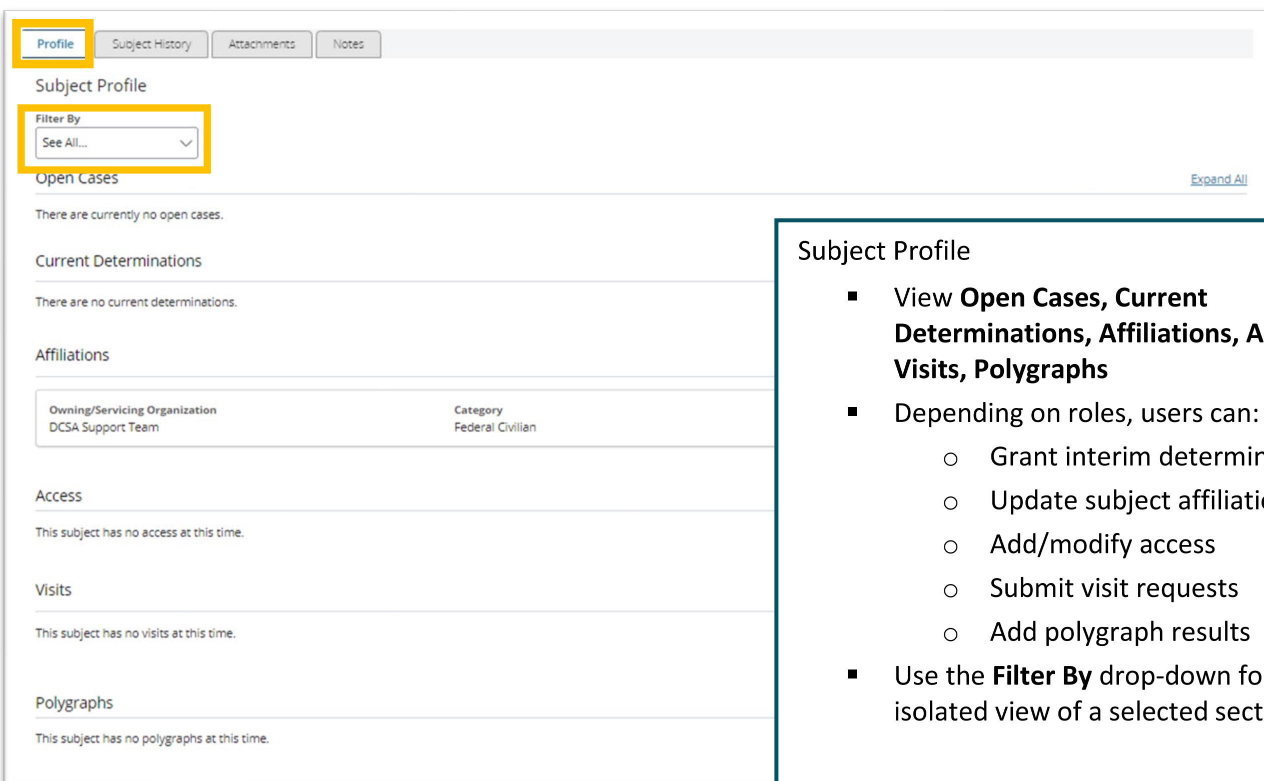
Access the Subject Banner (Steps 4-5)



Access Subject Worksheet Tabs (Step 1)

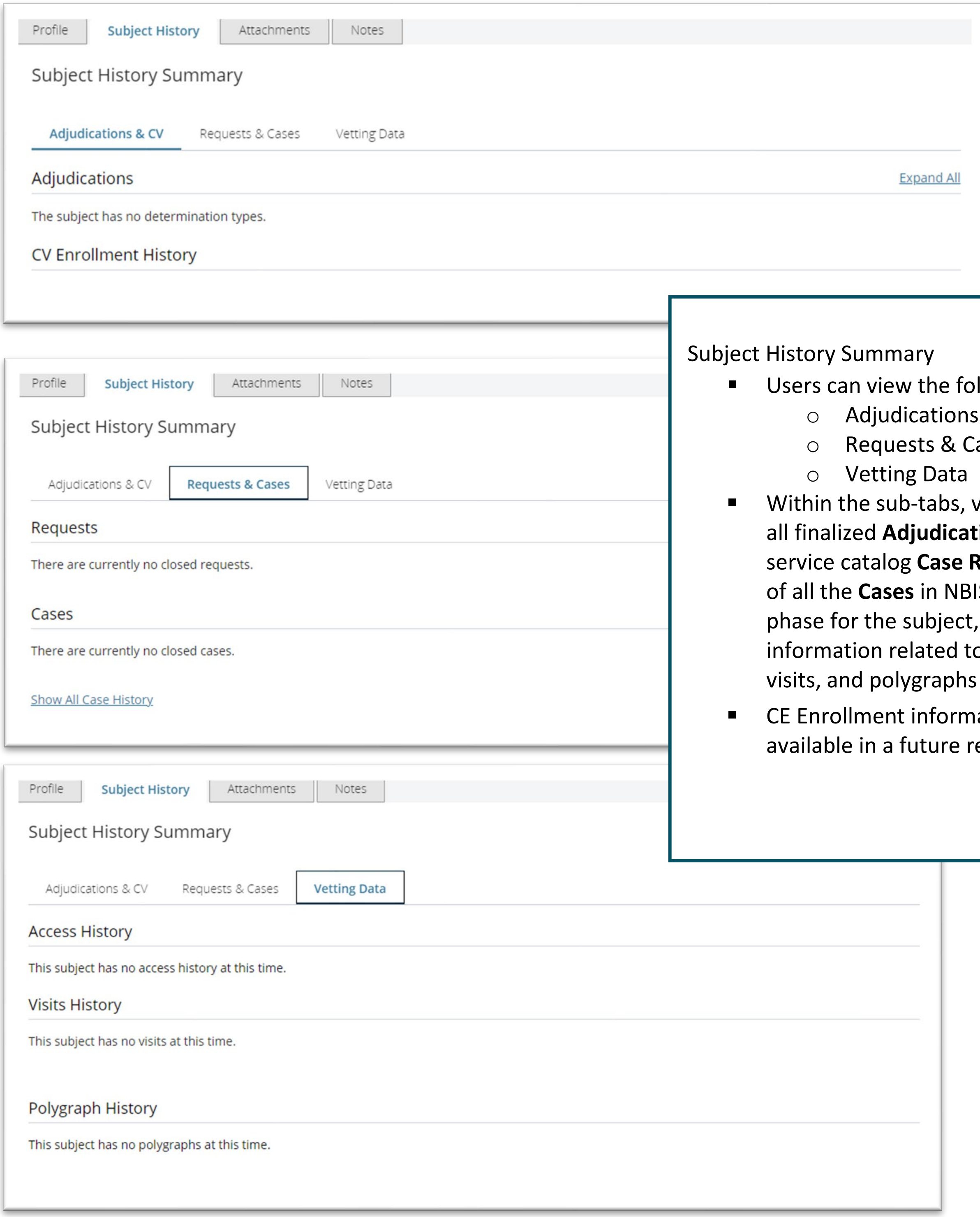


Access Subject Worksheet Tabs (Step 2)



Subject Profile

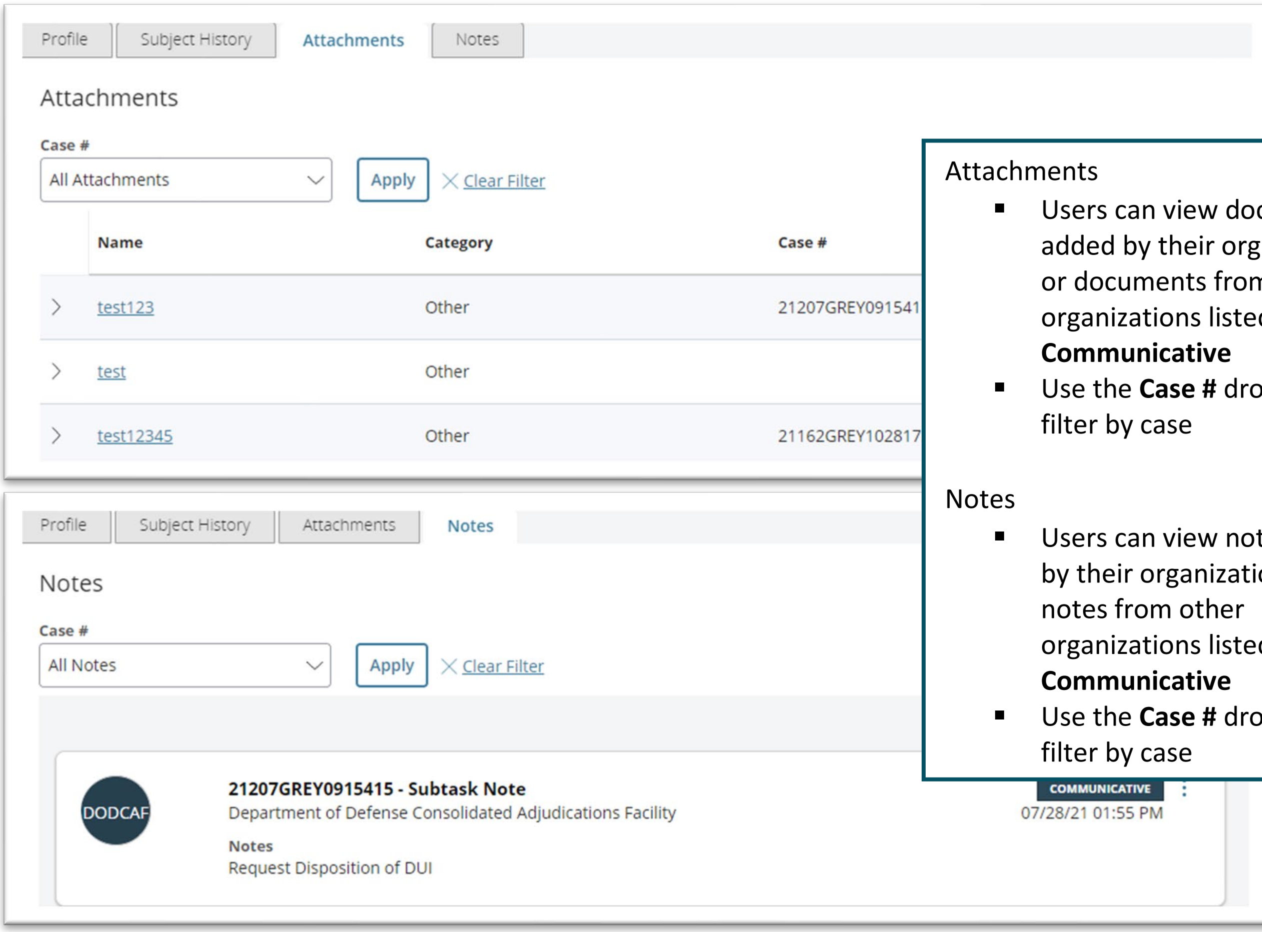
- View **Open Cases, Current Determinations, Affiliations, Access, Visits, Polygraphs**
- Depending on roles, users can:
  - Grant interim determinations
  - Update subject affiliations
  - Add/modify access
  - Submit visit requests
  - Add polygraph results
- Use the **Filter By** drop-down for an isolated view of a selected section



Subject History Summary

- Users can view the following sub-tabs:
  - Adjudications & CV
  - Requests & Cases
  - Vetting Data
- Within the sub-tabs, view a history of all finalized **Adjudication** information, service catalog **Case Requests,** record of all the **Cases** in NBIS across each phase for the subject, and **Vetting** information related to previous access, visits, and polygraphs
- CE Enrollment information will be available in a future release

Access Subject Worksheet Tabs (Step 3)



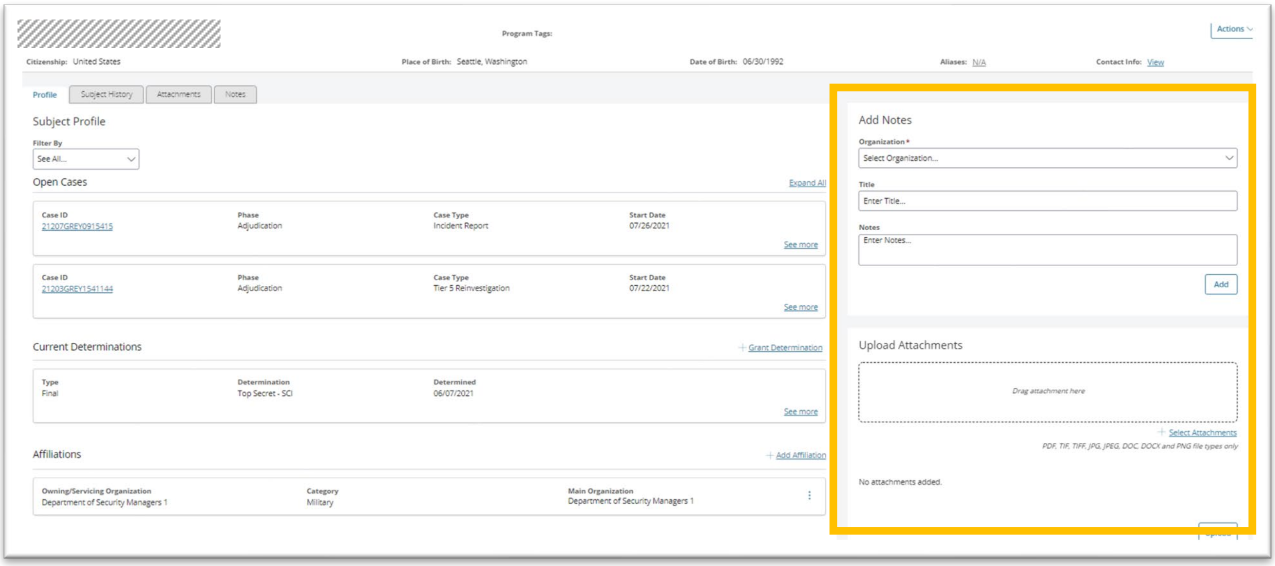
Attachments

- Users can view documents added by their organization, or documents from other organizations listed as **Communicative**
- Use the **Case #** drop down to filter by case

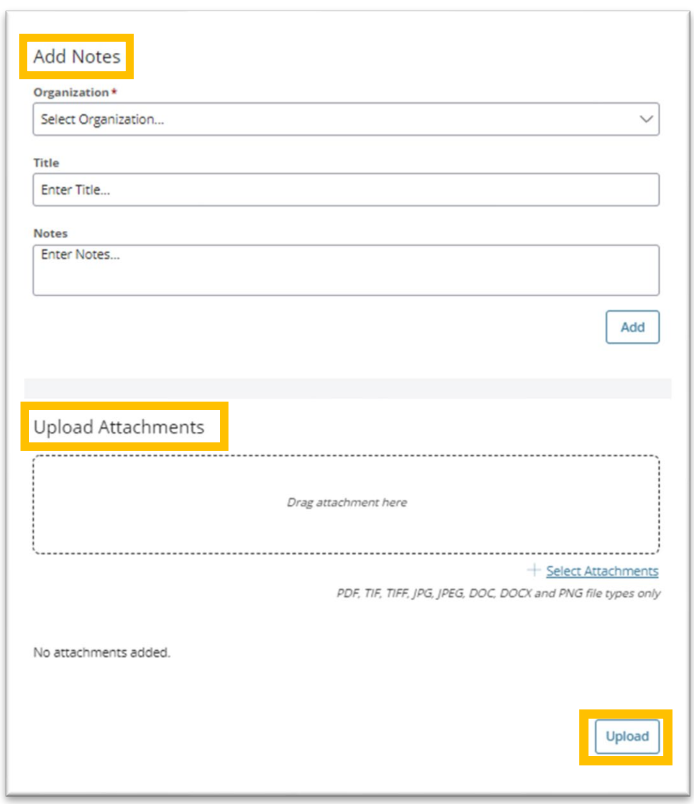
Notes

- Users can view notes added by their organization, or notes from other organizations listed as **Communicative**
- Use the **Case #** drop down to filter by case

Access Subject Worksheet Tabs (Step 4)



Access Action Cards (Step 1)



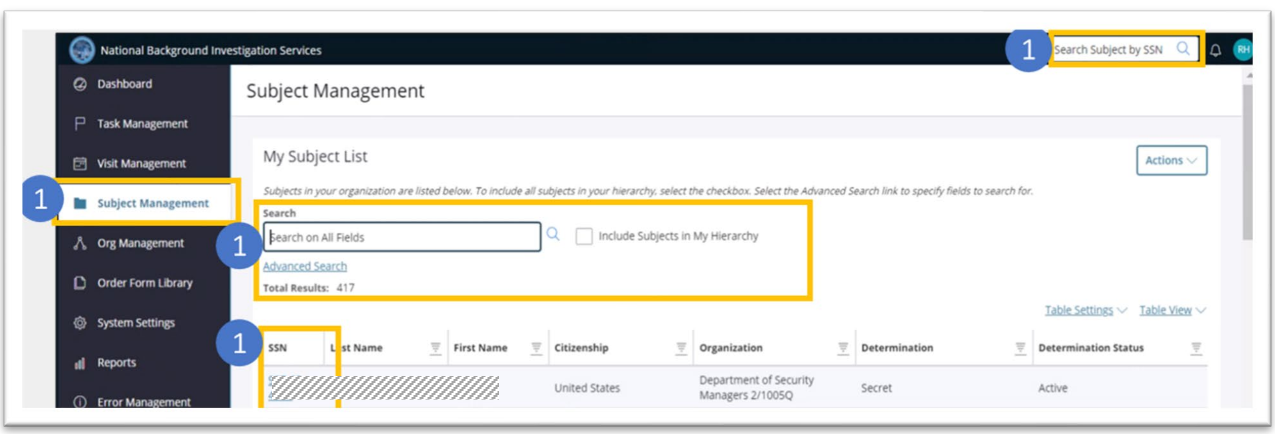
HOW TO VIEW AND EDIT A SUBJECT'S PII

Users with the Authorizer, Case Processor, Reviewer and Subject Manager roles can view and edit all fields of a Subject's Personal Identifying Information (PII), except the SSN. Users with the Program Tag Manager or Operations Manager roles can access and add Program Tags. Only users with the Subject Profile Editor role can edit a Subject's SSN. Subject Profile details include the Subject's SSN, citizenship, birth information (date and place of birth) and any applicable Program Tags.

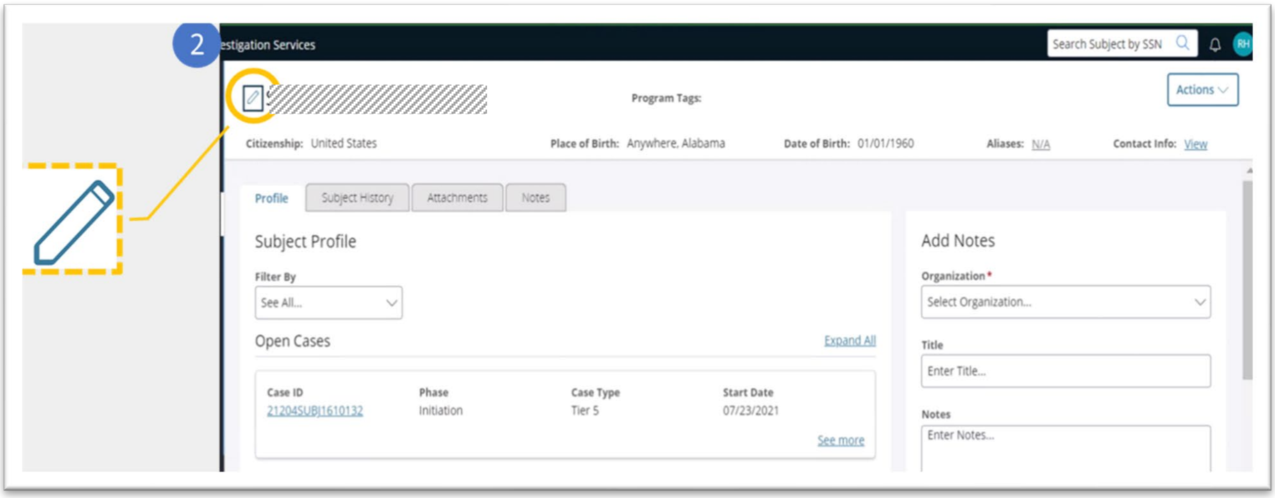
Below is the 5-step process to view and edit a subject's PII.

1. Search for the Subject's SSN and select the **SSN hyperlink** to open the Subject's profile.
2. Select the pencil icon next to the Subject's name to show the Subject's PII. Review or add any missing information about the Subject in the Subject's profile.
3. Program Tags are optional and can be associated with a Subject to route a Subject's case to specific users. Program Tags must first be configured in Organization Management and can be applied to a user's profile and the Subject's profile. Select the **Program Tag** from the drop-down menu.
4. When all required fields are completed, select **Submit** to save updates.
5. Added Program Tags will appear at the top of the Subject's profile.
6. A green success banner also shows that the Subject was updated.

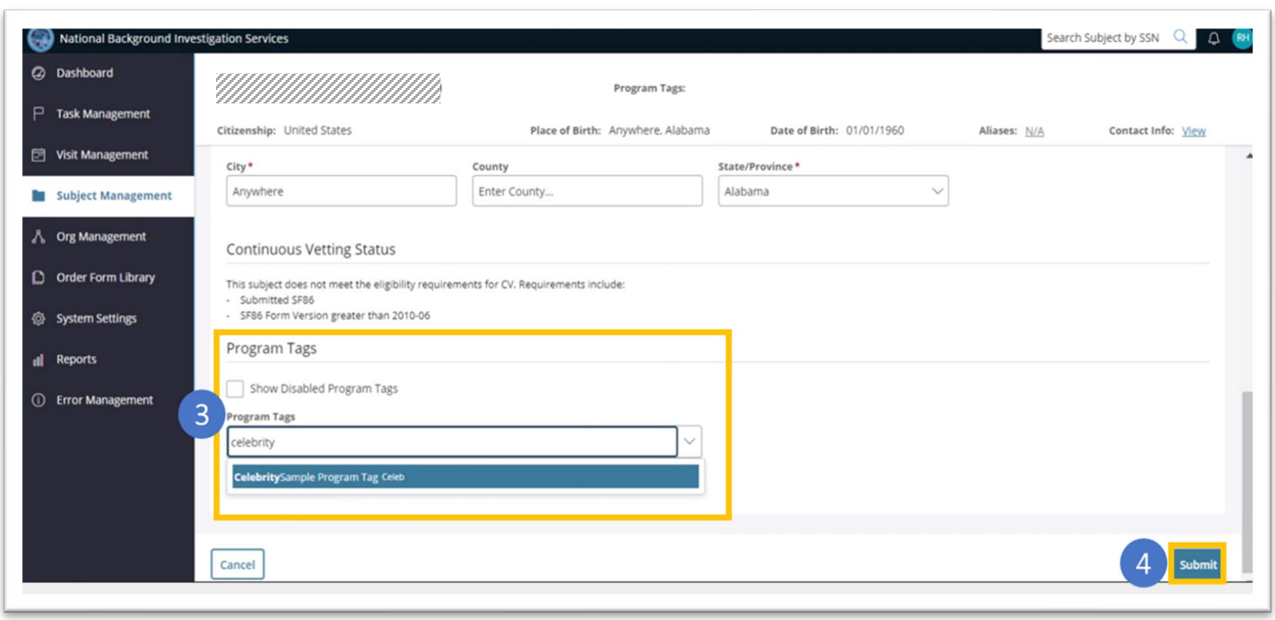
Step 1



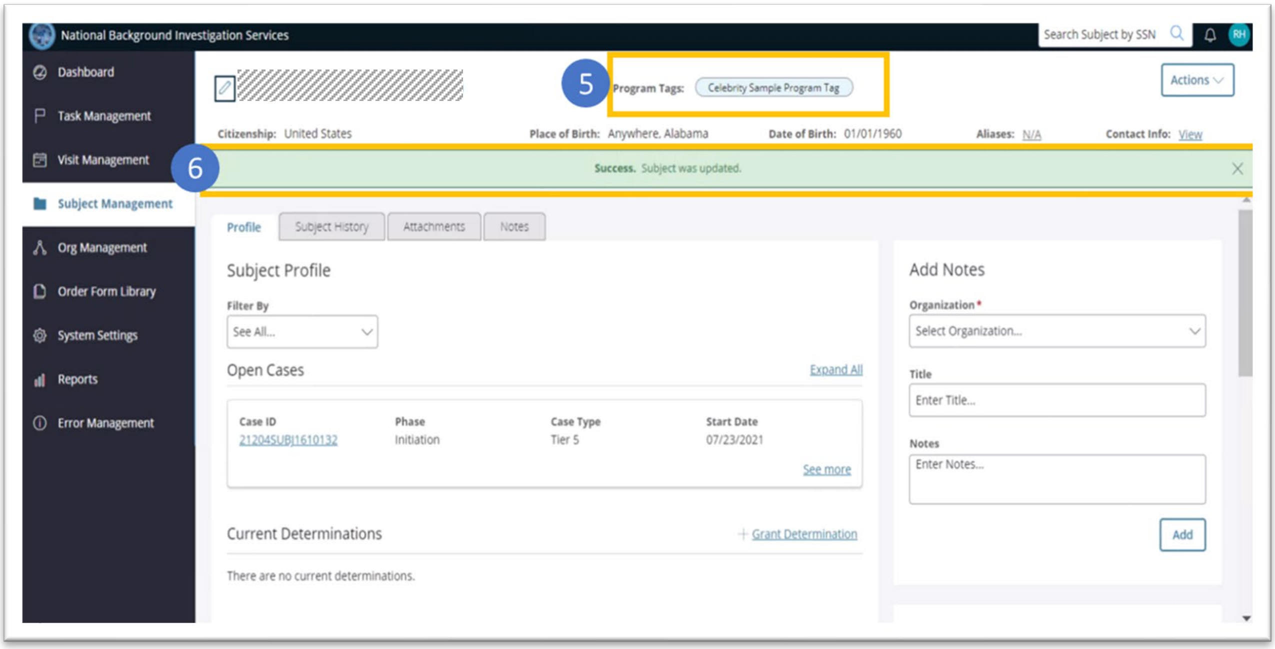
Step 2



Steps 3 and 4



Steps 5 and 6


National Background Investigation Services
Search Subject by SSN
RH
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
5
Program Tags:
Celebrity Sample Program Tag
Actions
Citizenship: United States
Place of Birth: Anywhere, Alabama
Date of Birth: 01/01/1960
Aliases: N/A
Contact Info: View
6
Success. Subject was updated.
Profile
Subject History
Attachments
Notes
Subject Profile
Filter By
See All...
Open Cases
Expand All
Case ID
21204SUBJ1610132
Phase
Initiation
Case Type
Tier 5
Start Date
07/23/2021
See more
Current Determinations
Grant Determination
There are no current determinations.
Add Notes
Organization *
Select Organization...
Title
Enter Title...
Notes
Enter Notes...
Add

HOW TO INITIATE A CASE REQUEST

There are two ways to initiate a case request. The first is for individual subject cases and the second is through the mass initiation process.

INITIATE A CASE REQUEST

Users with the Initiator, Subject Manager and Facility Security Officer (FSO) roles can create and search for Subjects, initiate Subject case requests, complete routing details, and edit order form details before receiving the Subject's Standard Form (SF) back from eAPP. Once the case request is initiated, form routing details are set and cannot be changed. If information was entered incorrectly when the case was initiated, then this case should be cancelled, and a new case request should be created.

Below is the 7-step process to initiate a case request.

1. From **Subject Management**, select the SSN of the subject for which you would like to initiate a case. Navigate to the "**Actions**" drop-down in the top right-hand corner.
2. Select "**Start Initiation**." Note: Users with the Initiator role do not require an affiliation to the Subject to start initiation. Organizations and workflows in Routing Details will be determined based on the Initiator's affiliation.
3. Use the drop-down menus to input the "Initiation Routing Details." There are three required fields: Initiating Organization, Workflow Type, and Form Type. Select the **Initiating Organization** from the drop-down menu.
4. Select the **Workflow Type** drop-down menu. A Workflow Template must already exist/have been created for the Org.
5. Select a **Form Type** from the drop-down menu. Select "Continue" after selecting the Form Type. Note: The Form Type drop-down options include: SF85, SF85P and SF86. The Case Type will auto-populate based upon the Form Type selected.
6. There is an optional checkbox for "**Send to Review Organization**." This checkbox will route the initiation immediately to the Review Organization. Once routed, a user will not be able to make any further updates on this initiation. If the checkbox is NOT selected, the Subject Manager or Initiator roles may update the case and manually send it to the Reviewer. Note: The Form Routing must be enabled in the Initiating Organization's Form Routing/Workflow, located in the Configuration Menu under Form Routing.
7. Select "**Continue**" to create a case request. A green success banner will appear that the case has been routed. Once you have successfully initiated the case, the case will move to the Review phase on the Position Details Tab. Two emails will be sent to the Subject with instructions on how to log into eAPP to complete the appropriate SF Form. The first email will have their eAPP link and username; the second email will have the eAPP link and temporary password.

- Note: If the user's organization is not authorized to Review, the case will move to the Reviewing organization. If the user is not authorized to Review, the case will move to the My Organization's Work tab under Task Management

MASS INITIATION PROCESS

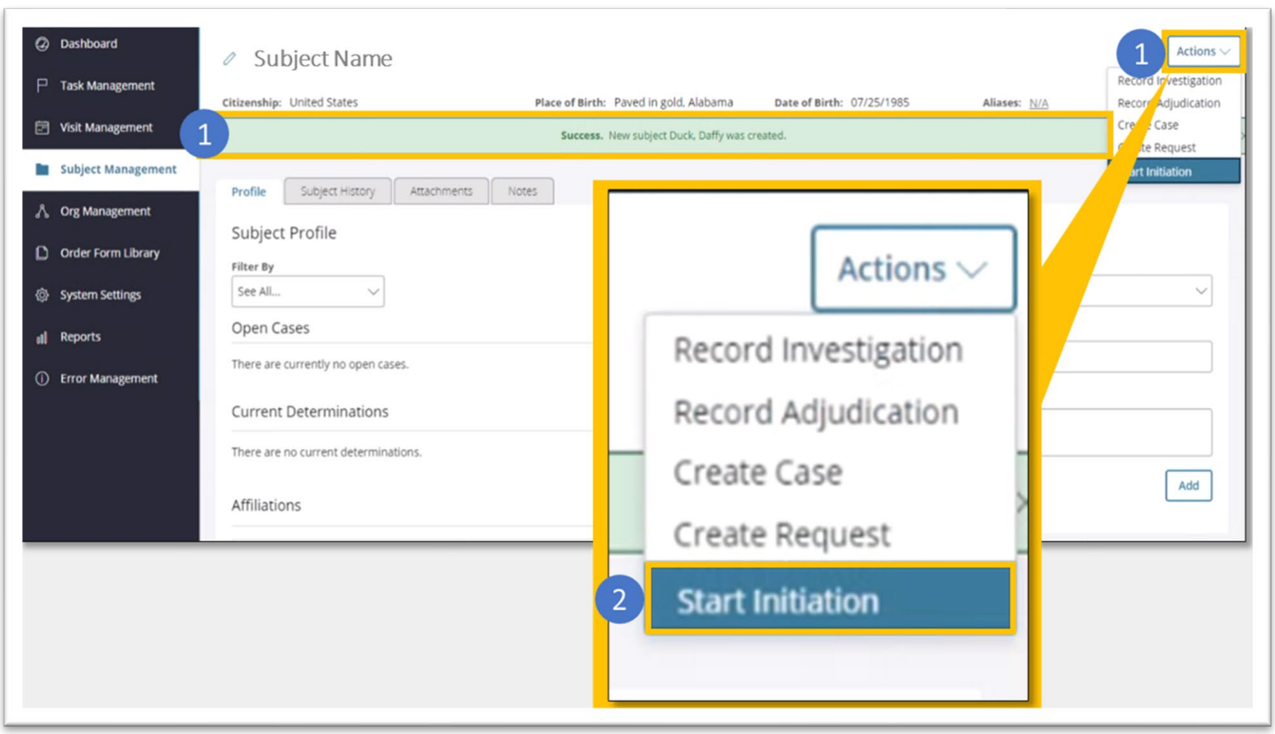
When entering and processing Mass Initiations, this workflow process supports the creation of multiple Subject case requests at once by uploading a CSV spreadsheet list of Subjects and their PII. This capability is available for users with the Subject Manager roles.

Below are the 19 steps to complete Mass Initiation.

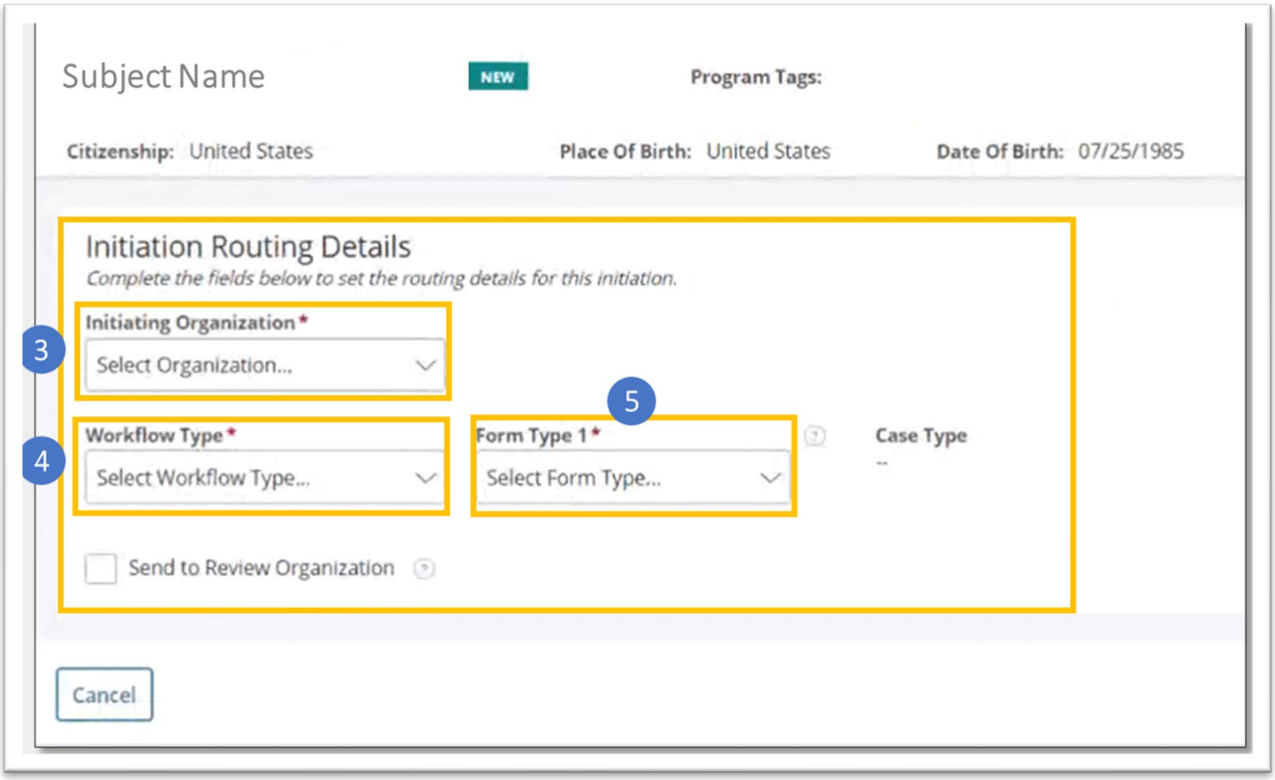
1. From the **Subject Management** tab, navigate to the "**Actions**" drop-down menu and select Mass Initiate Subjects.
2. In the Setup Org Associations page, use the **blue hyperlink** to download the template file and/or the Mass Initiation CSV template file. Add the Subject data and save the CSV file for uploading. Note: The subjects' first and last names in the CSV file must match the subject information in NBIS.
3. In the Setup Org Associations page, select the **+Add Owning Organization hyperlink**. Use the drop-down menus to select the Residing Organization and Organization Affiliation. Depending on the Residing Organization selected, the Organization Affiliation will auto populate.
4. If necessary, use the ellipses to select "Add Servicing Organization." Use the drop-down menu to select the **Residing Organization** and **Organization Affiliation**. Note: The Grouped Level Organization field will populate based on the Residing Organization selected. If the Residing Organization is a Grouped Level Org, then the two fields will be the same. Facility Security Officer roles will only be able to select "Contractor" for an Org Affiliation.
5. If performing Mass Affiliation and not initiating subject cases, select the checkbox for "**Create Subjects Only and Skip Initiation**."
6. Select **Continue** to proceed to the Setup Tier and Template tab.
7. In 2. **Setup Tier and Template tab** select the Initiating Organization from the drop-down menu options. Choose a Workflow Type (a Form Routing Template) and Form Type (SF8X). A Workflow Template must already exist/have been created for the Org.
8. Select **Continue** to proceed to #3. Upload File.
9. In 3. **Upload File tab**, select "upload file" and then "browse."
10. Locate and select the saved CSV template file on the computer. Select **Open** to upload the saved file. The uploaded file will appear in a list below "File Name."
11. Select **Continue**.
12. Select the **Error tab** to display any errors. From the Details column, select **View** to display additional information about the Subject and errors.
13. Check "**Include Validation Messages**" so the specific error information will be included when exporting the CSV.
14. Select "**Export to CSV**" and ensure that the Subjects and their error validations are captured outside the system.

15. Navigate to the **Valid and/or Warning tabs** and uncheck any Subjects to exclude them from the mass initiation process. Note: A "warning" will still allow you to start processing, however an error will not.
16. From the Details column, select **View** to display additional information about the Subject.
17. Select **Start Processing**.
18. A list of successful cases with case numbers or failed case initiations will be displayed. Users can view info about cases in the Details column.
19. Select **Close** to successfully close out the Mass Initiation case and receive visual confirmation that mass initiation is completed. Select Close to return to My Subject List in Subject Management.

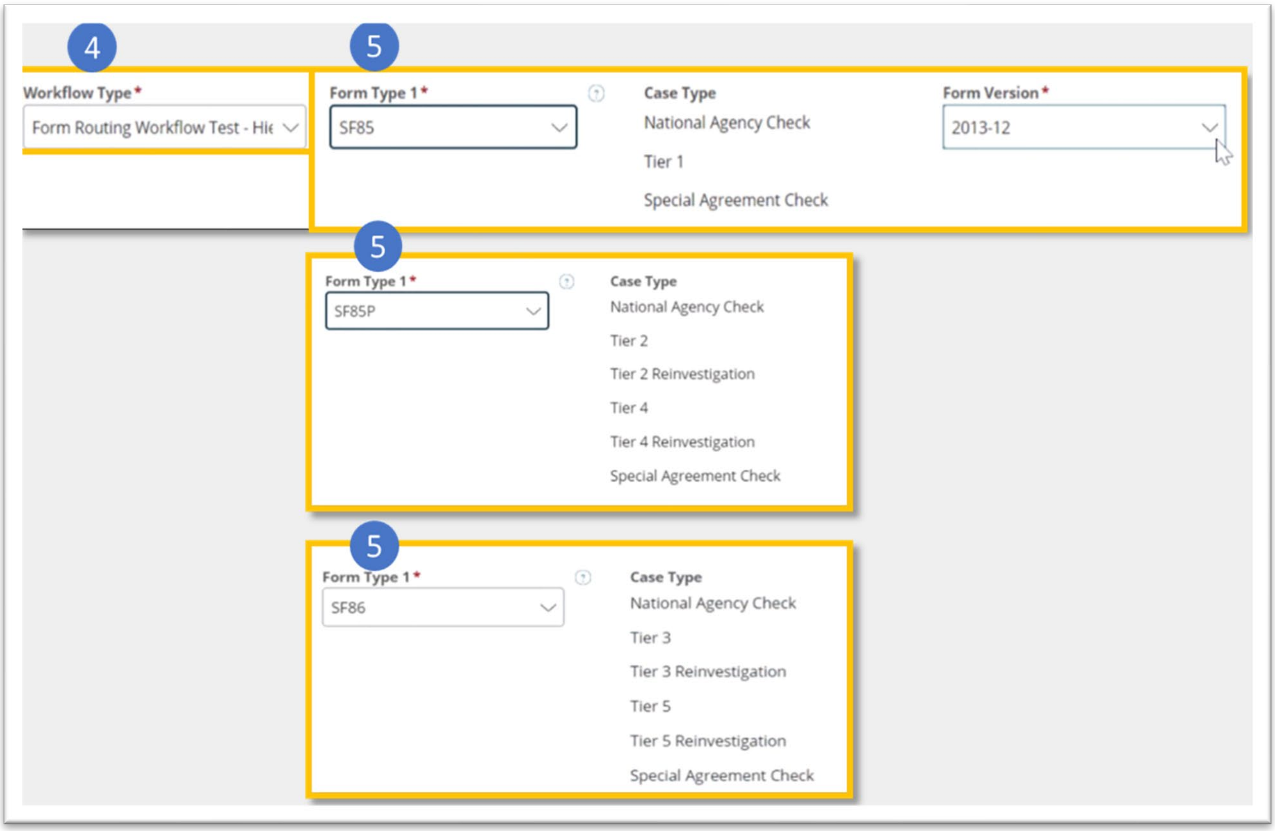
Initiate a Case Request (Steps 1-2)



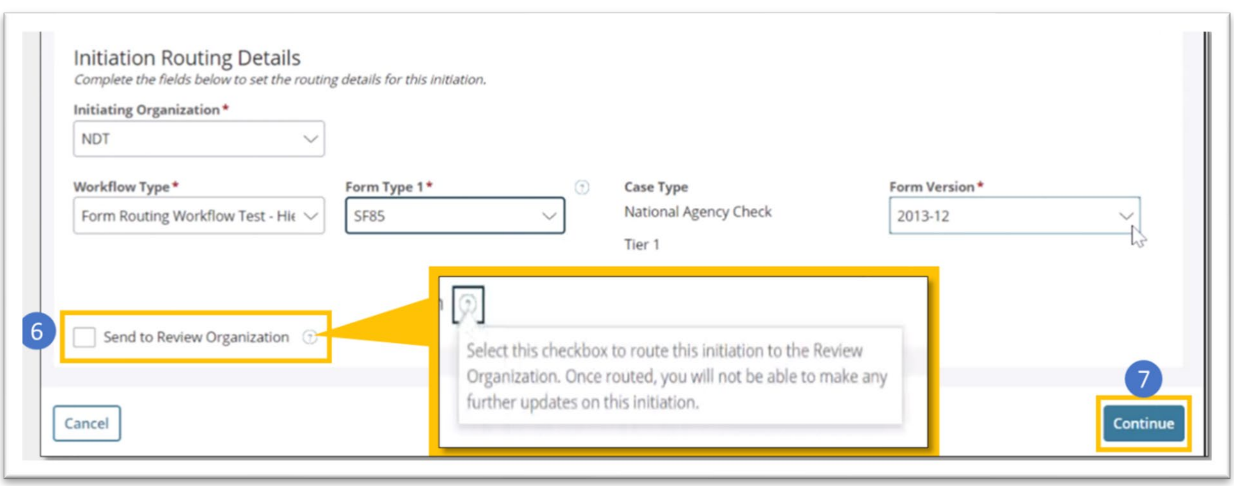
Initiate a Case Request (Steps 3-5)


Subject Name
NEW
Program Tags:
Citizenship: United States
Place Of Birth: United States
Date Of Birth: 07/25/1985
Initiation Routing Details
Complete the fields below to set the routing details for this initiation.
3
Initiating Organization *
Select Organization...
4
Workflow Type *
Select Workflow Type...
5
Form Type 1 *
Select Form Type...
Case Type
--
Send to Review Organization
Cancel

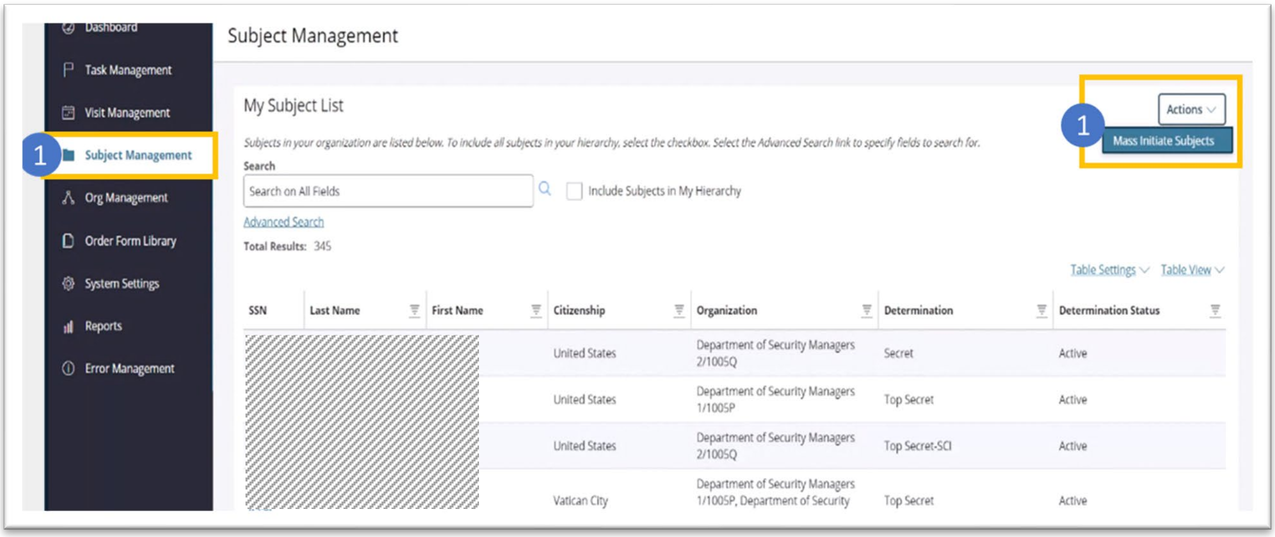
Initiate a Case Request (Steps 4-5 Continued)



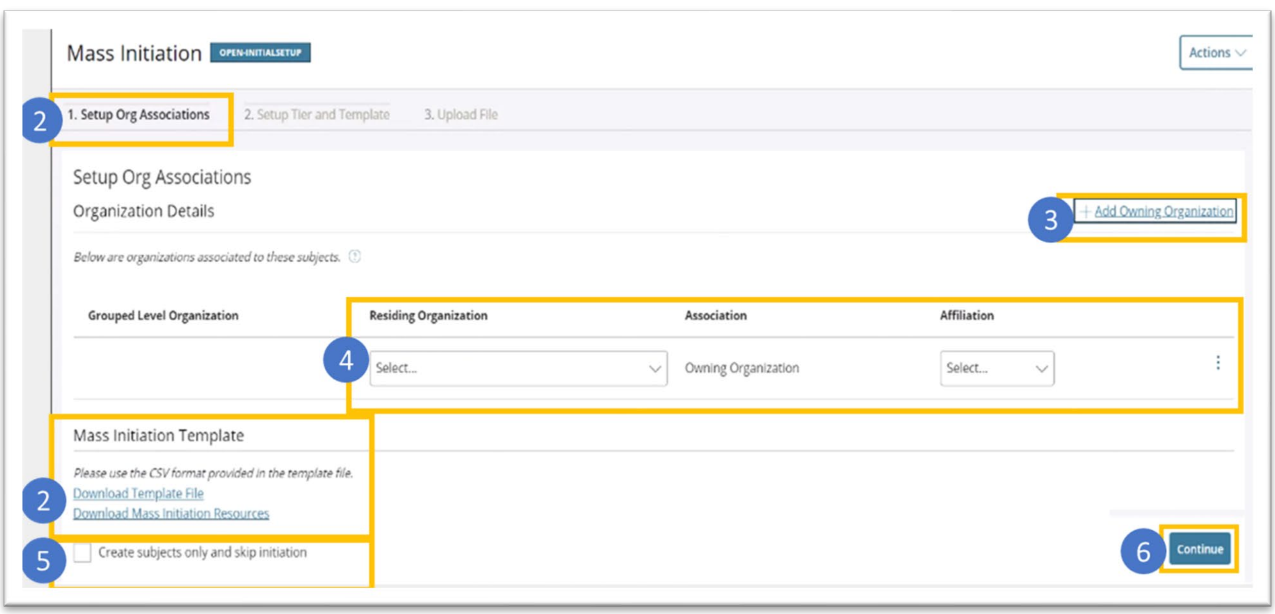
Initiate a Case Request (Steps 6-7)



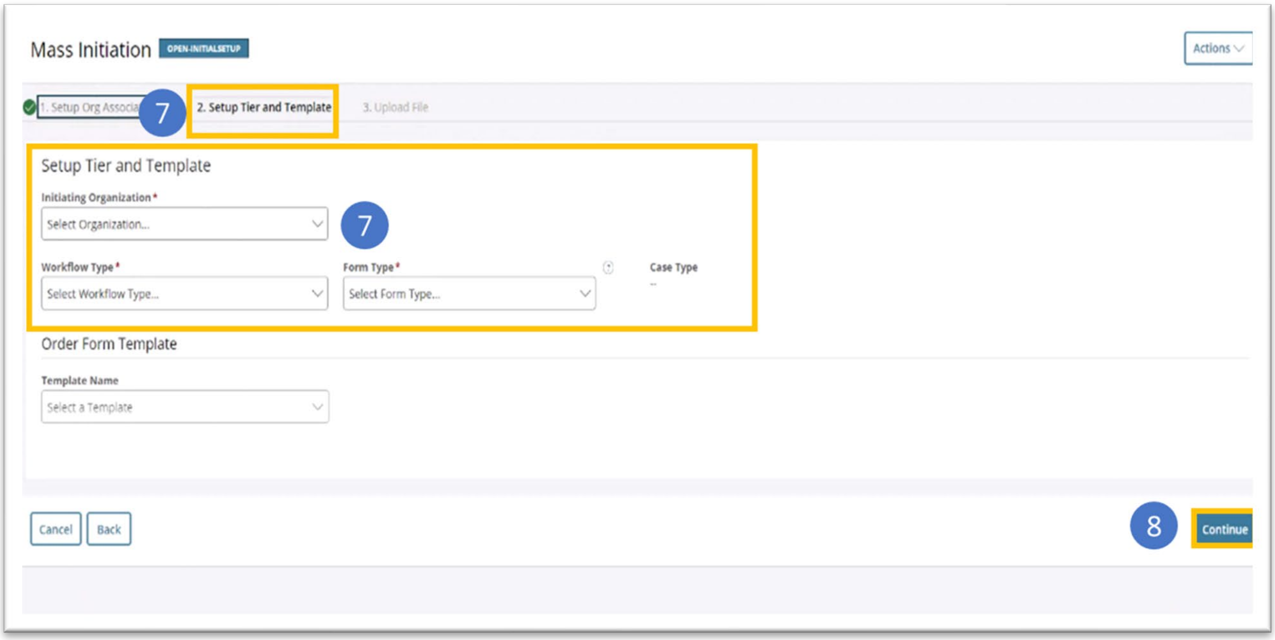
Mass Initiation Process (Step 1)



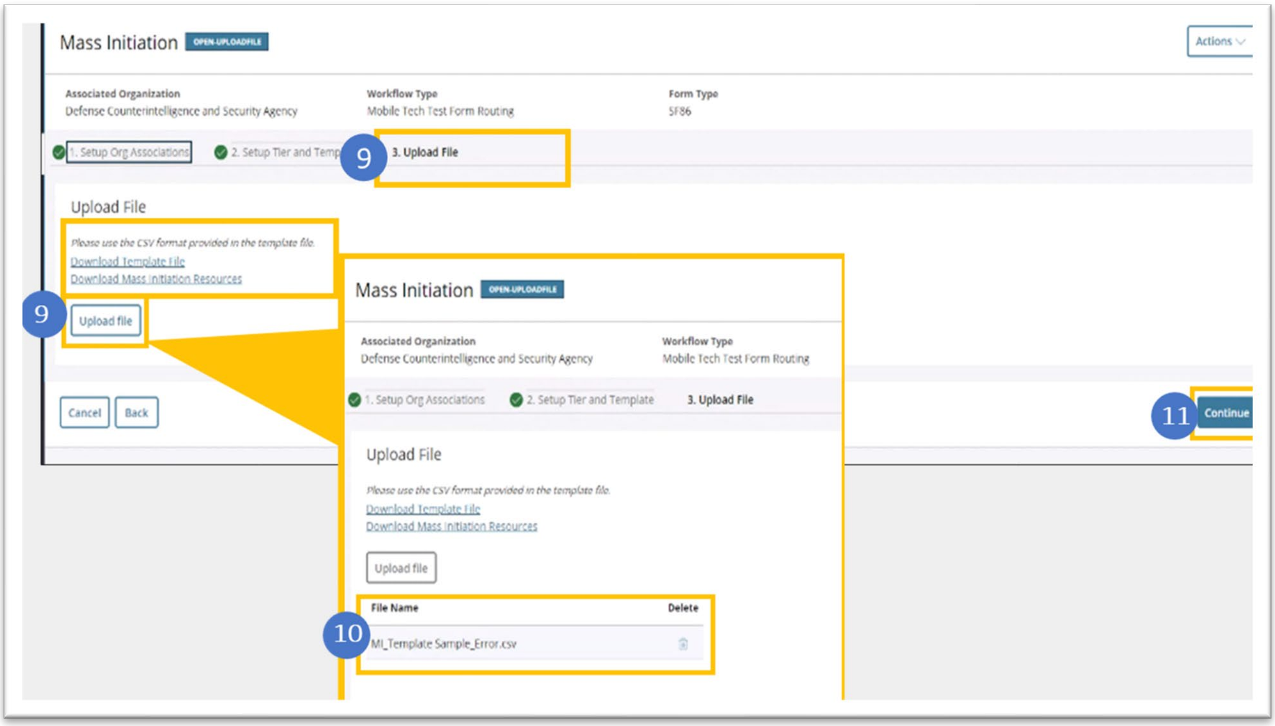
Mass Initiation Process (Steps 2-6)



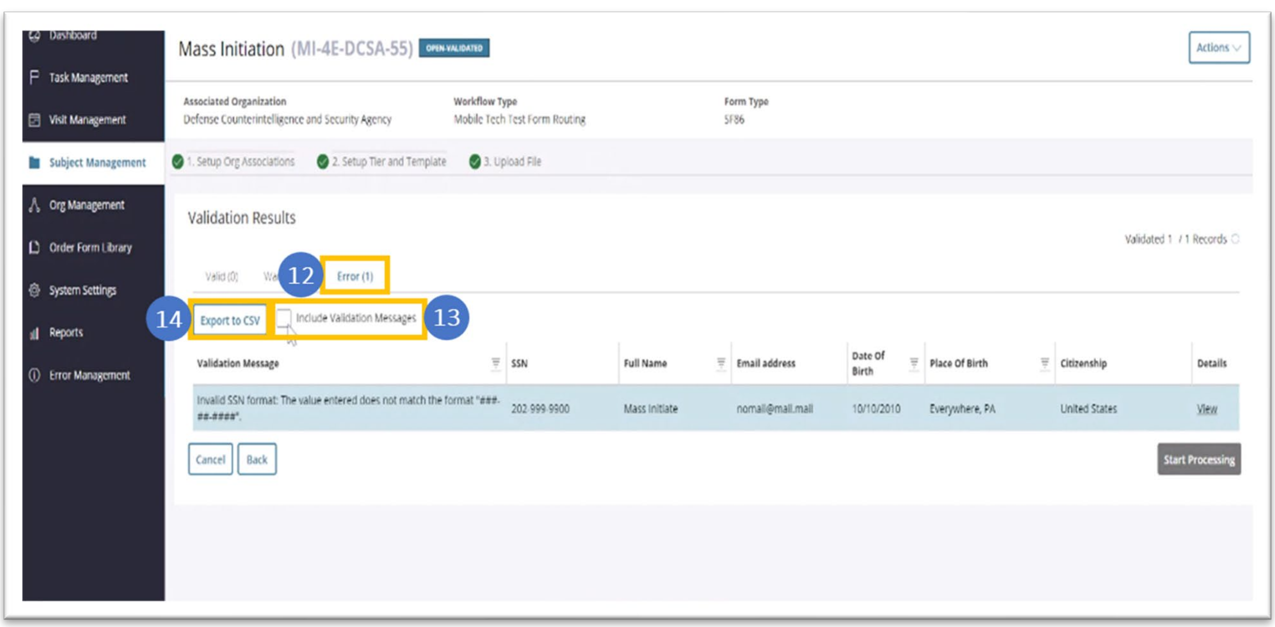
Mass Initiation Process (Steps 7-8)



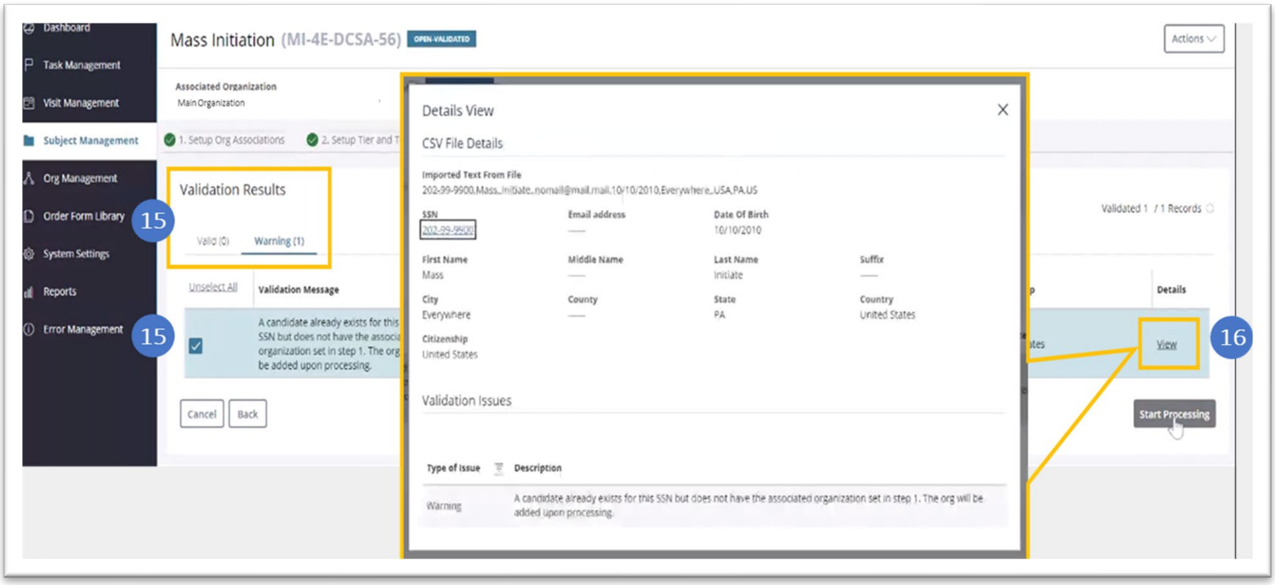
Mass Initiation Process (Steps 9-11)



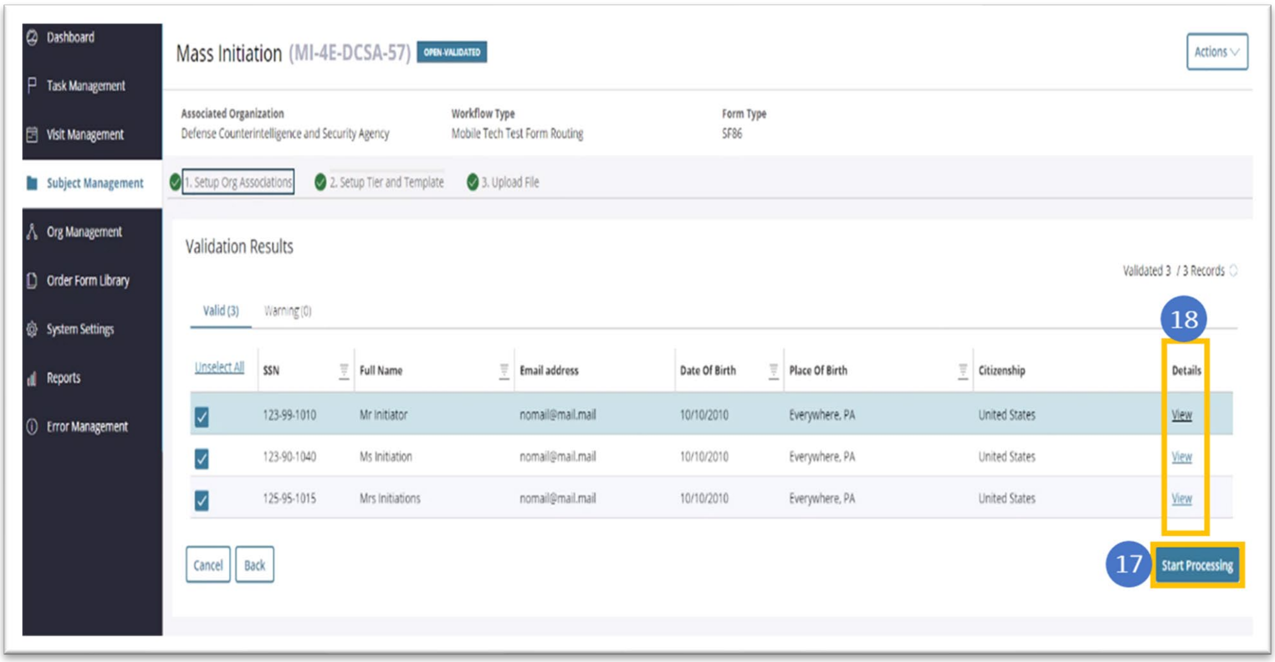
Mass Initiation Process (Steps 12-14)



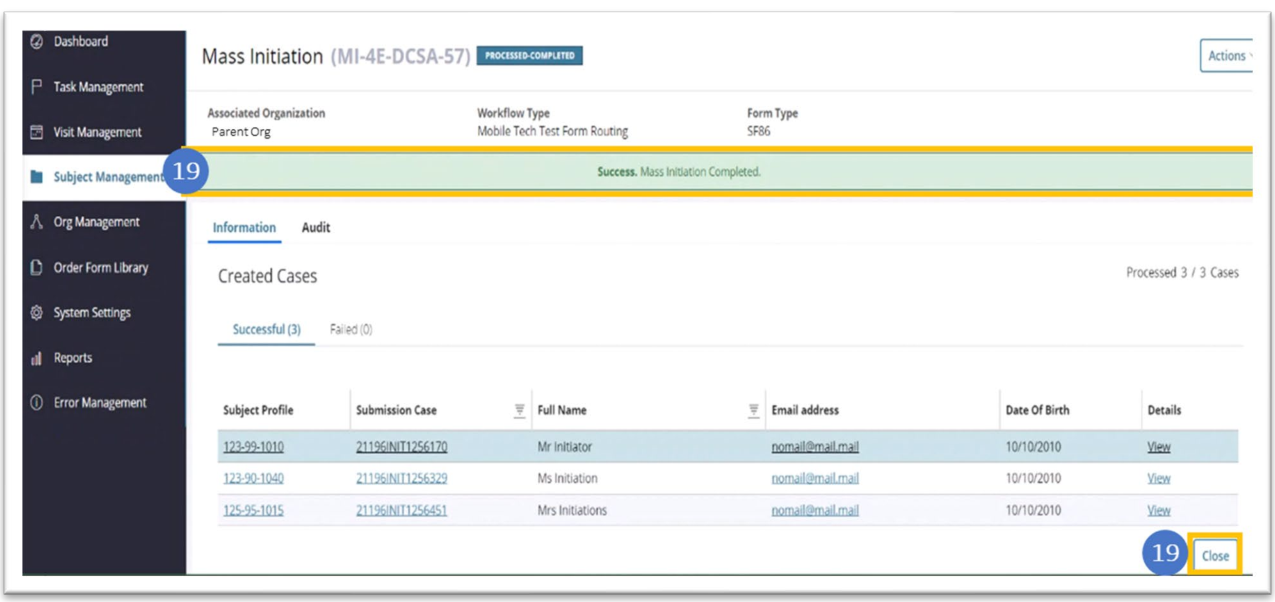
Mass Initiation Process (Steps 15-16)



Mass Initiation Process (Steps 17-18)



Mass Initiation Process (Step 19)



HOW TO REVIEW A CASE REQUEST

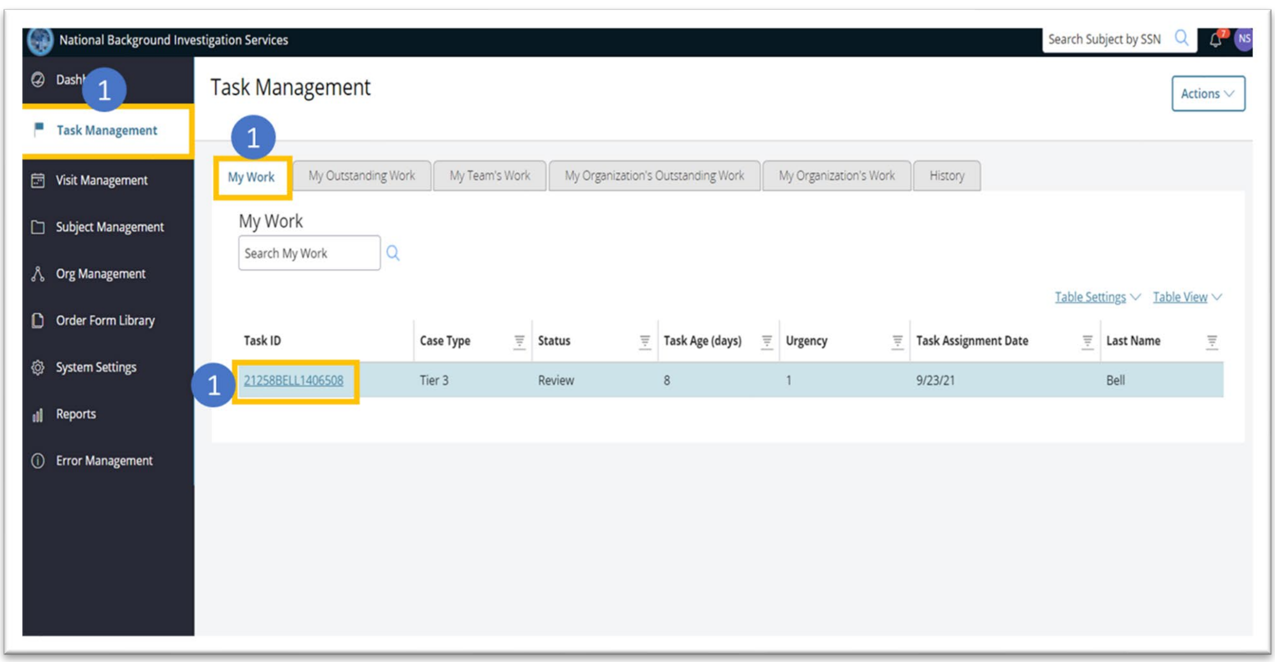
There are two steps to reviewing a case request. The first is completing the Position Details and Optional Coverage. The second step is updating incomplete or incorrect subject data.

COMPLETE POSITION DETAILS AND OPTIONAL COVERAGE

Users with the Reviewer role can select a case to review and use an Organization's Order Form Template to streamline the review process. Users with the Reviewer role are required to complete the Position Details and Optional Coverage tab sections. Additionally, the Position Details section is optional for Facility Security Officers, Initiators, and Subject Manager roles. Authorizer roles can edit the Position Details tab after the Reviewer has completed this section. Prior to completing a Subject's case, the SSC Org must first configure a Form Routing Workflow from the Configuration Menu in the Org Management tab.

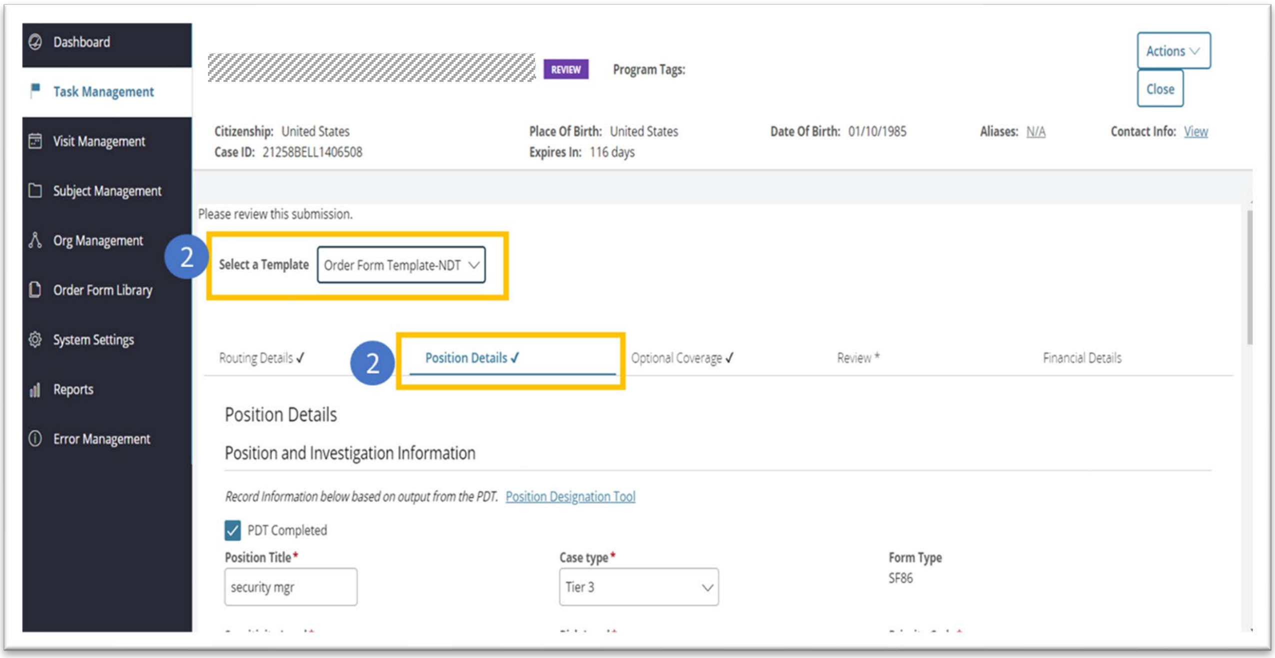
Below is the 4-step process to complete position details and optional coverage for a case request in the Review Phase.

1. From the Task Management tab, navigate to the **My Work** tab. Select the Task ID hyperlink to open the Subject's Case Request. A case first needs to be assigned to a user in order to assign an Order Form Template.

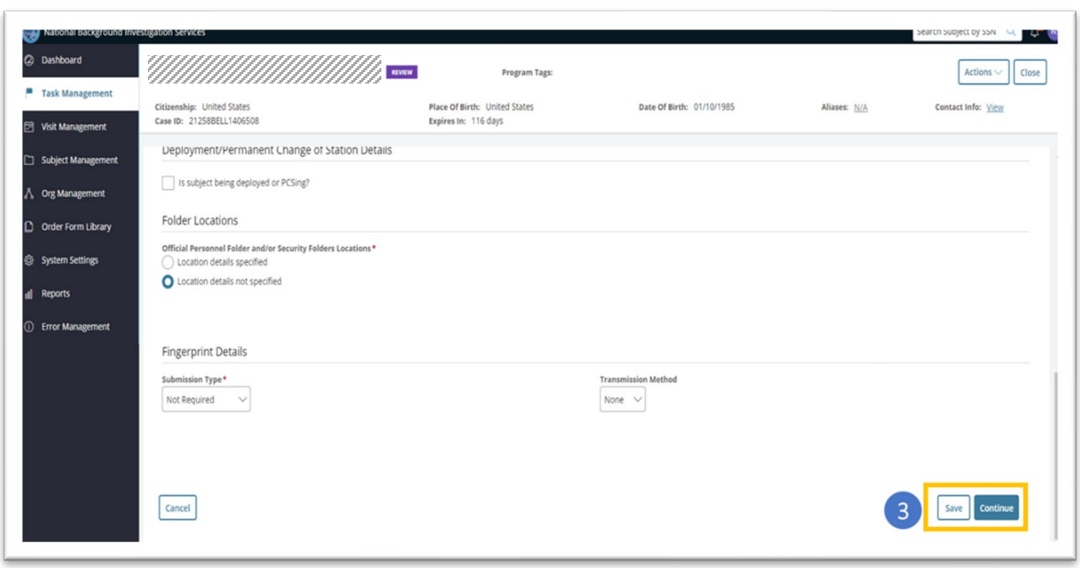


2. The **Position Details** tab of a Subject's Order Form automatically opens for the Reviewer to complete all required fields. Select an **Order Form Template** from the "Select a Template" drop-down menu. If no template is available, manually complete all the necessary Position and

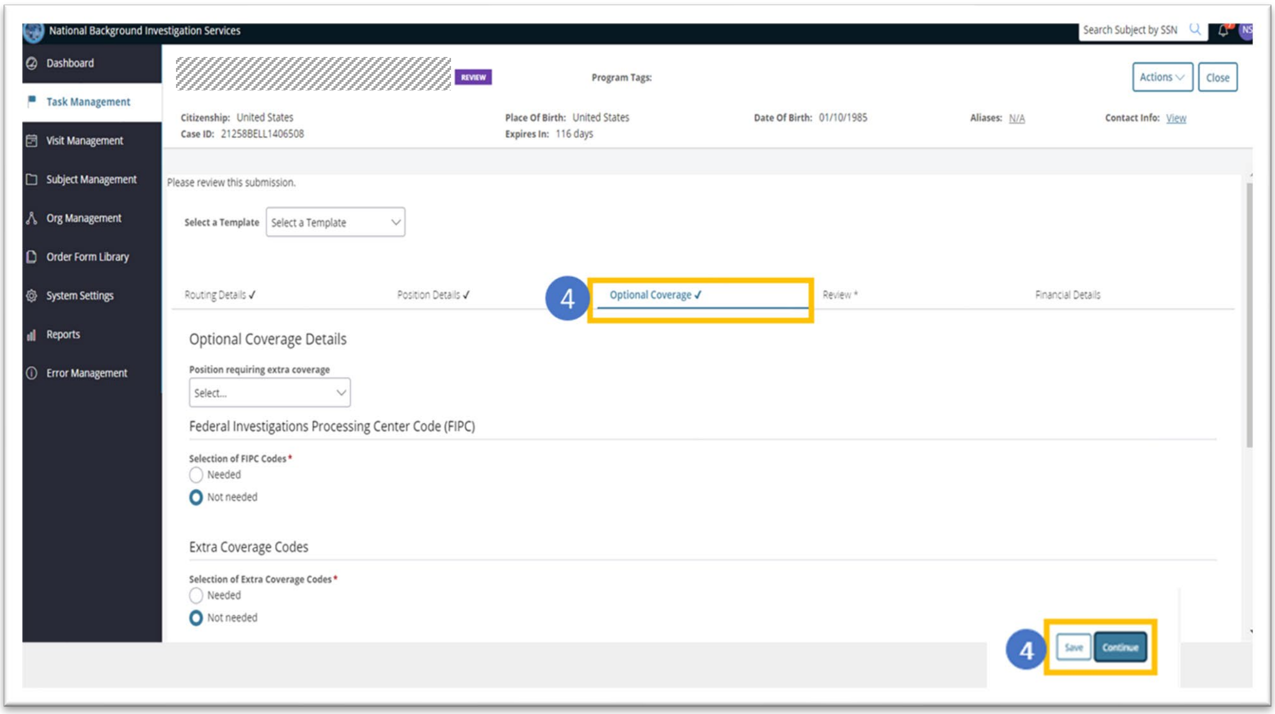
Investigation information. Any changes made to the case request will not change the selected Order Form Template.



3. Select "**Save**" or "**Continue**" to continue making case updates.



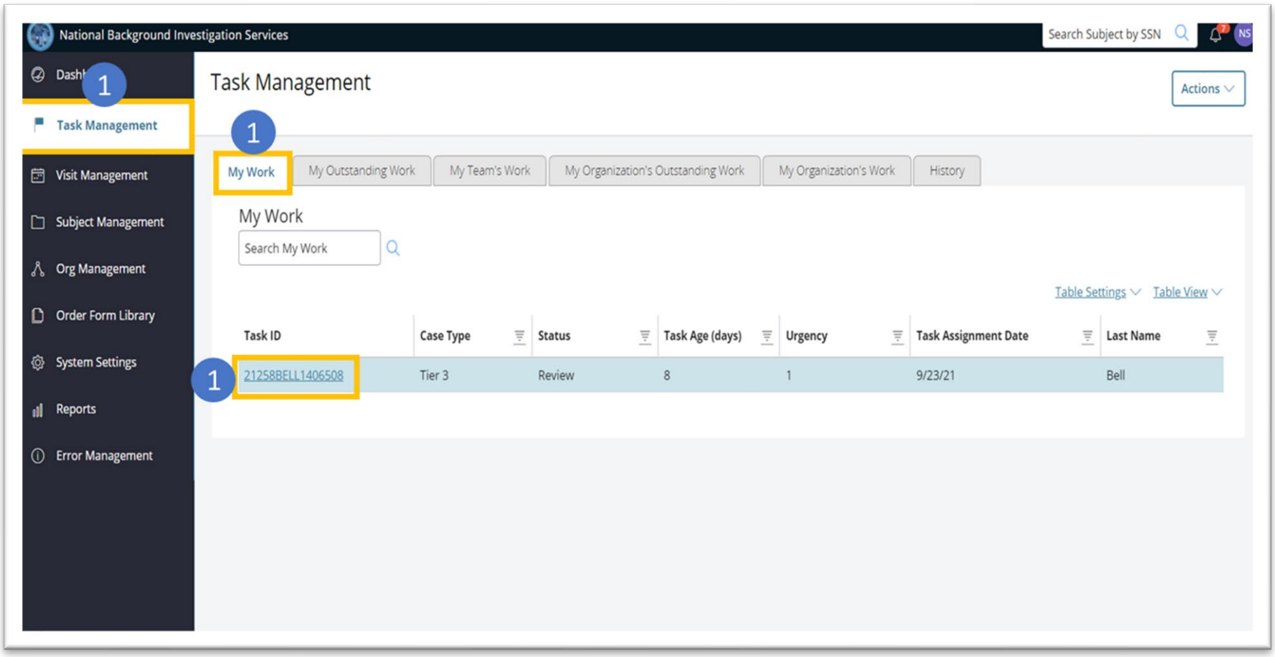
4. Select "**Optional Coverage**" to make any changes or additions. Once complete, select "**Continue**" at the bottom of the page.



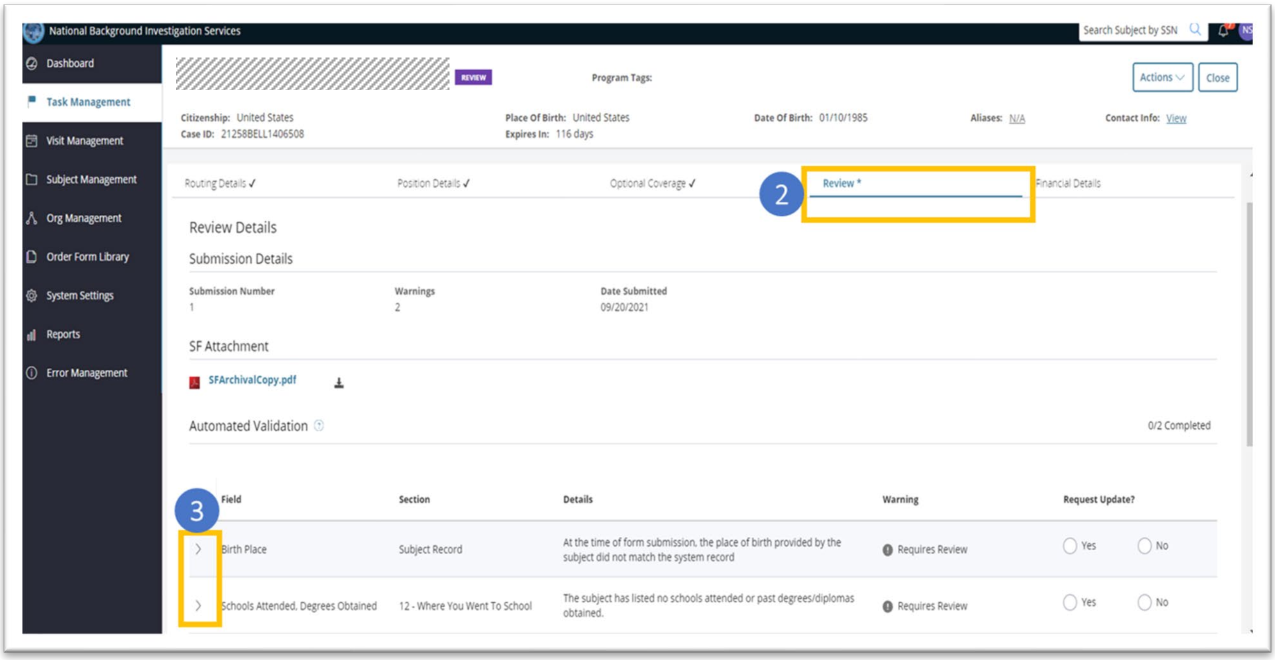
UPDATE SUBJECT RESPONSES

Assigned cases are accessible to users with the Review or Authorize roles from the Task Management tab. Within a Subject's case request, the Review tab will automatically identify potential issues with the case request, such as incomplete or incorrect Subject data. Below is the 4-step process to review a subject's case request from the Task Management tab.

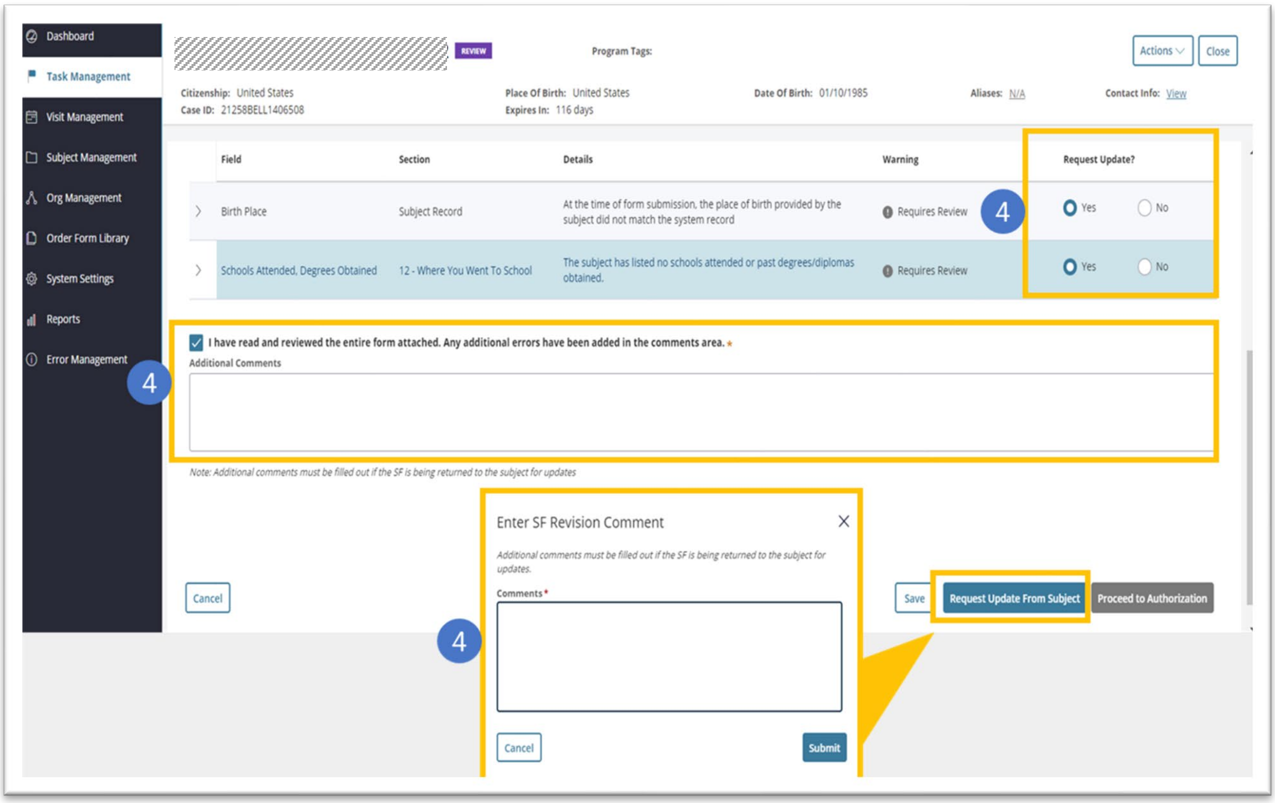
1. From Task Management, select the **My Work** tab. Select the Subject's Task ID hyperlink. The Subject's case request will open the Review tab with any errors a Subject will need to correct.



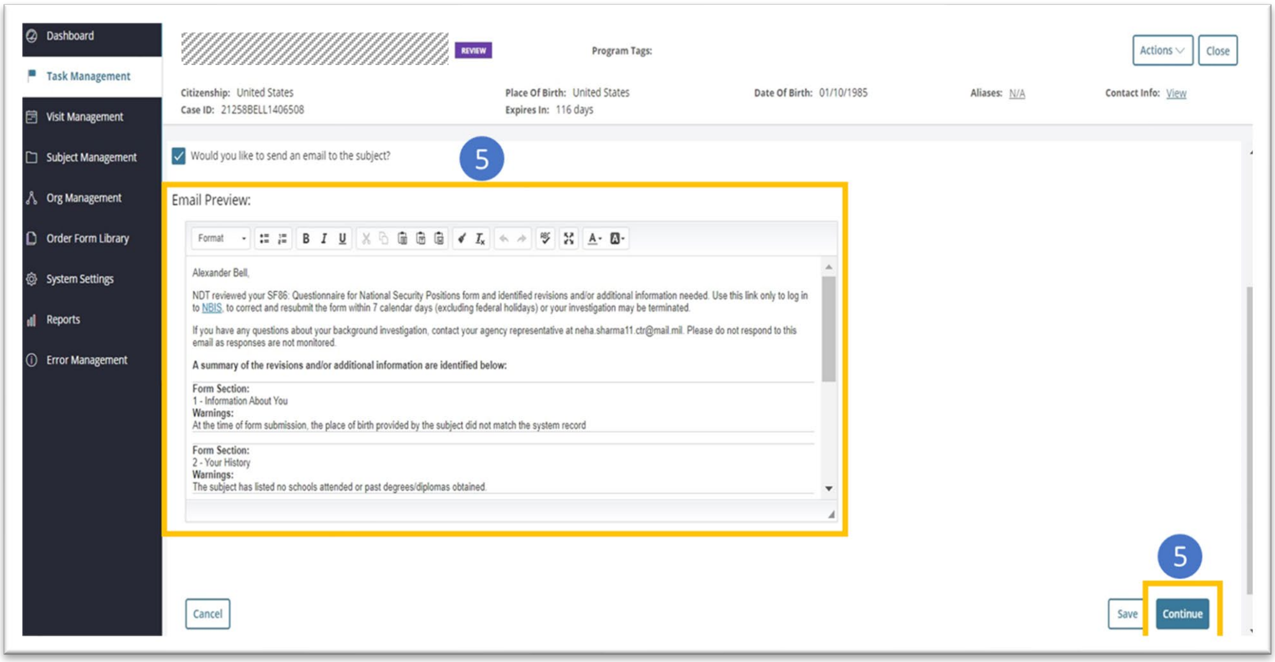
2. The **Review tab** displays errors identified in the subject's eAPP submission that require review and potential correction. The Reviewer is responsible for choosing Yes/No under the Request Update column for each warning.
3. Select the **arrow** at the left of each row to expand it and display warning details. Details include information such as the section pending on review, discrepant values received, and previous logged comments, if any. Post comments under the Reviewer Comments free-text field.



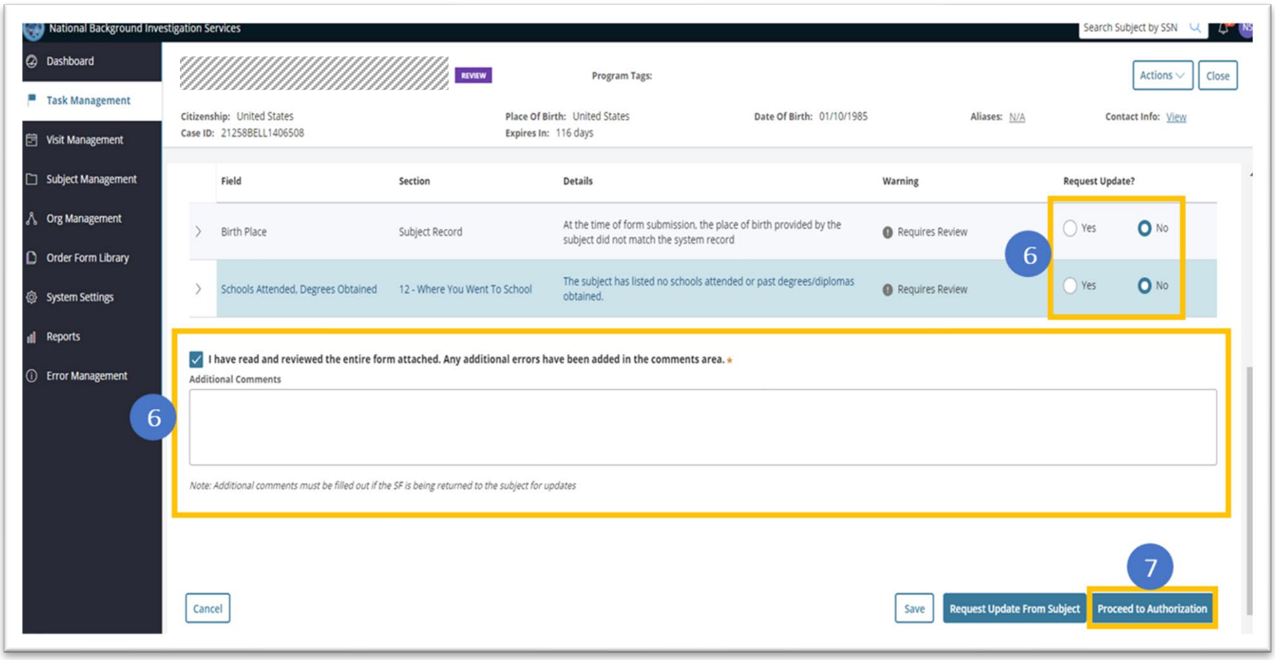
4. To request updates from the Subject, select the "**Yes**" radio button option, select the check box next to "I have read…," provide any additional comments, and select **Request Update from Subject**.



5. An email will be generated/sent to the Subject, instructing the Subject to log back into eAPP to provide revisions and/or additional information that is provided in the email. Before sending an email to the Subject, there will be an option to review the email via Email Preview. Select "**Continue**."



6. For non-critical errors, the Reviewer can choose to accept and error by selecting the "**No**" radio button in the "**Request Update**" column and entering any appropriate comments in the Reviewer Comments free-text field.
7. After all warnings have been cleared, select the check box next to "**I have read**…," provide any additional comments, and click **Proceed to Authorization**. This will move the case forward and begin the authorization process.

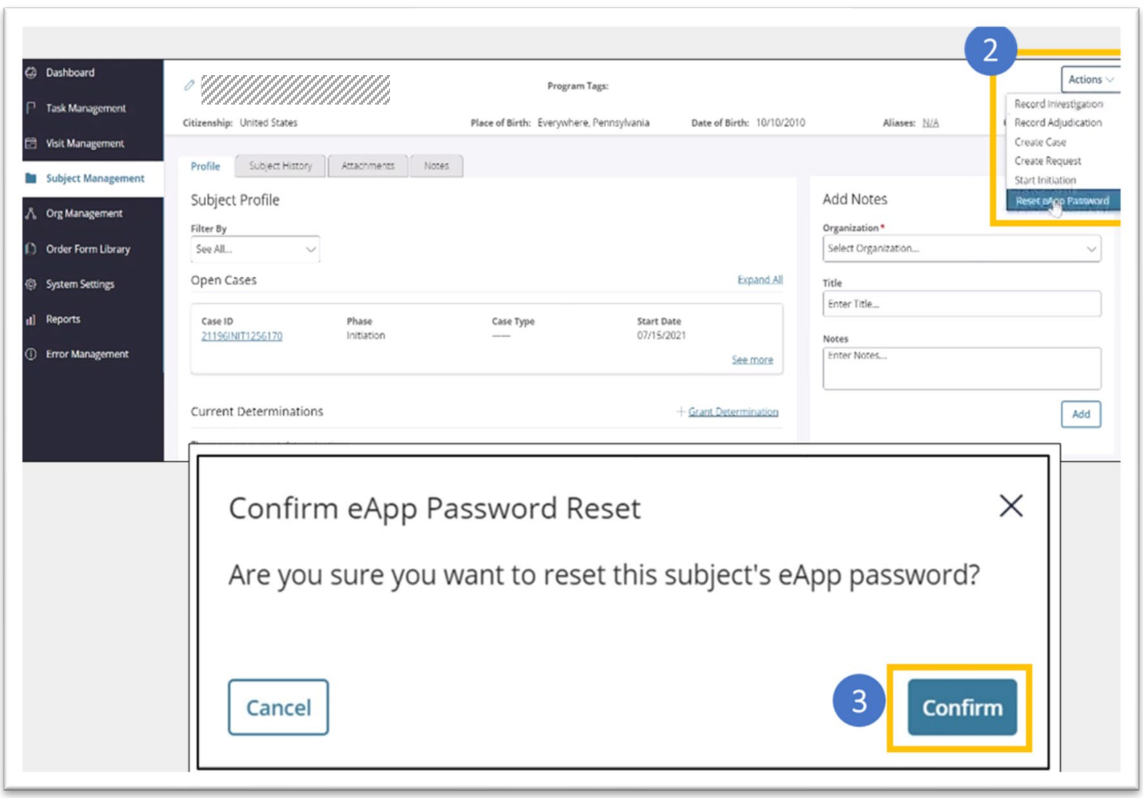

National Background Investigation Services
Search Subject by SSN
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
REVIEW
Program Tags:
Actions
Close
Citizenship: United States
Case ID: 21258BELL1406508
Place Of Birth: United States
Expires In: 116 days
Date Of Birth: 01/10/1985
Aliases: N/A
Contact Info: View
Field
Section
Details
Warning
Request Update?
Birth Place
Subject Record
At the time of form submission, the place of birth provided by the subject did not match the system record
Requires Review
Yes
No
Schools Attended, Degrees Obtained
12 - Where You Went To School
The subject has listed no schools attended or past degrees/diplomas obtained.
Requires Review
Yes
No
6
I have read and reviewed the entire form attached. Any additional errors have been added in the comments area. *
Additional Comments
6
Note: Additional comments must be filled out if the SF is being returned to the subject for updates
7
Cancel
Save
Request Update From Subject
Proceed to Authorization

HOW TO RESET A SUBJECT'S eAPP PASSWORD

Users with the Authorizer, Reviewer and Subject Profile Editor roles can reset the password of a Subject with the same Org affiliation using the Subject's profile. Only users with the Subject Profile Editor role can reset a Subject's password regardless of their Org affiliation. Note that the "Reset eAPP Password" option is only visible after a case request is initiated/opened.

Below is the 3-step process to reset a Subject's eAPP password.

1. From the Subject Management tab, search for the Subject's SSN and open the **Subject's Worksheet.**
2. From the "**Actions**" drop-down in the upper right-hand corner, select the "**Reset eAPP Password**" option. A pop-up message prompts users to "Confirm" resetting the Subject's eAPP password.
3. After confirming, a second pop-up message will appear confirming that the password has been successfully reset. An email is immediately sent to the Subject's email on file with instructions on how to reset their password.

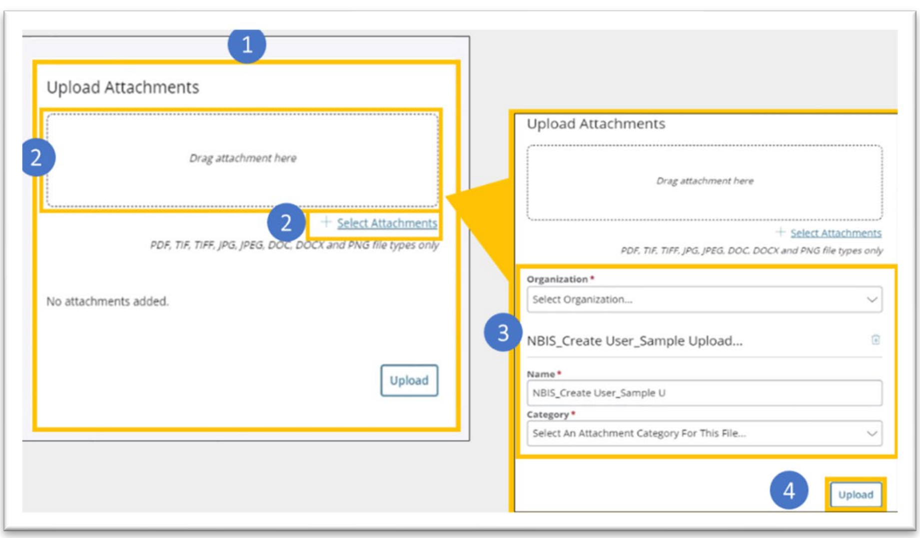


HOW TO ADD ATTACHMENTS TO A SUBJECT'S PROFILE

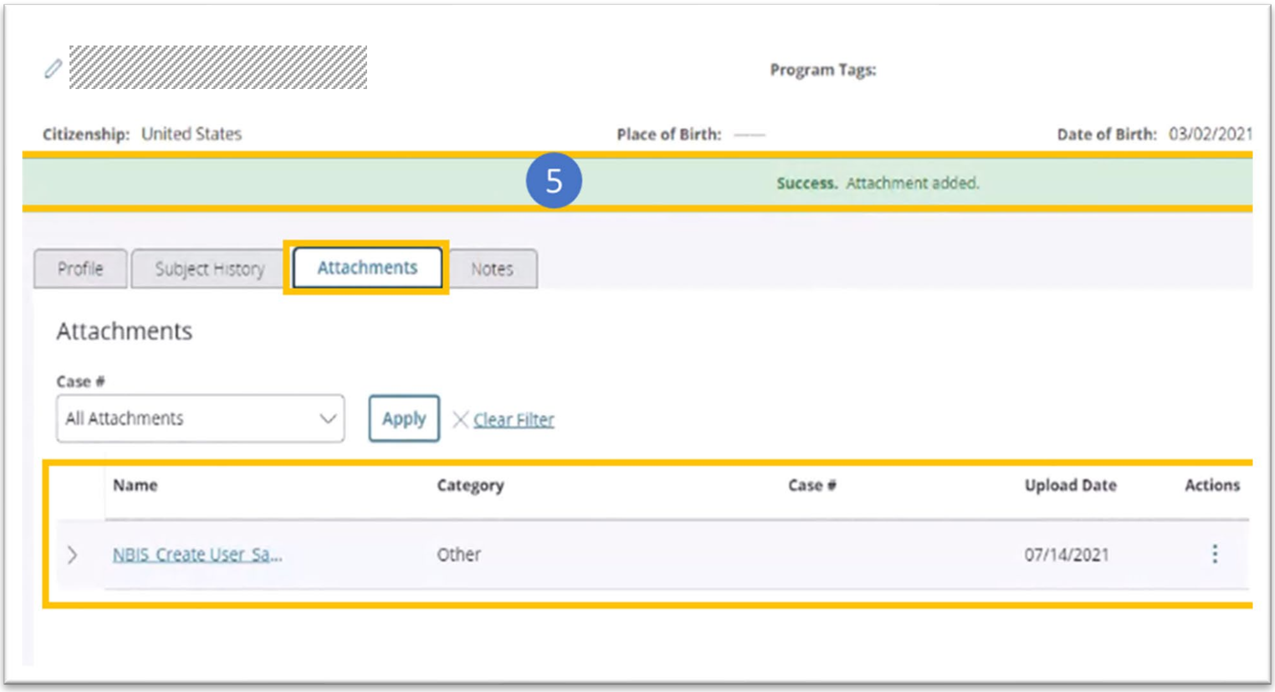
Users with the Subject Manager, Authorizer, Reviewer, Initiator, Mass Initiator, Screener, Subject Profile Editor, Subject Viewer and Facility Security Officer (FSO) roles can access the Attachments section in a Subject's case. Users can add, manage, and upload attachments associated with the Subject's profile. New attachments will appear near the top of the Attachments tab list in the Subject's Worksheet.

1. From the Subject Management tab, search for the Subject's SSN and open the Subject's Worksheet. Locate the "**Upload Attachments**" box on the right-hand side of the screen.
2. Drag an attachment into the "Drag Attachment Here" box or select the "Select Attachments" hyperlink below the "Upload Attachments" box.
3. Browse for and add the attachment. Enter the Organization, document name, and category for the document.
4. Select **Upload**.
5. A green success banner will appear when the attachment has been uploaded. To view the new attachment, navigate to the Attachment tab in the Subject Worksheet. Select the "**Attachment Name**" hyperlink. Note: If the attachment does not immediately appear in the list, select "Clear Filter."

Steps 1-4



Step 5


Program Tags:
Citizenship: United States
Place of Birth: —
Date of Birth: 03/02/2021
5
Success. Attachment added.
Profile
Subject History
Attachments
Notes
Attachments
Case #
All Attachments
Apply
Clear Filter
Name
Category
Case #
Upload Date
Actions
NBIS Create User Sa...
Other
07/14/2021

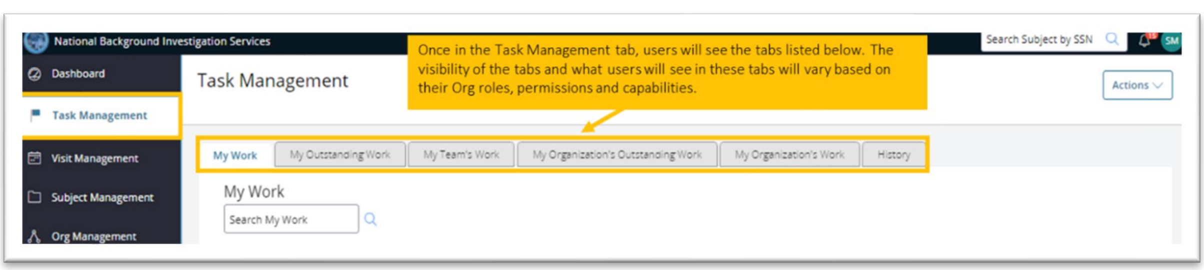
TASK MANAGEMENT

UNDERSTANDING TASK MANAGEMENT TABS

After initial login, users with specific manager roles can access Task Management from the navigation menu on the left. Task Management is where case operators (Reviewers, Authorizers, and Case Processors) can view the work assigned to them and review the cases they have worked on previously. It is also where managers can view the work assigned to their orgs or teams. There are multiple tabs within Task Management that allow users with Team Manager or Org Workload Manager roles to view and manage work assigned to their persona, their team, or their organization.

Visibility of the following tabs will vary based on assigned roles and permissions associated with those roles.

- My Work: Reveals a list of all tasks currently assigned to users.
- My Outstanding Work: Shows a list of cases assigned to users that are waiting for actions to be completed by other team members or processes. This only applies to case owners for adjudication and appeals cases.
- My Team's Work: This tab is only visible to Team Managers and only applies to adjudication/appeals cases and is only visible to users with the Team Manager role. Cases will only appear if users are assigned to a team. This tab will display a list of tasks assigned to user's team well as sub-team's work.
- My Organization's Outstanding Work: This tab is only visible to users with the Org Workload Manager role. This tab will display a list of adjudication cases pending subtask completion. There will be a drop-down to select the org users want to display.
- My Organization's Work: This tab is only visible to users with the Org Workload Manager role. This tab will display a list of all cases or items in the org currently (assigned or unassigned) as well as cases within the org hierarchy. There will be a drop-down to select the org users want to display.
- History: This tab will display a list view of cases users have worked on.



HOW TO CONFIGURE TASK MANAGEMENT DISPLAY

Task Management tabs shows the work by displaying data elements that the user desires to see in a configurable column format. Users can create multiple views of their work to account for various task scenarios. Users that have roles to look across subordinate teams and users that have access to the entire organization's inventory can also create and configure multiple views of their work.

CUSTOMIZE TABLE LAYOUT

1. To customize the columns visible, select **Table Settings** and then select "**fields**" to view a list of all the columns available for the table. You can check or uncheck to change the columns that are visible.
2. To rearrange columns, **c**lick anywhere inside the column header and drag to reposition the columns in a different order.
3. To save the Customized Table View, select Table View and then **Save Table** to save the columns that you configured for the table. You can also select Delete Saved Table to revert to the default view and remove your configurations.

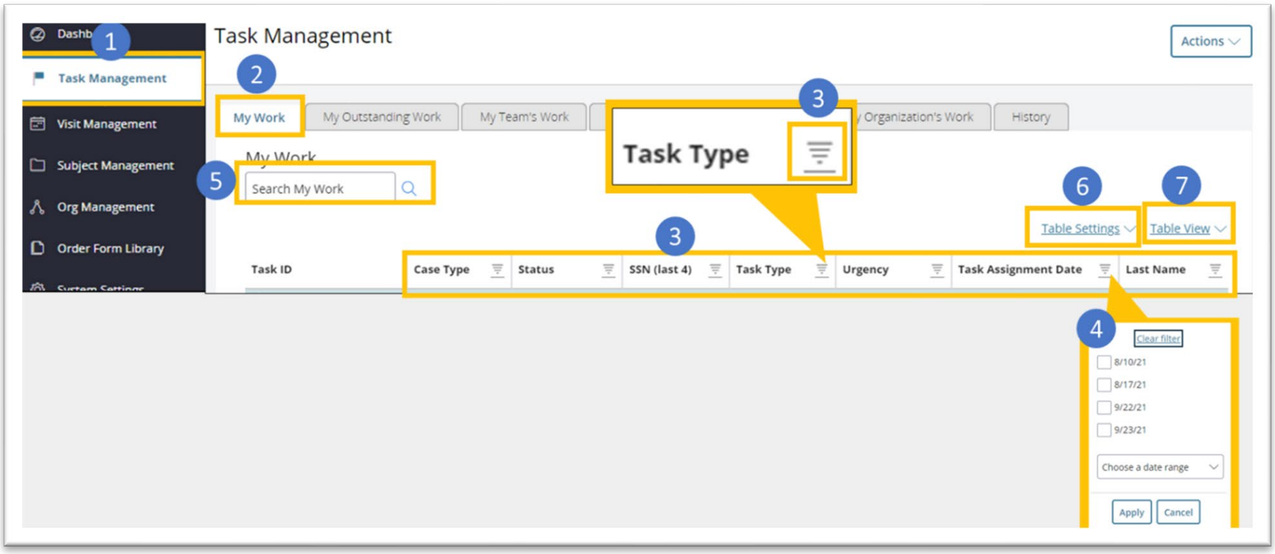
SORT AND FILTER COLUMNS

There are multiple tabs within Task Management that allow users with Team Manager or Org Workload Manager roles to view work assigned to their persona, their team, or their organization. Visibility of the tabs will vary based on assigned roles and permissions associated with those roles. Filtering and sorting through tasks can be applied on any column to allow for dynamic views of the work. Users can use filters such as Task ID, Case Type, Status, Task Age, Task Assignment Date and Last Name to sort and filter through multiple tasks.

Below is the 6-step process for how to Sort and Filter Columns Within Task Management.

1. From initial log in, select **Task Management** from the navigation menu on the left.
2. Users can **select the tab** they would like to access, such as "My Work" or "My Organization's Work."
3. Users can sort and filter by column. To filter specific data, select the **triangle icon** located to the right of the designated column.
4. After selecting the triangle filter icon, select the specific filter criteria in the pop-up window. Place a checkmark in one or more of the small boxes next to the applicable criteria to filter for. Once search criteria has been identified, select "**Apply**."
5. Alternatively, users can manually type into the "**Search My Work**" field to search, sort, and filter for specific data.
6. To change the search fields to filter and sort, select the **Table Settings hyperlink**. From the Field Visibility pop-up, place a checkmark in each box to populate the table. Or remove the checkmark from the box to leave out the search field.

7. To save the new current search view and table settings of results, select the **Table View hyperlink**. Select "Save View."

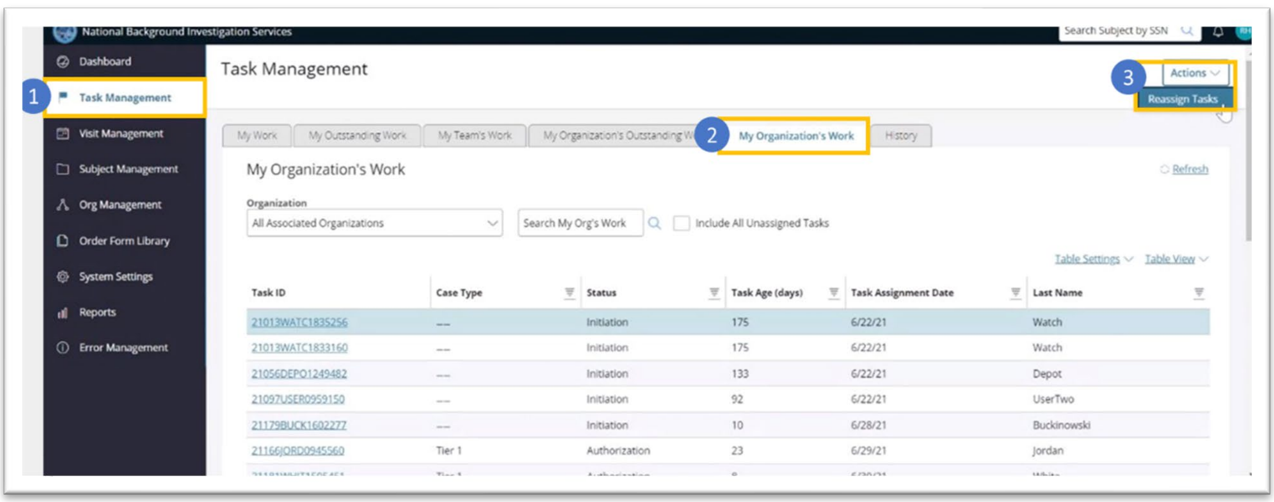


HOW TO REASSIGN TASKS

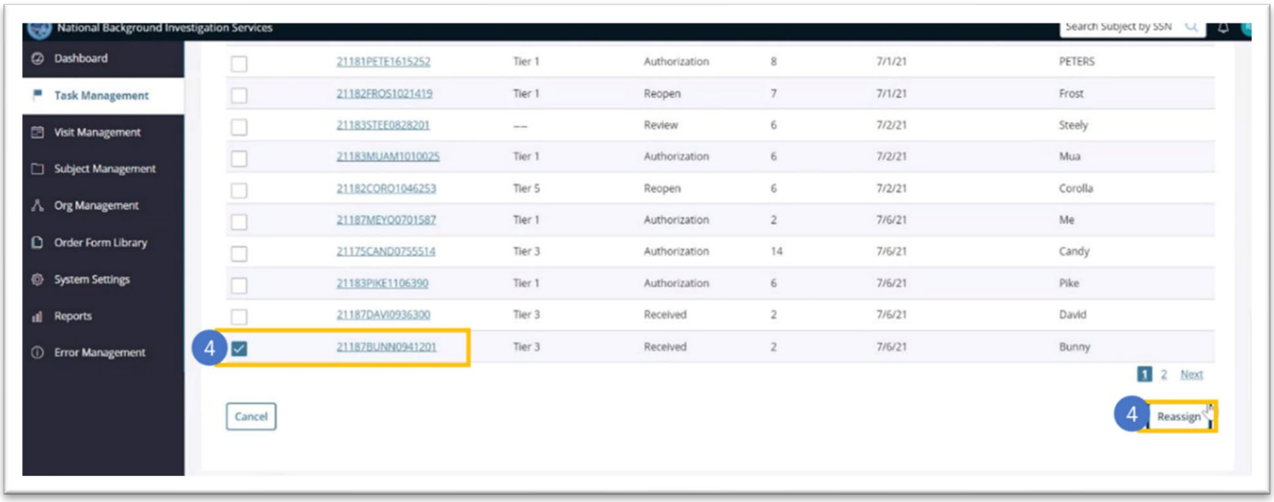
As the Team Manager or Org Workload Manager, you have the ability to bulk reassign tasks or cases. The reassignment options will be based on the organization and team affiliations.

Below is the 6-step process for how to Reassign Tasks.

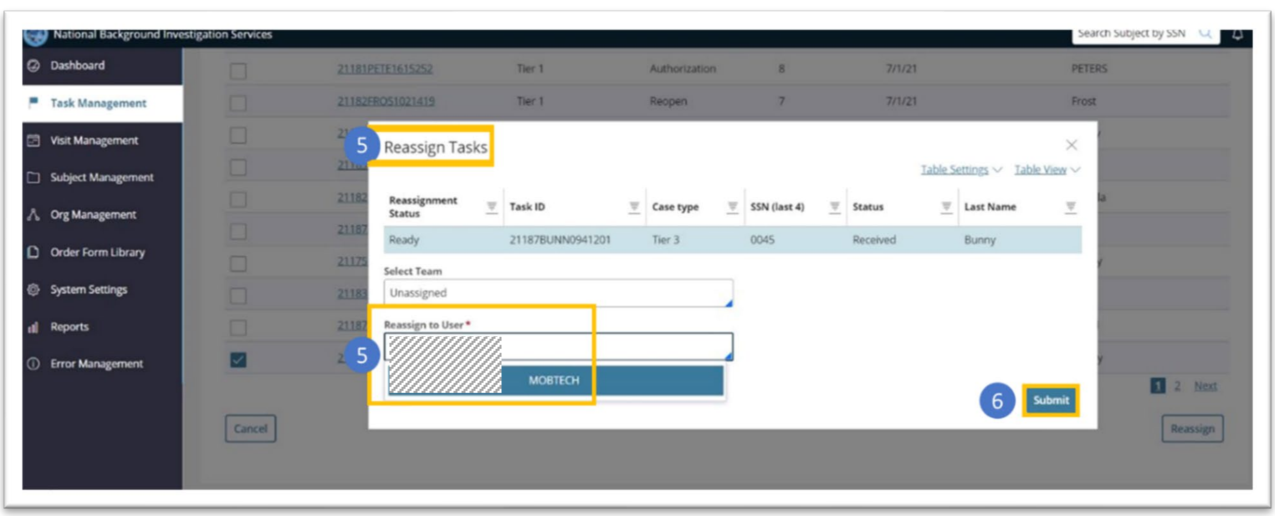
1. From initial log in, select **Task Management** from the navigation menu on the left.
2. Select **My Organization's Work**.
3. Click the **Actions** button to reveal the drop-down menu then click **Reassign Tasks**.



4. On the row of the task that users would like to Reassign, click the box in the "**Selected Items**" column to insert a checkmark. Once users have selected all the tasks that they would like to reassign, users can click the Reassign button in the bottom right corner of the screen to reassign those tasks.



5. Users will be prompted with the "Reassign Tasks" screen. Select a team if applicable. Begin typing into the **Reassign to User field** to search for the users that the task(s) will be reassigned to. Note: The Select Team field only applies to adjudication and appeals cases. When applicable, your team will be pre-populated in the Team Name field in read-only mode when reassigning from My Teams Work. Users in your team will be populated in the User drop-down.
6. After selecting the appropriate users, click **Submit**. Users will be prompted with a message that confirms that users were successfully reassigned the task to a new user. Once you close the modal, the case list will repopulate reflecting the reassignment.



USER MANAGEMENT

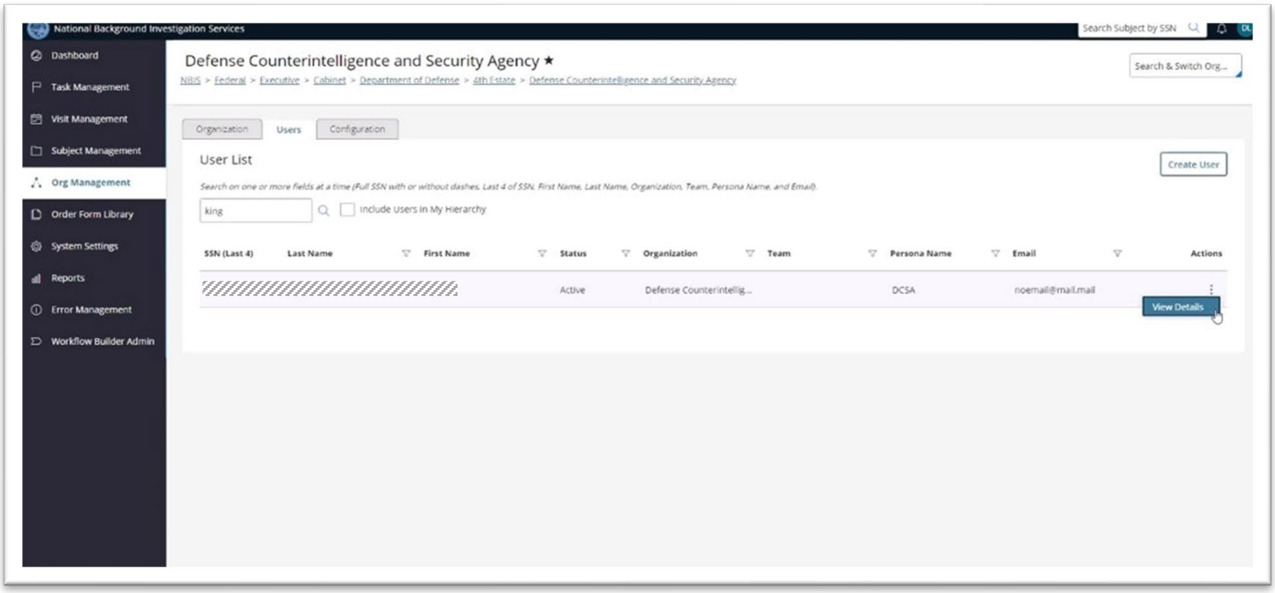
HOW TO RESET A USER

Users with the User Manager role can reset the authentication of a user within an organization's hierarchy. A user may experience difficulties logging into NBIS and may need to have their authentication reset in order to log back into the system. Once the below steps are completed, users will receive two separate emails containing a Persona ID and Enrollment Key to log back in. If the emails are sent to the users successfully, there will be a message indicating so. Otherwise, a failure message will appear.

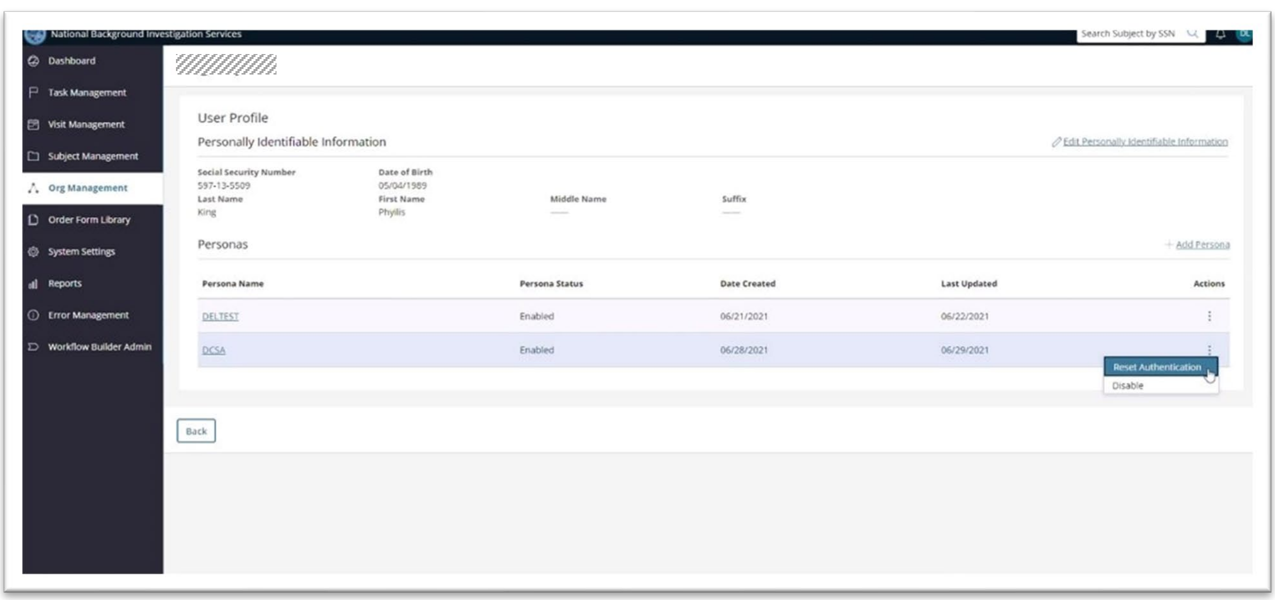
Below is the 5-step process to reset a user.

1. Navigate to **Organization Management** on the left-hand side and locate your organization (if needed).
2. Select the **Users tab** to view a list of users within the selected Organization.
3. From the Actions column, select the ellipses icon next to the user row you wish to reset authentication. Select **View Details**.
4. Select **Reset Authentication**.
5. Select **Confirm** to reset the user's authentication.

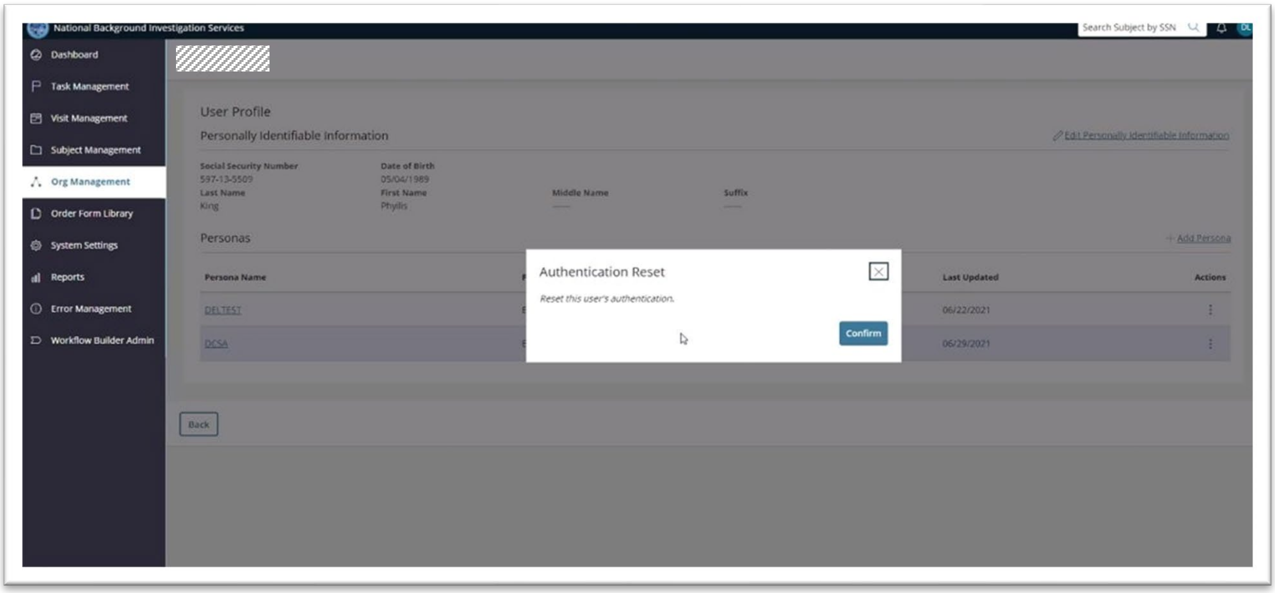
Steps 1, 2, and 3


National Background Investigation Services
Search Subject by SSN
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Workflow Builder Admin
Defense Counterintelligence and Security Agency ★
NBIS > Federal > Executive > Cabinet > Department of Defense > 4th Estate > Defense Counterintelligence and Security Agency
Search & Switch Org...
Organization
Users
Configuration
User List
Create User
Search on one or more fields at a time (Full SSN with or without dashes, Last 4 of SSN, First Name, Last Name, Organization, Team, Persona Name, and Email)
king
Include Users in My Hierarchy
SSN (Last 4)
Last Name
First Name
Status
Organization
Team
Persona Name
Email
Actions
Active
Defense Counterintellig...
DCSA
noemail@mail.mail
View Details

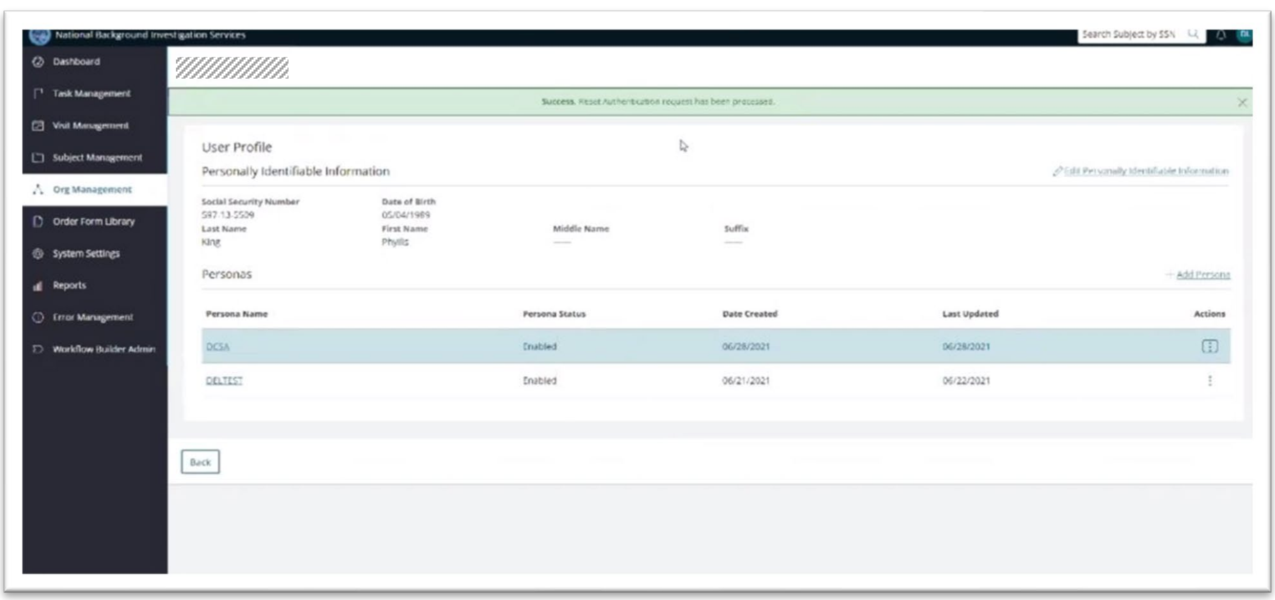
Step 4


National Background Investigation Services
Search Subject by SSN
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Workflow Builder Admin
User Profile
Personally Identifiable Information
Edit Personally Identifiable Information
Social Security Number
597-13-5509
Date of Birth
05/04/1989
Last Name
King
First Name
Phyllis
Middle Name
Suffix
Personas
Add Persona
Persona Name
Persona Status
Date Created
Last Updated
Actions
DELTEST
Enabled
06/21/2021
06/22/2021
DCSA
Enabled
06/28/2021
06/29/2021
Reset Authentication
Disable
Back

Step 5



Step 5 Continued



HOW TO EDIT PERSONAL USER INFORMATION

Users with the User Manager role can edit a user's Personally Identifiable Information (PII) information and User Persona information as needed.

EDIT USER PII

Users with the User Manager role can edit a user's Personally Identifiable Information (PII) information as needed. Below is the 6-step process for editing a user's PII. Please reference the latest NBIS Service Provider Guide or Job Aid for detailed instructions on this process.

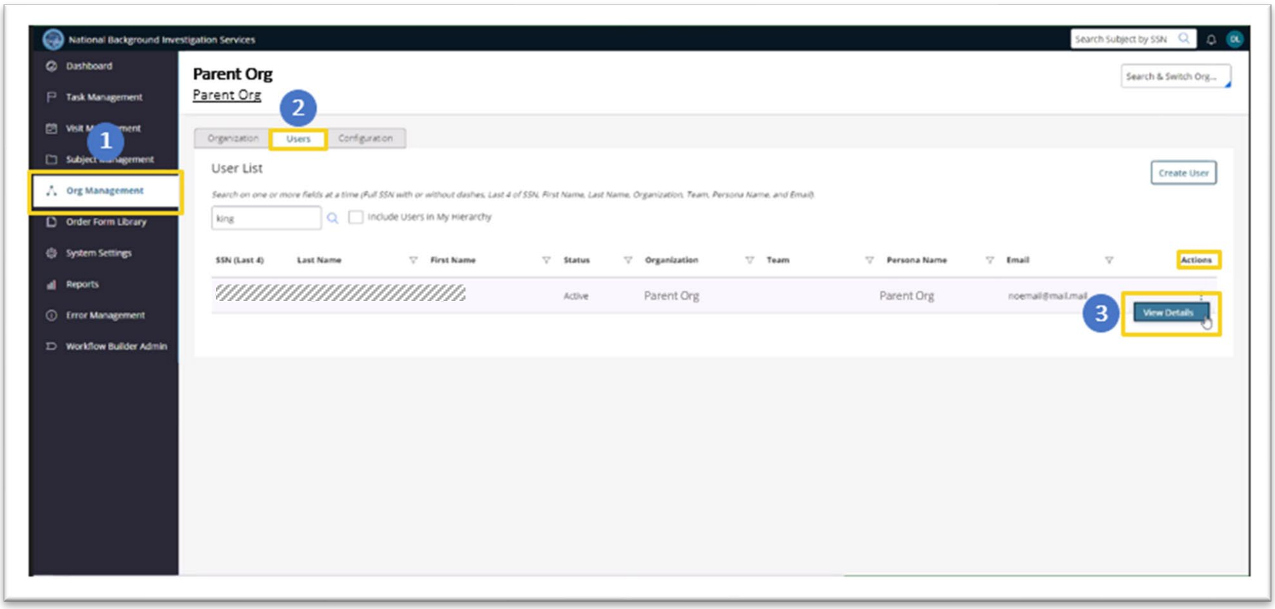
1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the **Users** tab to see the list of users in the Org a user is viewing.
3. To open a User Profile, select the **vertical ellipses** under the Action column next to the desired user. Select **View Details** to open User's Profile.
4. Select the hyperlink **Edit Personally Identifiable Information** in the top right-hand corner.
5. Make the changes and select **Save**.

EDIT USER PERSONA INFORMATION

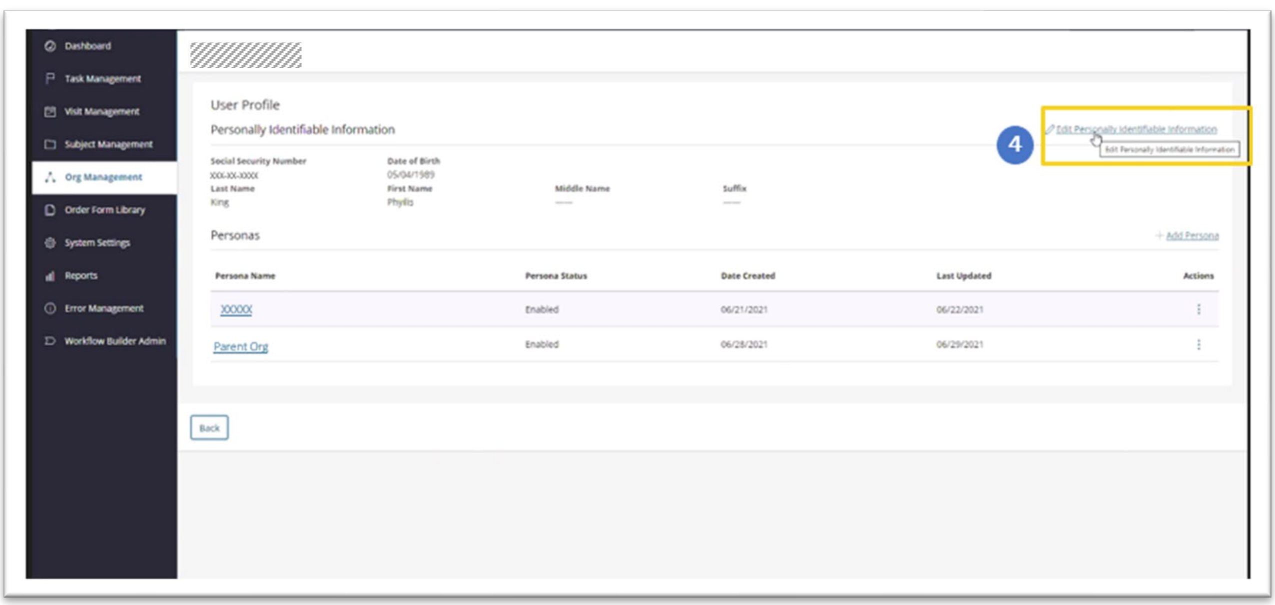
Users with the User Manager role can also edit a user's personal information as needed. It is important to note that if a persona is disabled, users will not be able to edit any information. Below is the 6-step process for editing a user's Persona information. Please reference the latest NBIS Service Provider Guide or Job Aid for detailed instructions on this process.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the **Users** tab to view the list of users.
3. From the Actions column, select the ellipses next to the user row and then select **View Details** to view the user's profile.
4. In the **User Profile**, select a hyperlinked Persona Name to edit.
5. From the bottom right of the Persona Settings screen, select **Edit** to edit the persona details. This includes editing the primary phone number, email, notification preferences, time zone, attachments, disable the Org, edit/delete the Org associations/roles, add additional Orgs and editing User Assignments.
6. Select **Save** to save the changes.

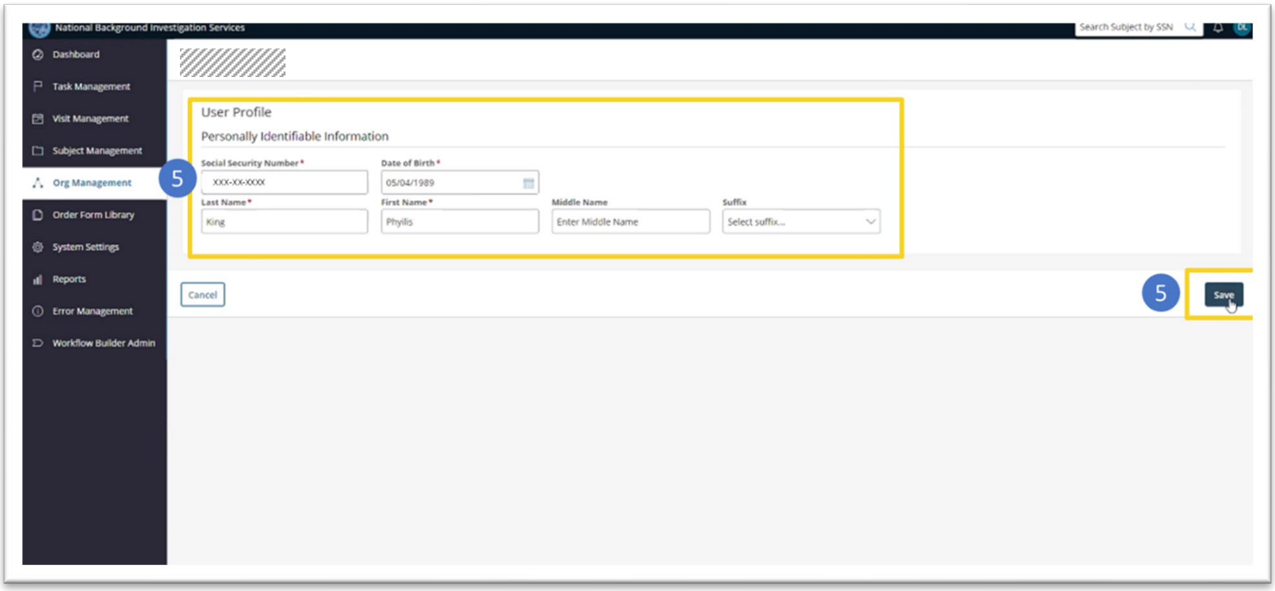
Edit User PII (Steps 1-3)



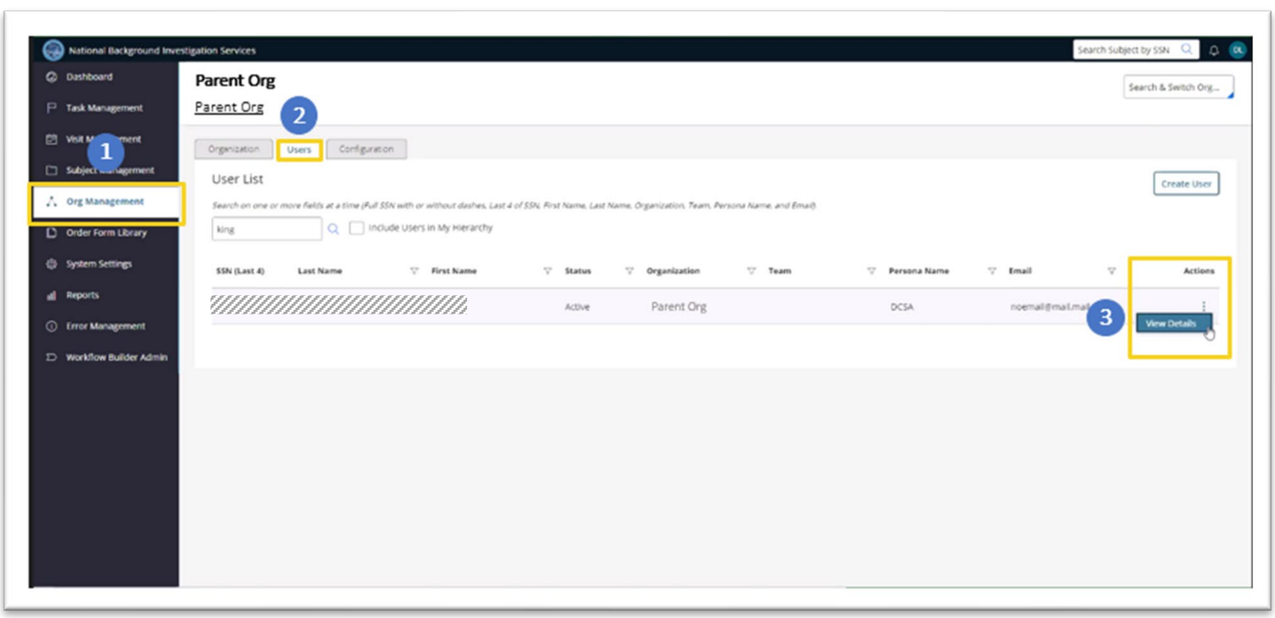
Edit User PII (Step 4)



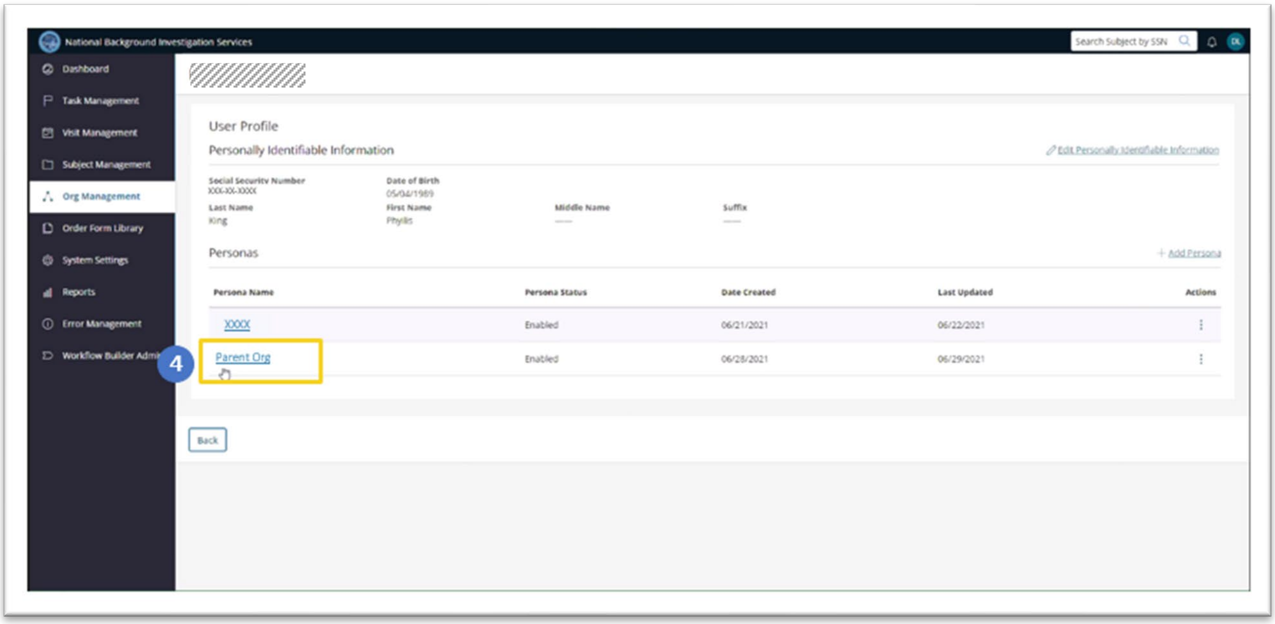
Edit User PII (Step 5)



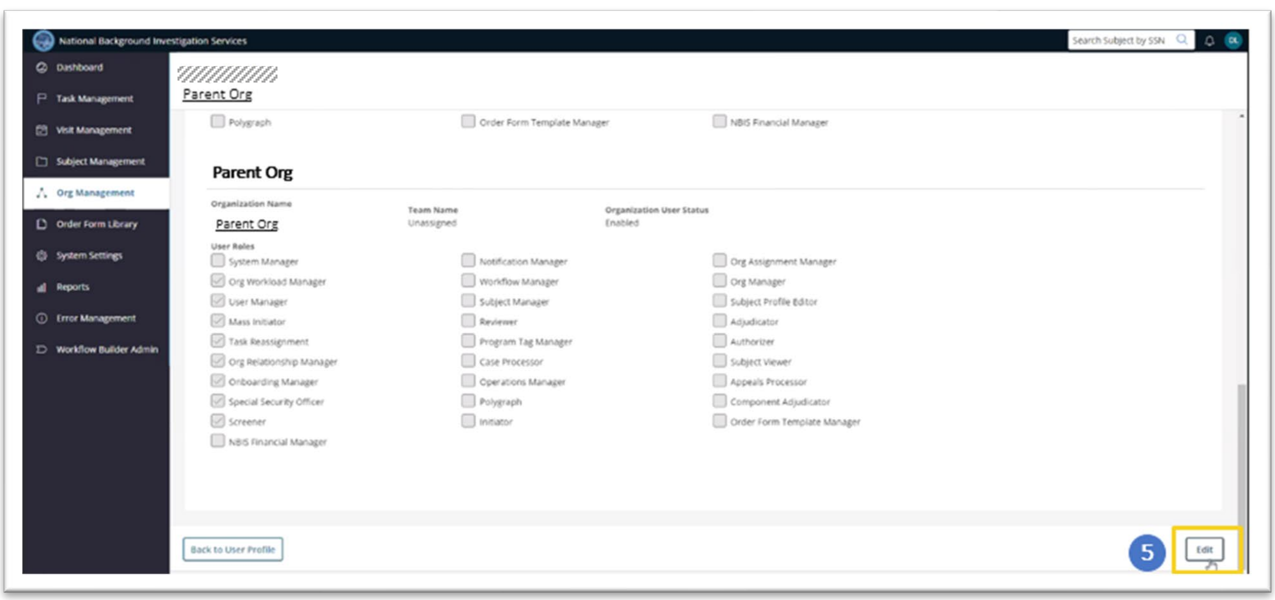
Edit User Persona Information (Steps 1-3)



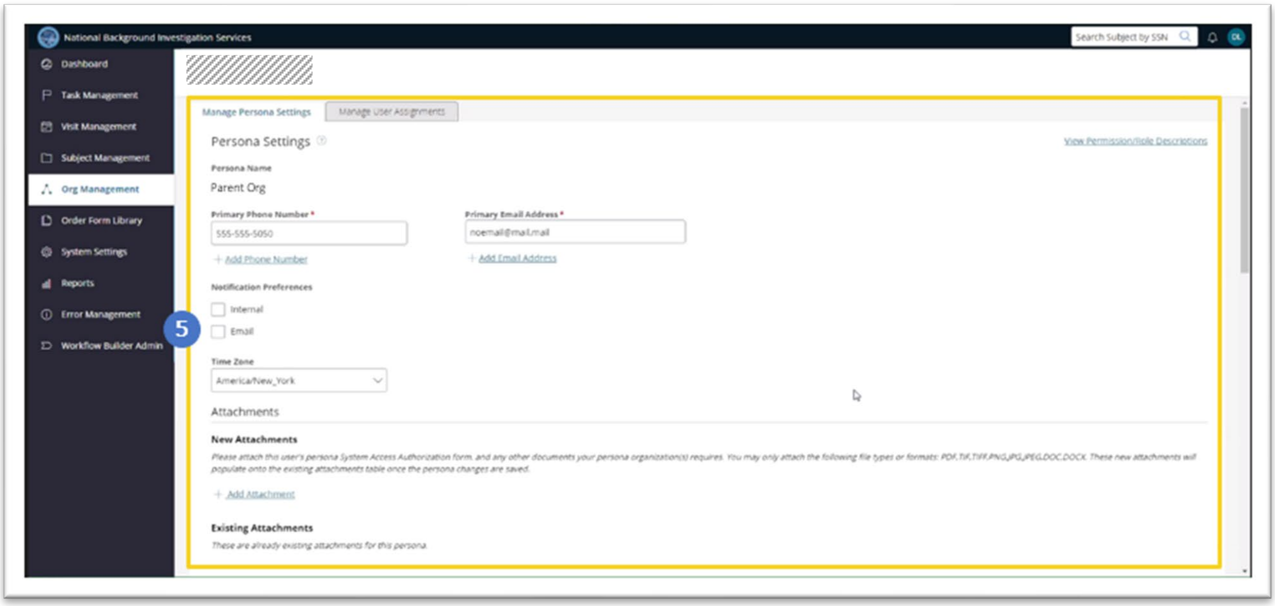
Edit User Persona Information (Step 4)



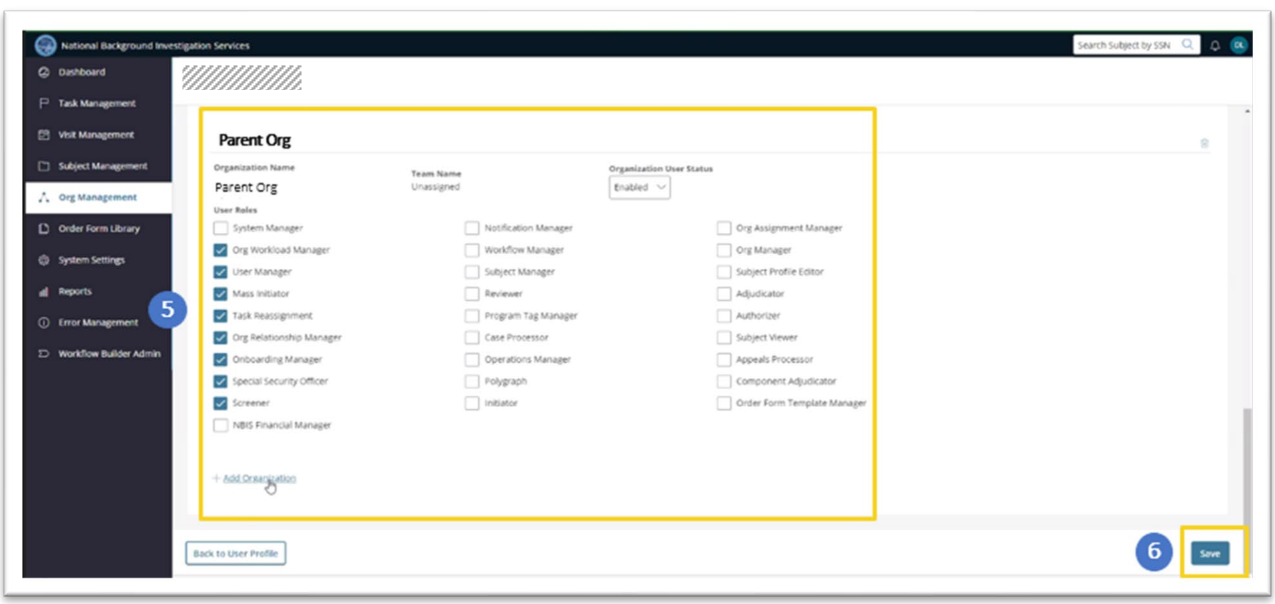
Edit User Persona Information (Step 5)



Edit User Persona Information (Step 5 Continued)



Edit User Persona Information (Steps 5-6)



HOW TO DISABLE OR ENABLE USER PERSONAS

DISABLE A PERSONA

Users with the User Manager role can disable user's persona. There are multiple reasons why one would want to disable a user's persona. For example, a user was retired, fired, moved to a new job, or otherwise no longer needs NBIS access for their role in the organization. If a persona is disabled, all cases in that user's worklist for their organization will return to their respective Organization's workbasket. Below is the 5-step process for disabling a Persona.

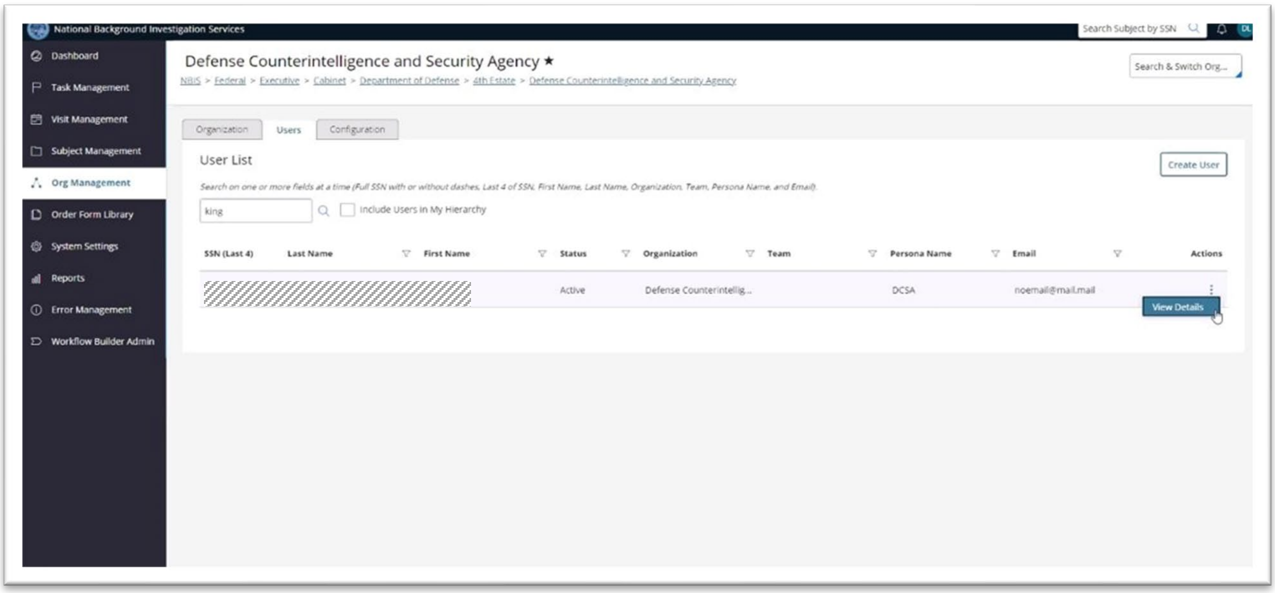
1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the **Users** tab to view the list of users.
3. From the Actions column, select the ellipses next to the hyperlinked persona name to disable and then select **View Details**.
4. Select Disable to disable the persona and choose a reason for disabling. There's an option to provide an Explanation (ex. Moved to a New Job, Retirement, Fired or Other).
5. **Select Continue**. A green success banner will appear at the top of the screen and the Persona Status will appear as Disabled.

ENABLE A PERSONA

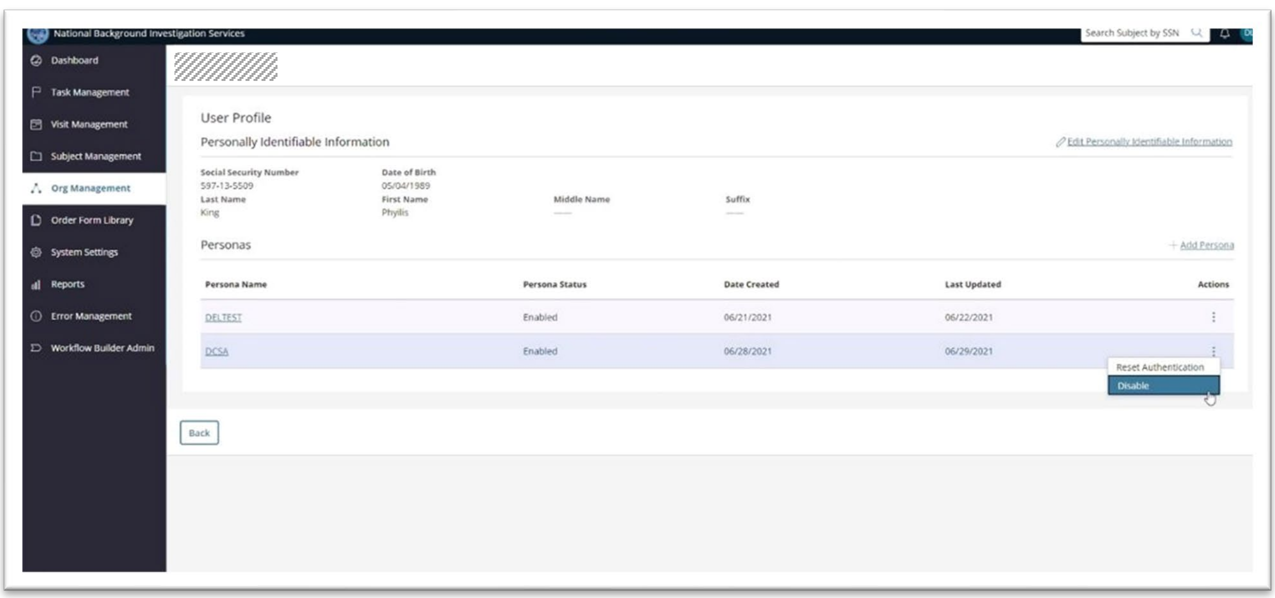
Users with the User Manager role can also enable a user's persona. The Enable option will appear once a persona is disabled if you want to re-enable it. Below is the 5-step process for enabling a persona.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the **Users** tab to view the list of users.
3. From the Actions column, select the ellipses next to the user row and then select **View Details.**
4. To Enable a Persona, choose the **Enable** option from the ellipsis's icon under the Actions column to re-enable. A confirmation screen will appear with an explanation of why the persona was disabled.
5. Select **Continue.** A green success banner will appear at the top of the screen and the Persona Status will go back to Enabled.

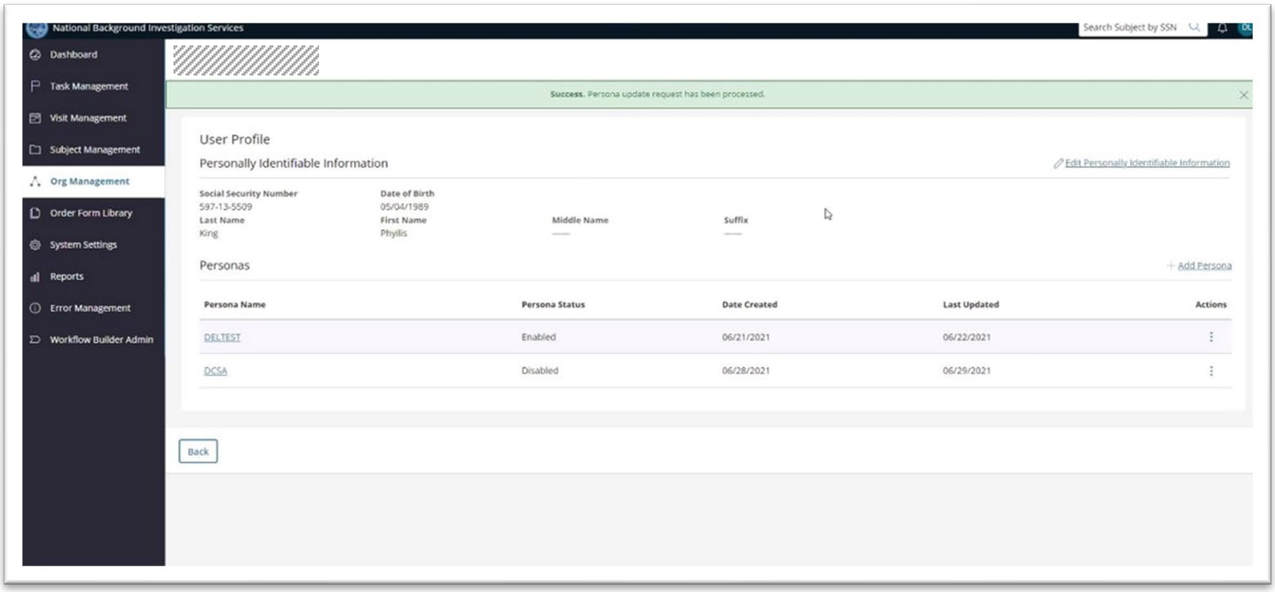
Disable a Persona (Steps 1-3)



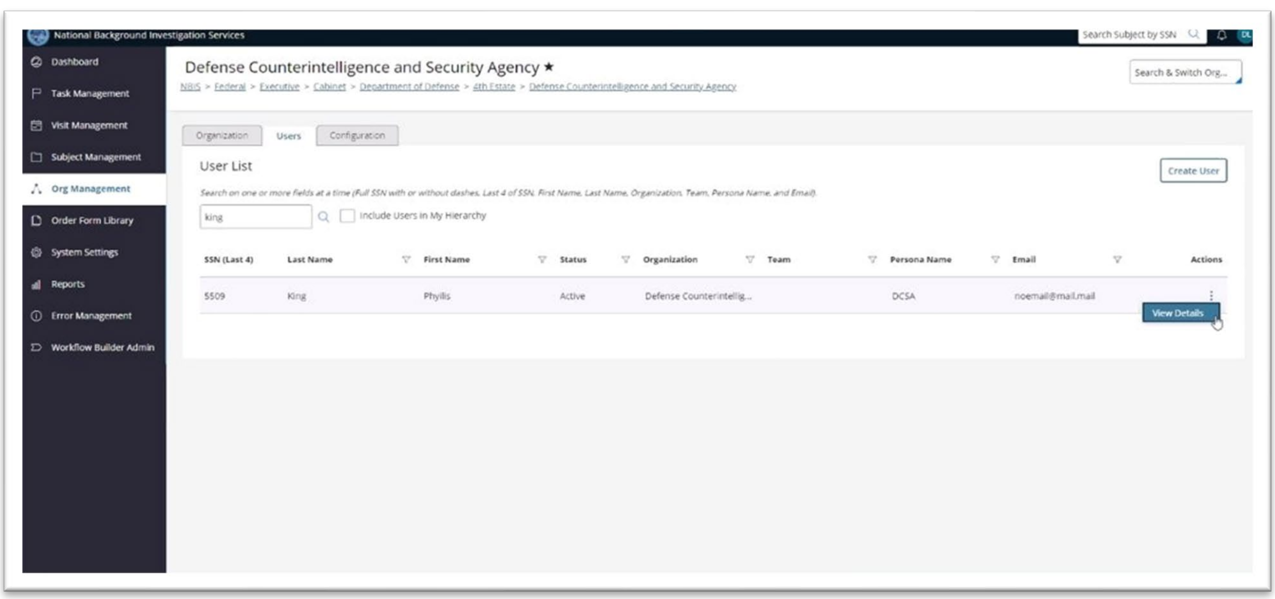
Disable a Persona (Step 4)



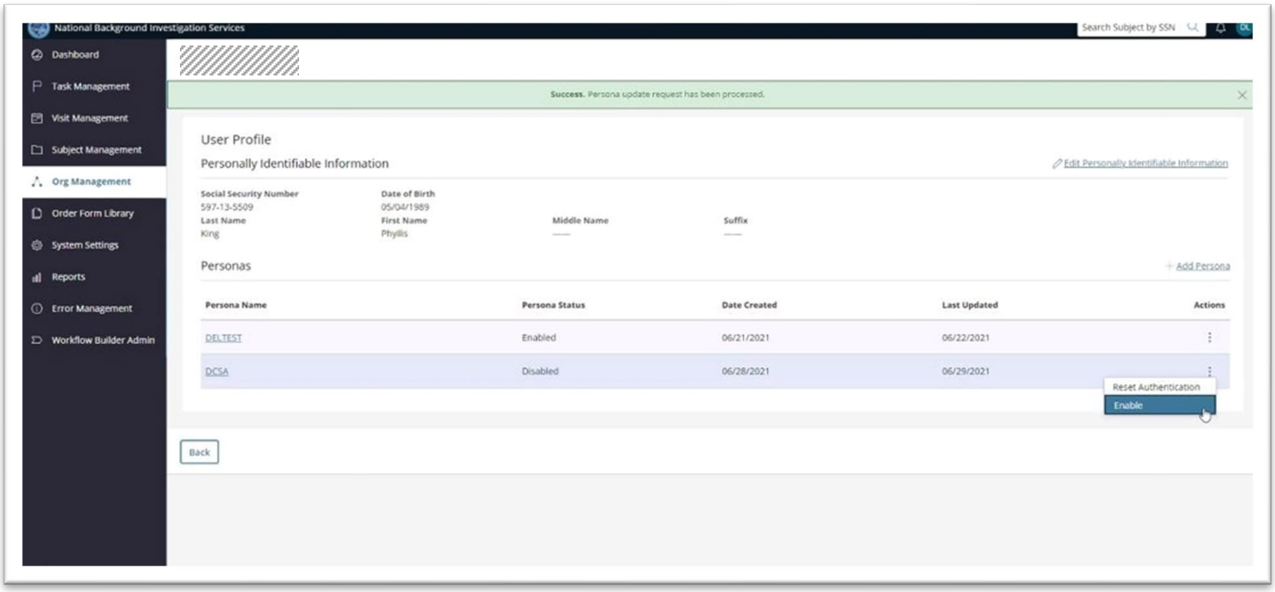
Disable a Persona (Step 5)



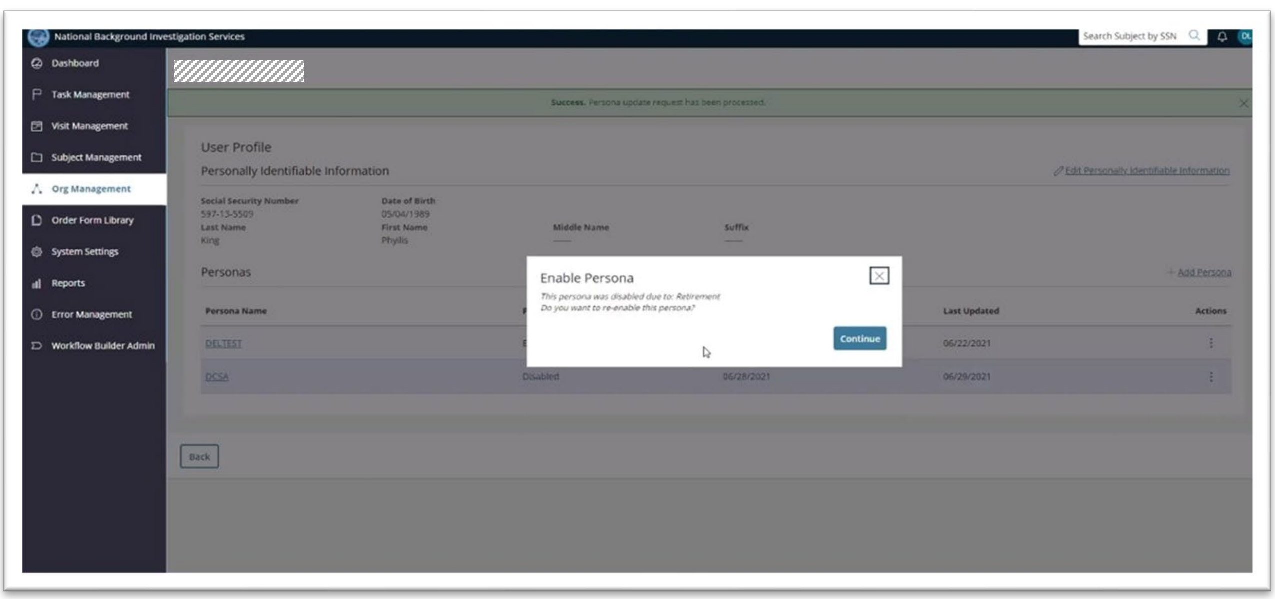
Enable a Persona (Steps 1-3)



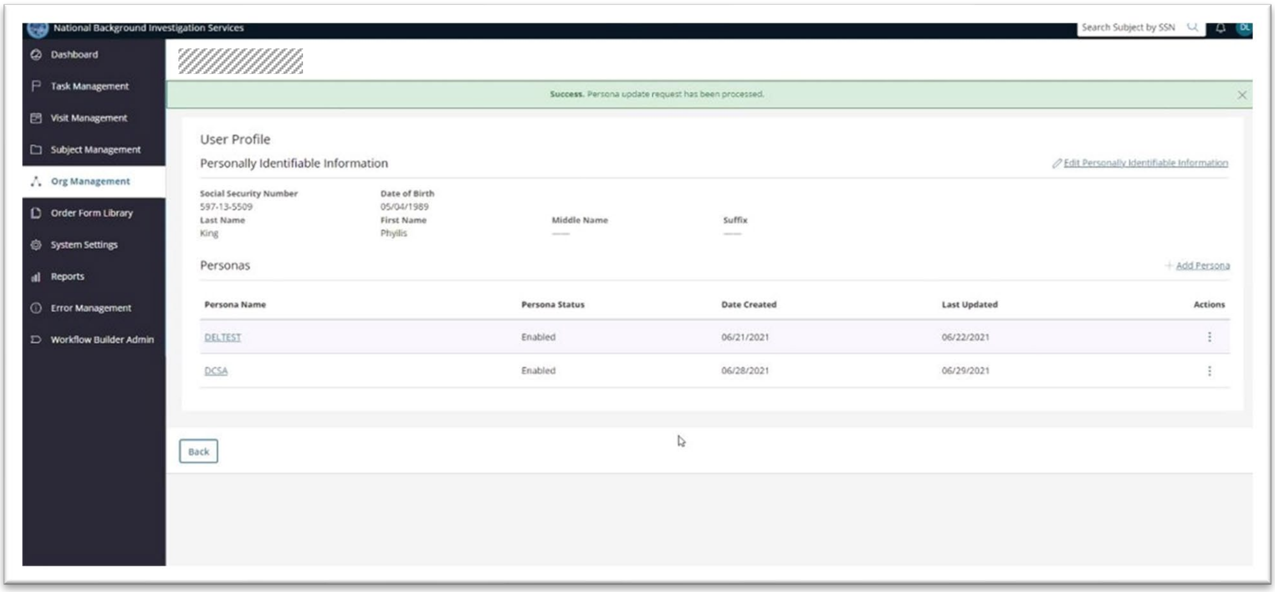
Enable a Persona (Step 4)



Enable a Persona (Step 5)



Enable a Persona (Step 5 Continued)



HOW TO CREATE A USER LEVEL

The User Manager can create User Levels within Org Management that can be applied to users. User levels dictate which workflow actions are available for a given task within your organization. Note that User Levels must be used in conjunction with user assignments or assignment rules. Below is the 5-step process to create a user level.

Below is the 5-step process to create a user level.

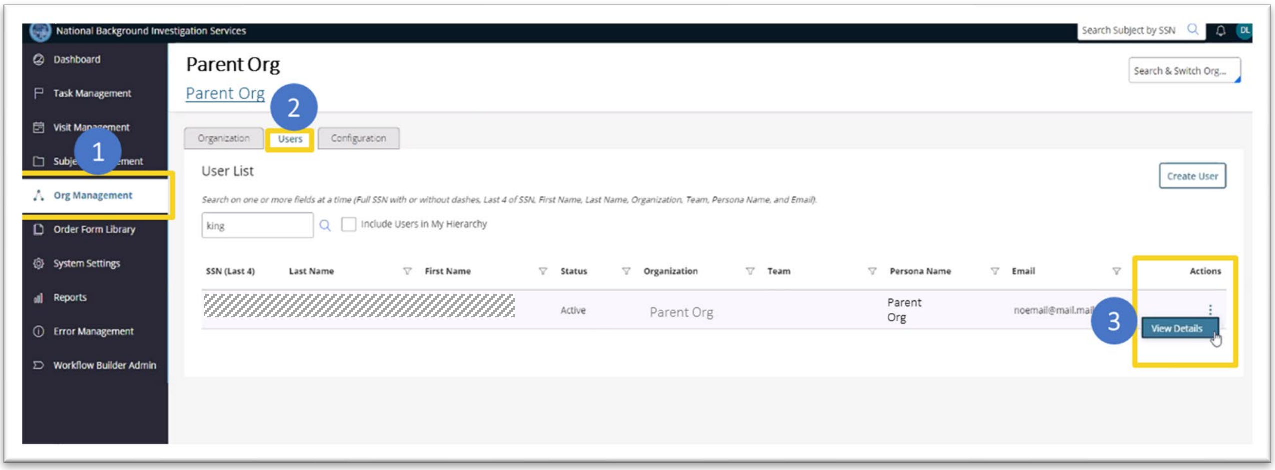
1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **User Levels.**
4. To create a new template, select **Add User Level**.
5. Enter a User Level Name (required) and description (optional). Enter a Display Order number (optional) to sequentially order the users within the table. Click **Save** and **Add**. Note: To disable the User Level, click the hyperlinked User Level Name. From the Actions drop-down menu, select Edit User Level and uncheck the “Enabled” box.

HOW TO ADD AN ORGANIZATION TO AN EXISTING USER PERSONA

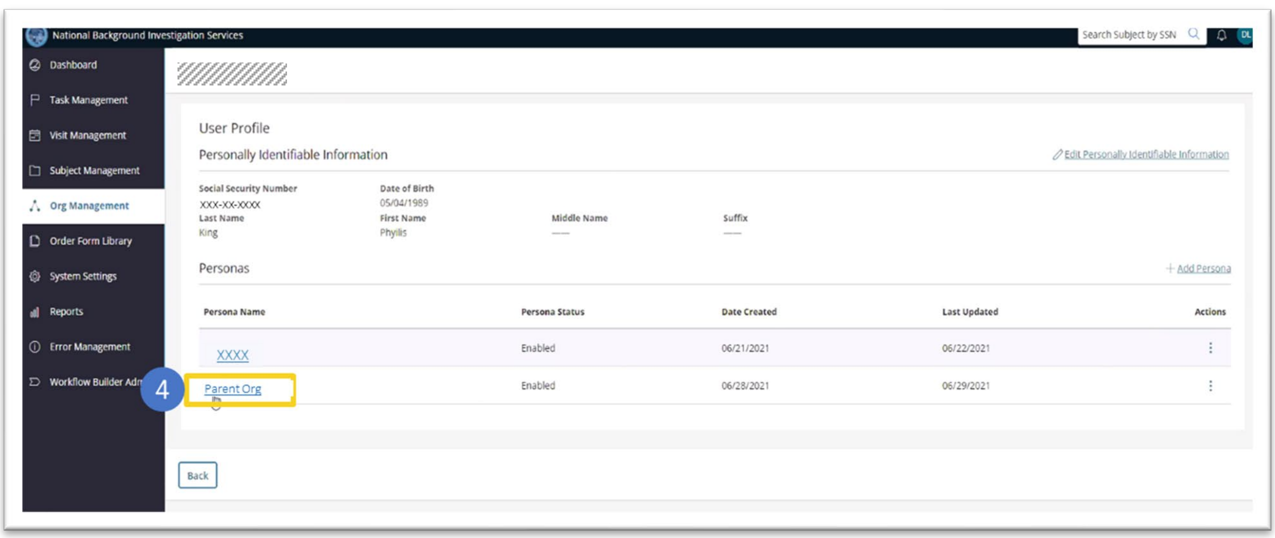
The User tab is accessed from Org Management in the left-hand side of the navigation panel. After the Org has been added, users with the Org Manager role must have someone with the User Manager role add them to the Org as a user—even if they have created/own the Org. Therefore, users with the User Manager role must be an existing user in NBIS with a persona already created. The existing users with the User Manager role must assign the Organization to the user persona. Below is the 9-step process for adding an organization to an existing user's persona after the Organization has been created.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the **Users** tab and navigate to the row showing the desired user.
3. Select the ellipses underneath the Action column and select **View Details**.
4. Select the desired **hyperlinked Persona Name** and ensure users are in the Manage Persona Settings tab.
5. Scroll down to the bottom of the page and select **Edit** on the bottom right-hand side.
6. To add the user to an additional Organization, scroll down and select the hyperlink **+Add Organization** in the bottom-left side underneath the User Roles field.
7. A pop-up will appear where you can search for an organization. Once you find the Organization you want to assign to the user persona, select **"add organization."**
8. Users can add roles for each organization; however, this is not required.
9. Select **Save** in the bottom right-hand corner to complete the process of adding an Organization to a User's Persona.

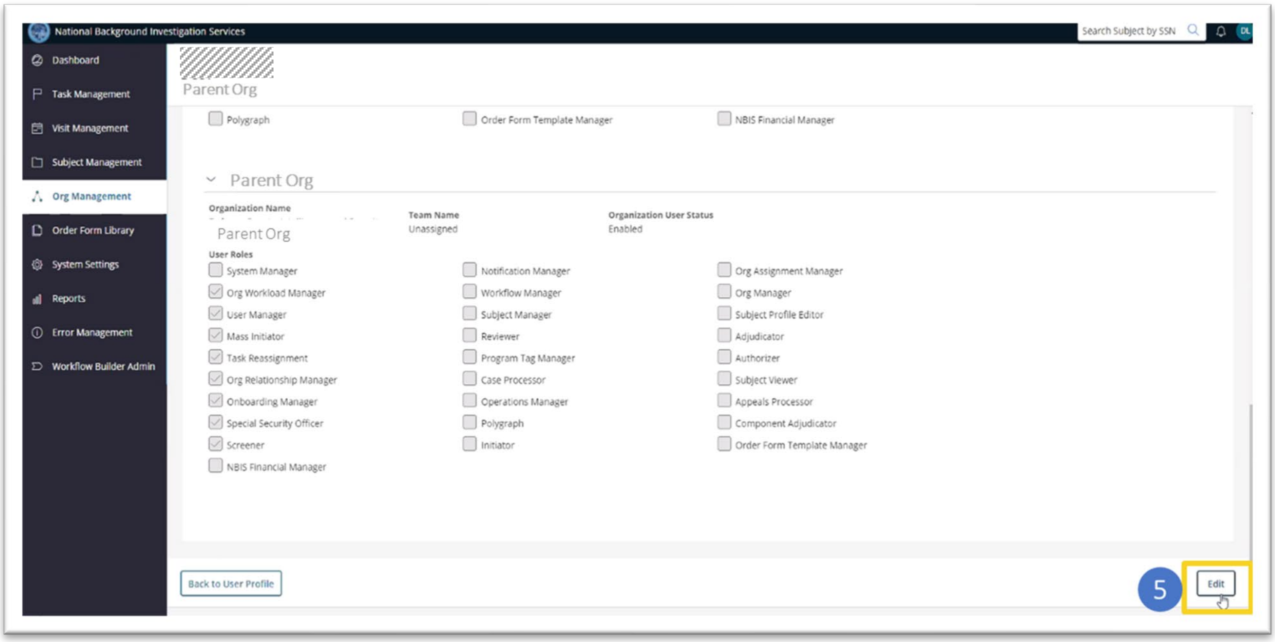
Steps 1-3


National Background Investigation Services
Search Subject by SSN
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Workflow Builder Admin
Parent Org
Parent Org
Search & Switch Org...
Organization
Users
Configuration
User List
Create User
Search on one or more fields at a time (Full SSN with or without dashes, Last 4 of SSN, First Name, Last Name, Organization, Team, Persona Name, and Email).
king
Include Users in My Hierarchy
SSN (Last 4)
Last Name
First Name
Status
Organization
Team
Persona Name
Email
Actions
Active
Parent Org
Parent Org
View Details
1
2
3

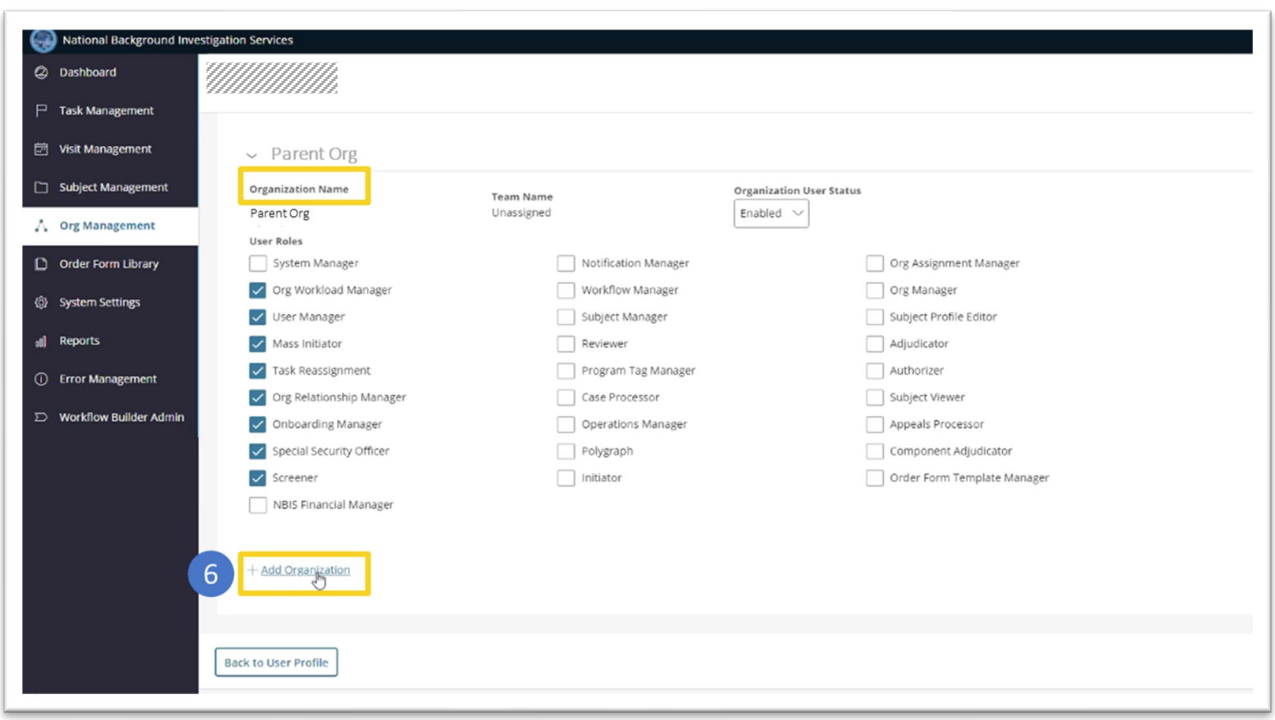
Step 4


National Background Investigation Services
Search Subject by SSN
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Workflow Builder Admin
User Profile
Personally Identifiable Information
Edit Personally Identifiable Information
Social Security Number
XXX-XX-XXXX
Date of Birth
05/04/1989
Last Name
King
First Name
Phyllis
Middle Name
Suffix
Personas
+ Add Persona
Persona Name
Persona Status
Date Created
Last Updated
Actions
XXXX
Enabled
06/21/2021
06/22/2021
Parent Org
Enabled
06/28/2021
06/29/2021
Back
4

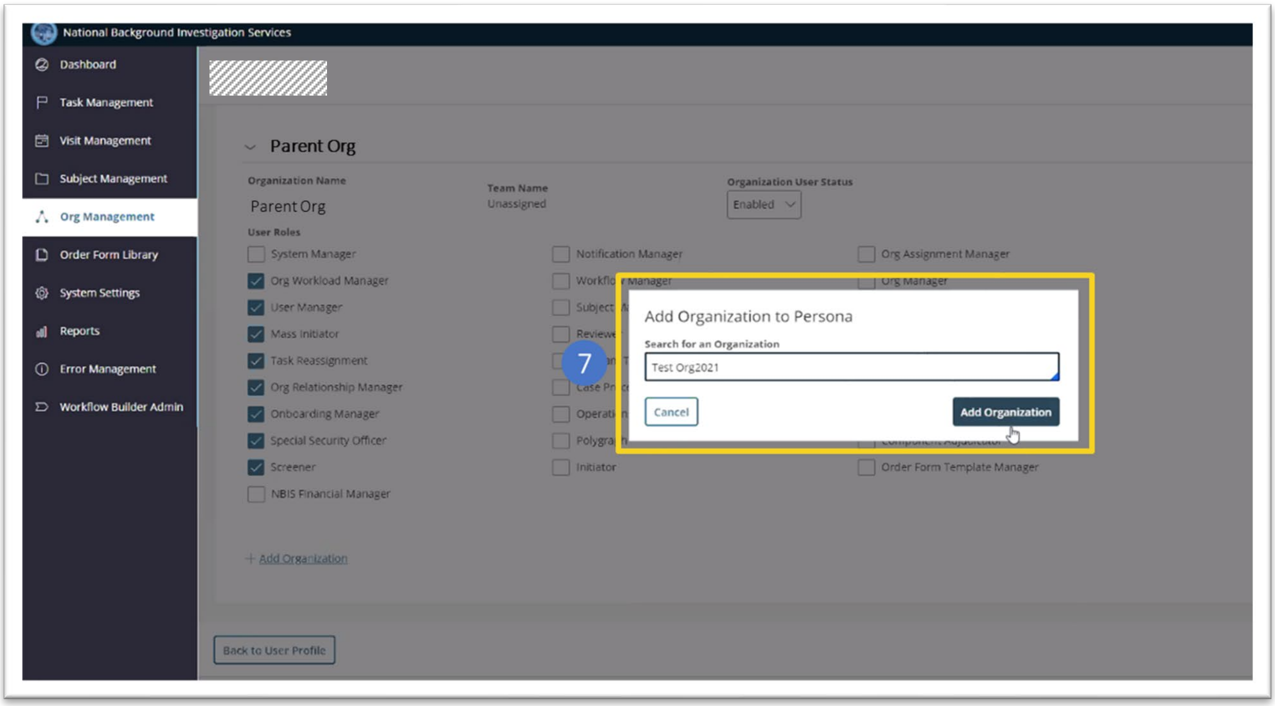
Step 5


National Background Investigation Services
Search Subject by SSN
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Workflow Builder Admin
Parent Org
Polygraph
Order Form Template Manager
NBIS Financial Manager
Parent Org
Organization Name
Parent Org
Team Name
Unassigned
Organization User Status
Enabled
User Roles
System Manager
Org Workload Manager
User Manager
Mass Initiator
Task Reassignment
Org Relationship Manager
Onboarding Manager
Special Security Officer
Screener
NBIS Financial Manager
Notification Manager
Workflow Manager
Subject Manager
Reviewer
Program Tag Manager
Case Processor
Operations Manager
Polygraph
Initiator
Org Assignment Manager
Org Manager
Subject Profile Editor
Adjudicator
Authorizer
Subject Viewer
Appeals Processor
Component Adjudicator
Order Form Template Manager
Back to User Profile
5
Edit

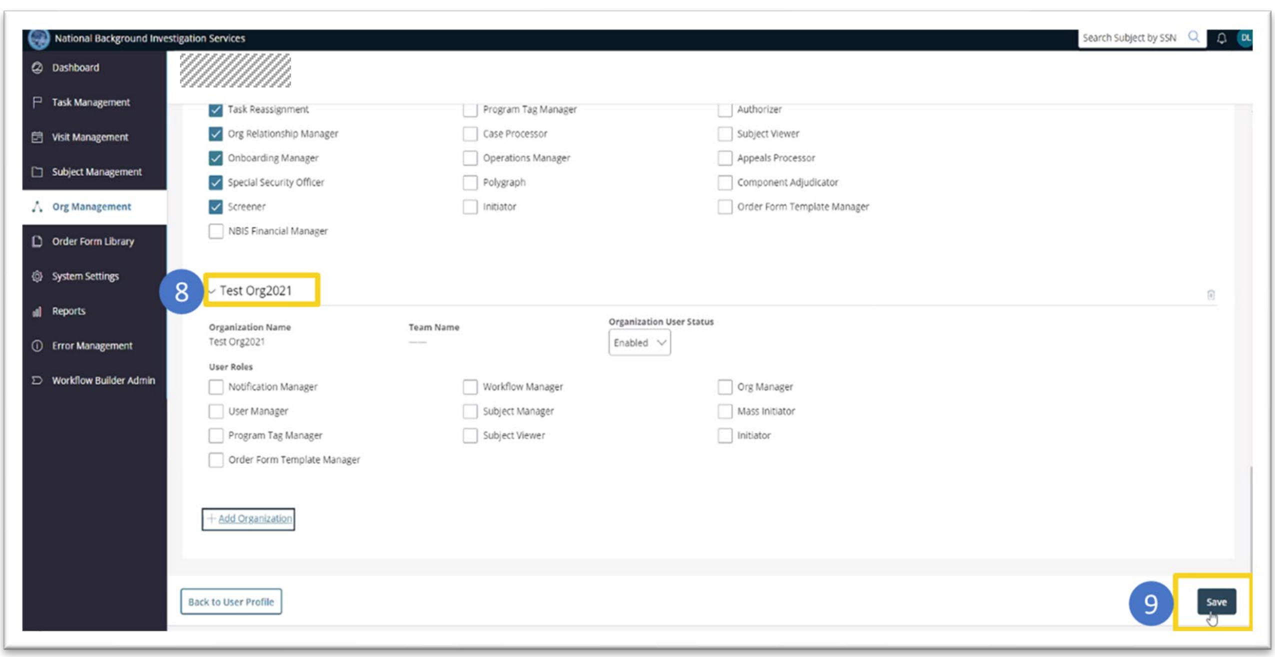
Step 6


National Background Investigation Services
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Workflow Builder Admin
Parent Org
Organization Name
Parent Org
Team Name
Unassigned
Organization User Status
Enabled
User Roles
System Manager
Org Workload Manager
User Manager
Mass Initiator
Task Reassignment
Org Relationship Manager
Onboarding Manager
Special Security Officer
Screener
NBIS Financial Manager
Notification Manager
Workflow Manager
Subject Manager
Reviewer
Program Tag Manager
Case Processor
Operations Manager
Polygraph
Initiator
Org Assignment Manager
Org Manager
Subject Profile Editor
Adjudicator
Authorizer
Subject Viewer
Appeals Processor
Component Adjudicator
Order Form Template Manager
6
+ Add Organization
Back to User Profile

Step 7



Steps 8-9



HOW TO MANAGE A TEAM

A Team is a group of users within a main or sub org, which is created for internal organizational workflow management. The Team Structure Manager role can create Teams, add users to the team, and edit/delete the team.

ADD A TEAM TO AN ORGANIZATION

Below is the 5-step process to create a new Team or add a Sub Team to an existing Team.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the **Teams tab** to view a list of all existing Teams.
3. To add a new Team to the organization, click the "**Add Team"** button. To add a Sub Team under an existing Team, select the ellipses next to the desired team and select **Add Sub Team.**
4. Complete all required fields, including a Team Name and Abbreviation, as well as any additional details. Ensure the status of the Team is "Enabled."
5. Select "**Save and Add**" to create the new team.

ADD USERS TO A TEAM

Below is the 5-step process to assign or reassign users to a team.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the **Teams tab** to view a list of all existing Teams.
3. Select the ellipses next to the desired team and click "**Assign/Reassign User**."
4. Begin typing and select the user's name you would like to assign/reassign. To reassign (i.e., move) a user from another team, begin typing and select the user's current team name in the "From Team" field. Note that the "Target Team" will be auto populated with the team selected.
5. Select "**Assign/Reassign User**" to save.

EDIT A TEAM

Below is the 5-step process to Edit a Team's information.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the **Teams tab** to view a list of all existing Teams.
3. Select the ellipses next to the desired team and click "**View Team**."
4. Click the **Actions** drop-down menu and select **Edit Team.**
5. Under the **Details** tab, modify any of the Team's information including the Team Name, Status (i.e., Enabled/Disabled), and Details.

6. Select the **Users** tab to view the current user list; click the "Assign/Reassign User" button to add new users to the team.
7. Select **Save** to save the updated information.

DELETE A TEAM

Below is the 5-step process to Delete a Team.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the **Teams tab** to view a list of all existing Teams.
3. Select the ellipses next to the desired team and click "**View Team**."
4. Click the **Actions** drop-down menu and select **Delete Team.** Note that you can only delete a Team once all users are removed from the Team and all sub-teams under the Team are removed.
5. A confirmation screen will appear to confirm the deletion of the Team.

UNDERSTAND USER ROLES

The NBIS methodology is to establish initial users in an organization. Then, those users create both the Subordinate Organizations (Sub-Orgs) and the users that populate them. A user's roles are bound by the Organization that they are part of. The parent Organization manages and controls user role options across their Sub-Orgs based on their required functions to support the end-to-end Personnel Vetting (PV) Process. Users can be assigned different roles across various Organizations/Sub-orgs within NBIS, which would give them unique roles in each Organization/Sub-org necessary to execute varied job functions from a single account. An account must be created for a user and given an assigned Persona name that is required when logging in. Multiple Personas can be utilized when a single user has multiple positions requiring NBIS access, as opposed to a single position with varied functions, which would only require a single persona.

HOW TO ACCESS USER ROLE DESCRIPTIONS

The User Role Descriptions document is a list of user roles and the privileges associated with each of them. It is important that users with the User Manager role leverage the User Role Descriptions that are available in NBIS to ensure they are assigning NBIS privileges based on the user's designated functions and roles. The User Role Descriptions can be accessed in the following three ways:

1. Org Management Tab > Actions > Add Org > Scroll down below Org role field to select the hyperlink titled View Permission/Role Descriptions.
2. Org Management Tab > User Tab > Ellipses > View Details > Select Persona Name > Link to View Permission/Role Descriptions is in the top right-hand corner.
3. User Initials Icon > Profile > Select the hyperlinked Persona Name > Link to View Permission/Role Descriptions is in the top right-hand corner of the "Persona Settings" screen

REVIEW USER ROLE DESCRIPTIONS

The User Role Descriptions can be accessed within NBIS as a link when creating an Org and referenced to make informed decisions when choosing roles assigned to each user. It is important to note that not every user will have the same roles based on their responsibilities and levels of access. In addition, the roles available to the users in a particular Organization is dependent upon the Organization's Type, Functions, and Roles. The list below provides examples of some of the user role descriptions.

- Authorizer: An Organization user who reviews entire cases, completes financial details, edits certain Order Form details, and decides whether to approve, reject or hold cases.
- Facility Security Officer: A user that can manage subjects and complete actions such as initiating case requests, manually create adjudication cases, add/edit subjects' PII, contractor affiliations, access, and complete appeals and visit requests for subjects. They can also create, edit, request, and approve visit events; manage interim determinations from the subject profile; and manually reassign tasks to users in their org.
- Initiator: An Organization user who initiates the Subject/employee investigation, selects form(s) to be completed by the Subject, completes the Top-Level Org Usage Block (AUB), contacts

Subjects/employees to inform them that they should complete the investigation form(s) using eApp, requests an Authentication reset and cancels/un-cancels requests.

- Mass Initiator: A user that can mass initiate subjects in the system. This role also has access to view subjects in Subject Management.
- Notification Manager: A user that is responsible for creating, customizing, and managing criteria for automatic alerts that can be used throughout the lifecycle of a case.
- Onboarding Manager: A user that can manage Org Levels and create Orgs with grouped Org Levels. This role also has permissions to add any function or Org type to an Org regardless of inherited restrictions.
- Order Form Template Manager: A user that can manage Order Form Templates for their organizations.
- Org Assignment Manager: A user that is Responsible for setting an organization's priorities for work assignments to enable the automatic routing of tasks.
- Org Manager: A user that is responsible for creating an organization's hierarchy and assigning associated roles for each hierarchy element.
- Org Relationship Manager: A user who can manage Org relationships established between Organizations outside each other's hierarchy or servicing relationships to Orgs in their hierarchy, in the Org Relationship tab.
- Org Workload Manager: A user that can manage skillsets of users in their organization and manually assign cases to users within their organizations.
- Program Tag Manager: A user that can manage the program tags that are available for their organizations.
- Reviewer: A user who reviews the submitted Standard Form (SF8X) for accuracy and completeness and determines whether the form is suitable to move the request for investigation forward (i.e., makes a go/no-go decision).
- Subject Viewer: A user that can view subject information from within Subject Management, as well as visit information within Visit Management.
- Task Reassignment: A user that can reassign cases to users within their team or, if unassigned to a team, to others who are unassigned within their organization from within the Order Form. Needs to be paired with Initiator, Reviewer, or Authorizer.
- User Manager: A user that is responsible for establishing roles and permissions for individuals within an Organization, Sub-Organization(s), and team(s).
- Workflow Manager: A user that is responsible for determining the routing of new case initiations through the Review, Authorize and Investigation processes.

HOW TO ADD A USER TO THE NBIS SYSTEM

Prior to creating a new user, an organization must receive the user's completed PSSAR form, to include necessary training certifications. The user then must be created in NBIS and added to their specific organization or hierarchy. Users with the User Manager role can create users and assign them appropriate roles and access privileges based on their responsibilities. Users are first created and then given a persona/multiple personas and roles for their specific duties. Below is the 15-step process for how to Grant NBIS System Access, create a User, and Add a Persona to a User.

HOW TO GRANT ACCESS

1. Users must submit a completed **Personnel Security System Access Request (PSSAR) form** to the Organization's Onboarding Manager(s). The PSSAR documents the formal account request, provides accountability for the User, requests account deletions, and makes changes to User roles and permissions.
2. Prior to provisioning a user into NBIS, an organization must review, approve, and maintain the User's PSSAR Form to confirm the following in order to grant system access:

a. The individual has completed the necessary training with regards to Security Awareness and safe-guarding Personally Identifiable Information (PII)

b. The Nominating Official has certified the applicant meets the requirements to grant the system access request

c. The Validating Official has verified that the individual meets the investigation requirements and has a need-to-know reason to access the system.

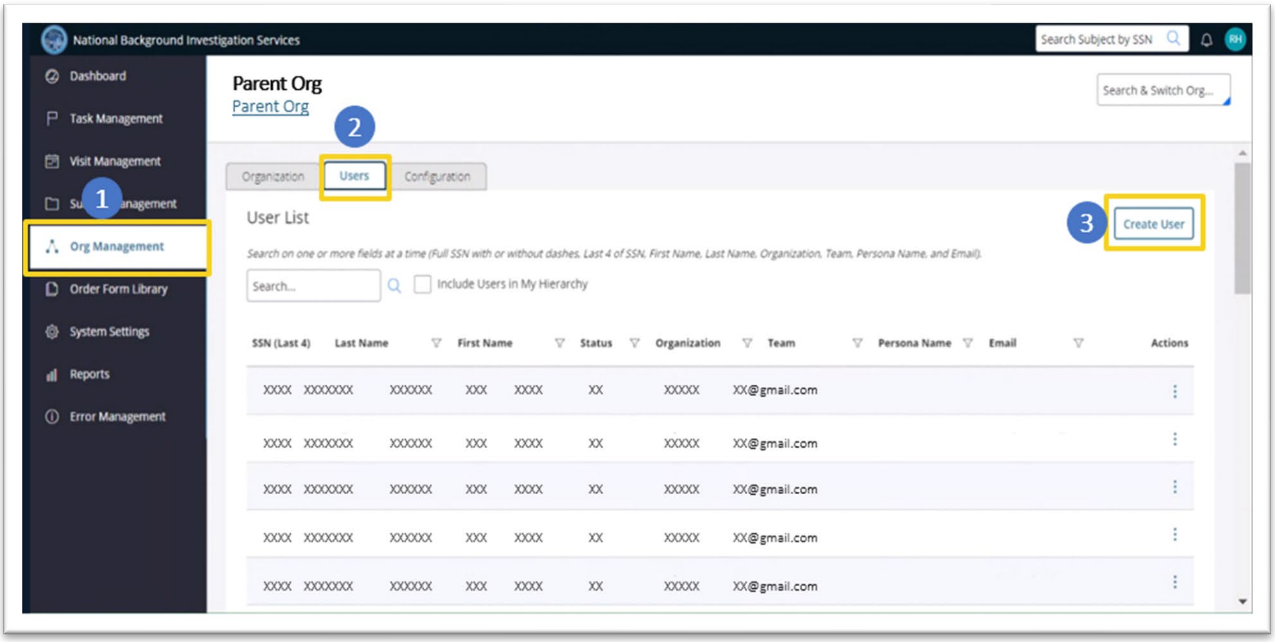
d. The completed PSSAR and training documents must be properly maintained by the Organization to adequately reflect policy compliance.

3. Once the User's PSSAR has been completed, reviewed, and approved, the User can be granted access to the NBIS System.

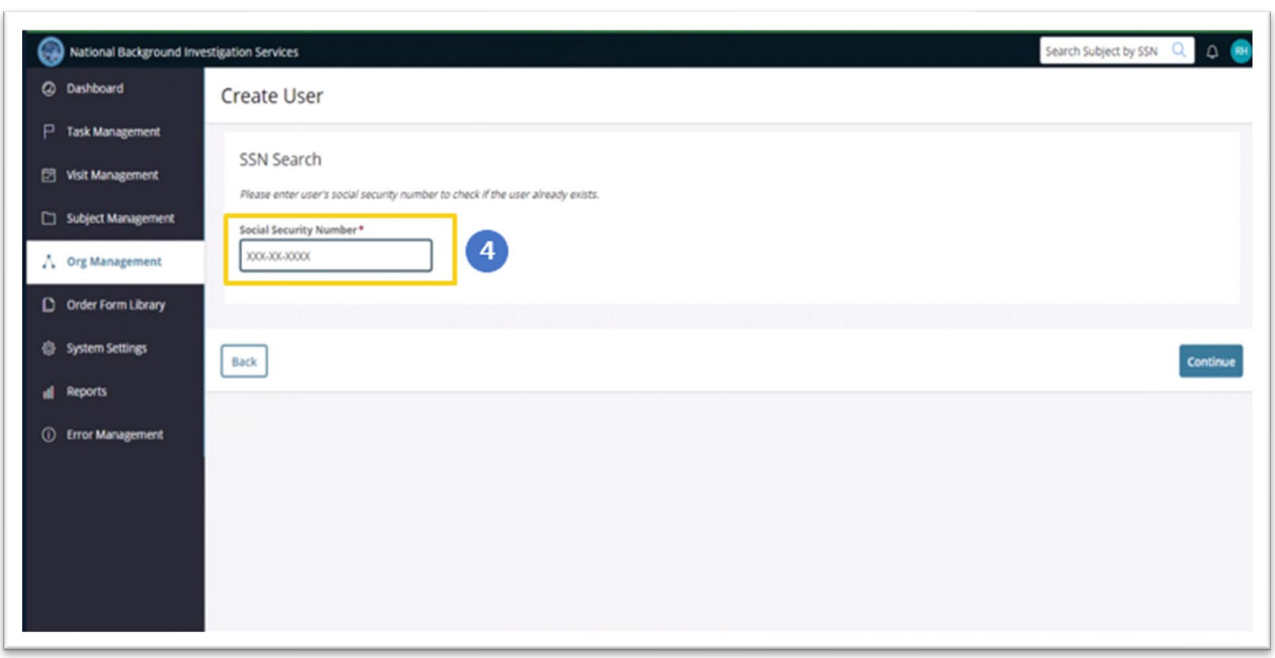
HOW TO ADD A USER AND USER PERSONA

1. Navigate to Org Management on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the Users tab.
3. From the right-hand side, select **Create User button**.
4. In the SSN Search text box, enter the user's **social security number** (located in Block 11 of the PSSAR) and select **Continue**. If the user does not exist in the system, the Create User screen displays. Note: If the user already exists, the existing user record will display, see View User for more information. User Managers will be able to modify the SSN and DOB after the user is created. However, the system will not allow users to search their own SSN.

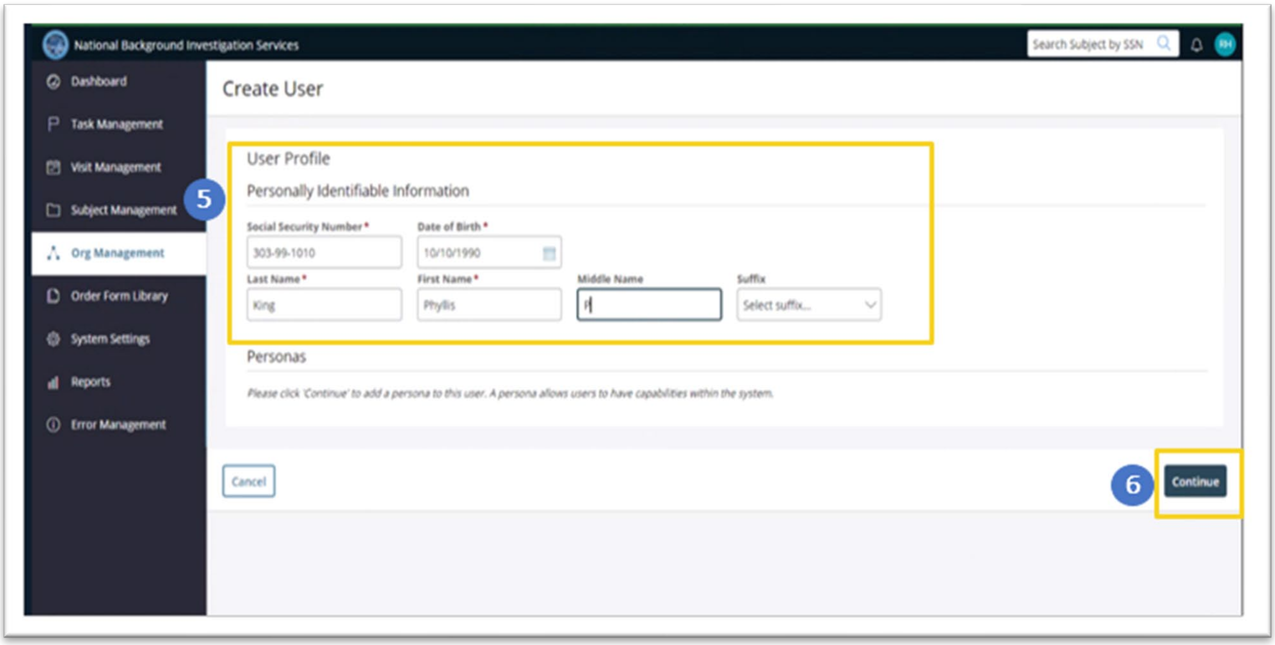
5. Fill in the required Personally Identified Information (PII) under **User Profile**, indicated with a red asterisk. Note: The User's First and Last Name can be found in Block 1 of the PSSAR and their DOB can be found in Block 9.
6. After filling out all user information, select **Continue** to create a Persona to add to a user. Note: A Persona represents an account with its roles and privileges that the user will have for the org associated to the persona. A persona will also represent an account the user will use to login to the system. A user can have multiple personas that are associated to multiple orgs.
7. In the Manage Persona Settings tab, enter "NBIS User" as the user's **Persona Name.** The Persona Name cannot be changed once the Persona is created.
8. Enter **Primary Phone Number** (PSSAR Block 4) and Email Address (PSSAR Block 5). Select a Notification Preference option and the appropriate Time Zone. Note: The Internal option displays notification alerts in the top right corner of the application where the bell symbol is located. The Email option will route notifications to the primary email address entered for the user.
9. Select **Add Attachment** to upload required documents. Users will receive a pop-up asking: "Are you sure you want to upload a file." Select "Browse" to search your files for the required documents. Select the following Attachment Categories for the required documents listed below:
   a. System Authorization Access Request (PSSAR Form)
   b. Training Certificate (Cyber-awareness Training Certificate and PII Training Certificate)
10. The Organization context should be pre-populated based on the Org in which the user with the User Manager role is creating the Persona. Select the **User Roles** the user will be granted within the Organization. At least one role must be selected at the time of creation. Enable is automatically selected as Organization User Status. Users can add additional Orgs by selecting +Add Organization.
    - Note: Users can also add User Assignments by entering information in the Manage User Assignments tab. The full process for how to add a User Assignment will be covered in the "Add User Assignments Template to a User" task. Users will receive a pop-up asking if they'd like to proceed with completing the User Profile if they do not create a User Assignment.
11. Select **Complete User Profile** to save it.



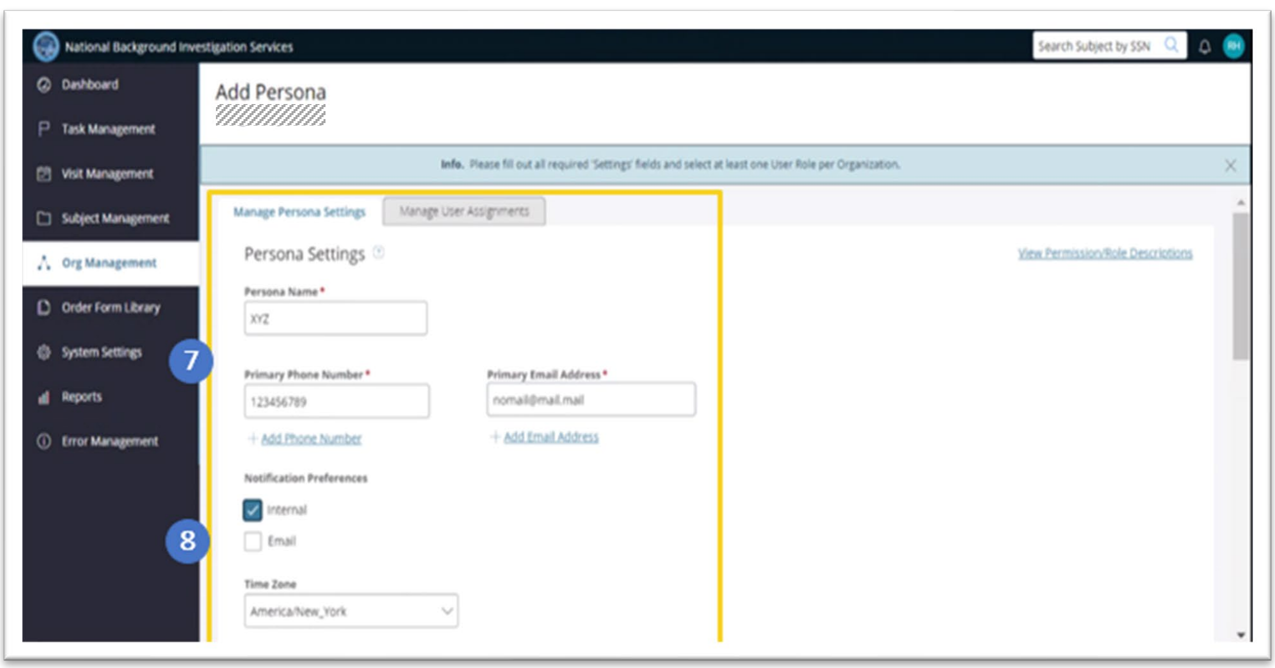
How to Add a User and User Persona (Step 4)



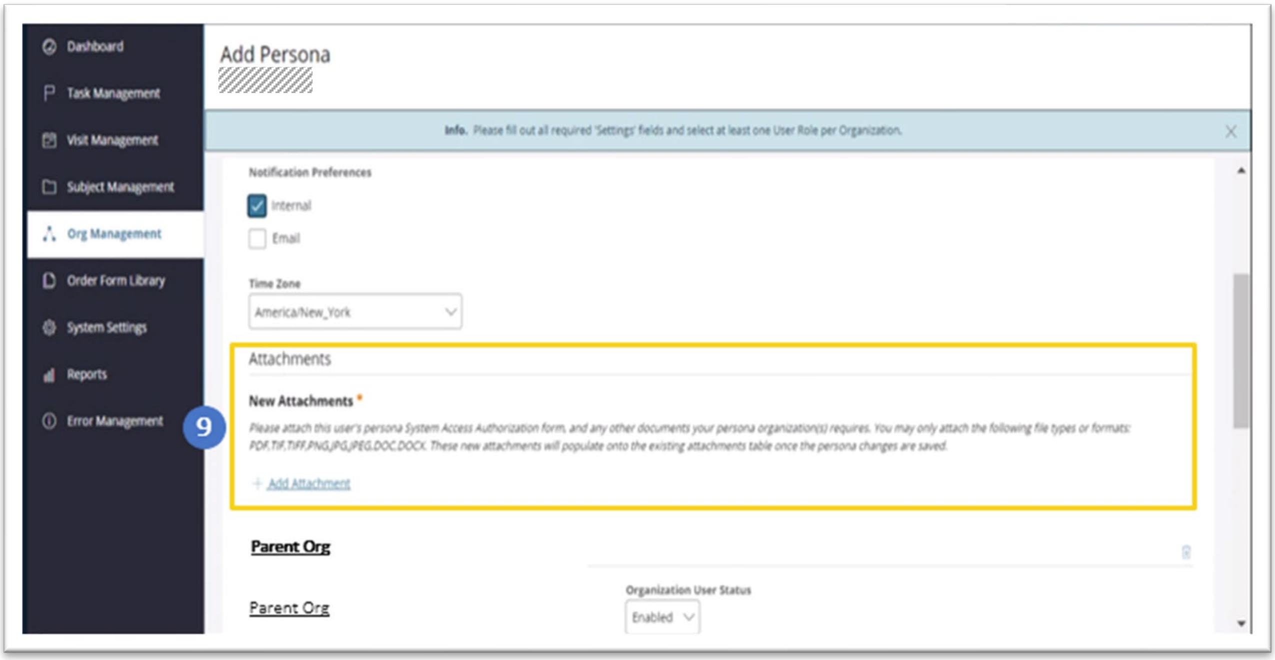
How to Add a User and User Persona (Steps 5-6)



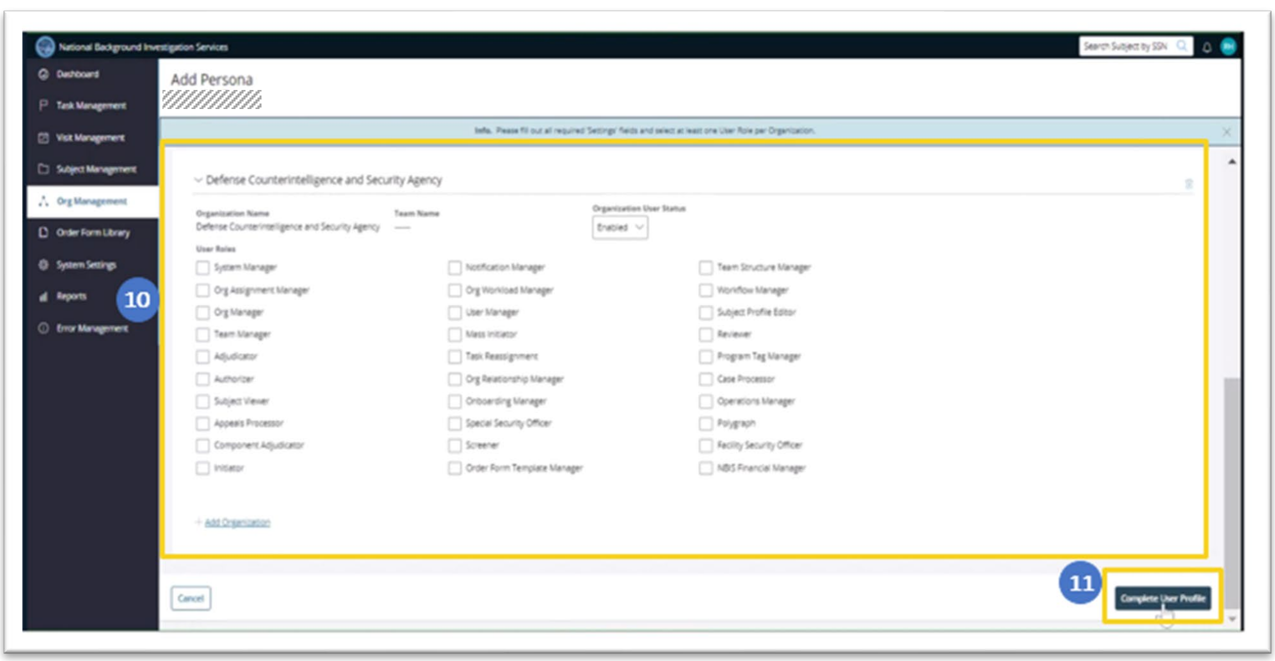
How to Add a User and User Persona (Steps 7-8)



How to Add a User and User Persona (Step 9)



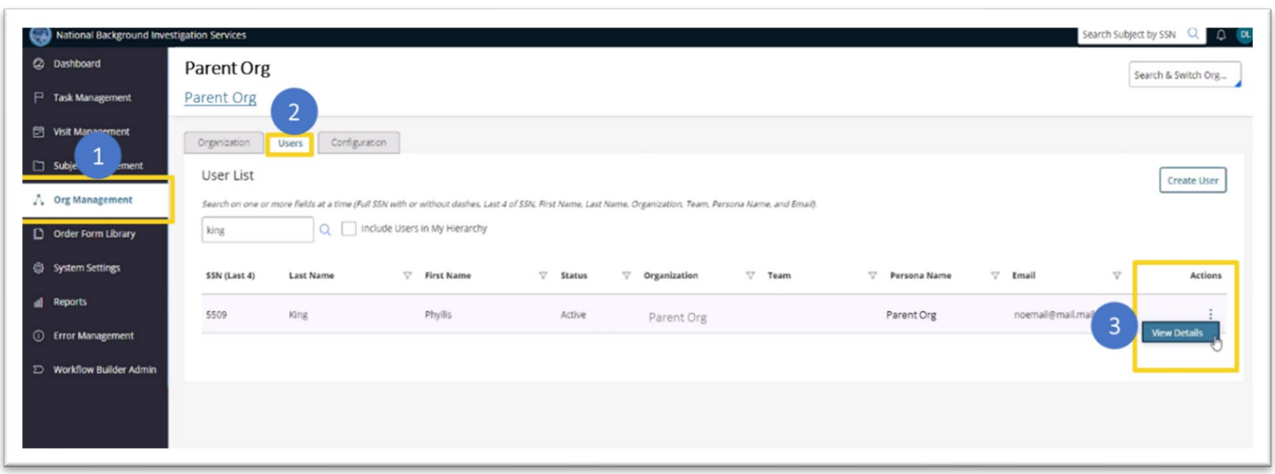
How to Add a User and User Persona (Steps 10-11)



HOW TO VIEW USER PROFILES

Users with the User Manager role can view user profiles within an organization hierarchy. Below is the 3-step process for viewing existing users in NBIS.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Select the **Users** tab to view a list of users within the selected Organization.
3. From the Actions column, select the ellipses icon (…) next to the desired user row, then select **View Details** to view the User's profile details.



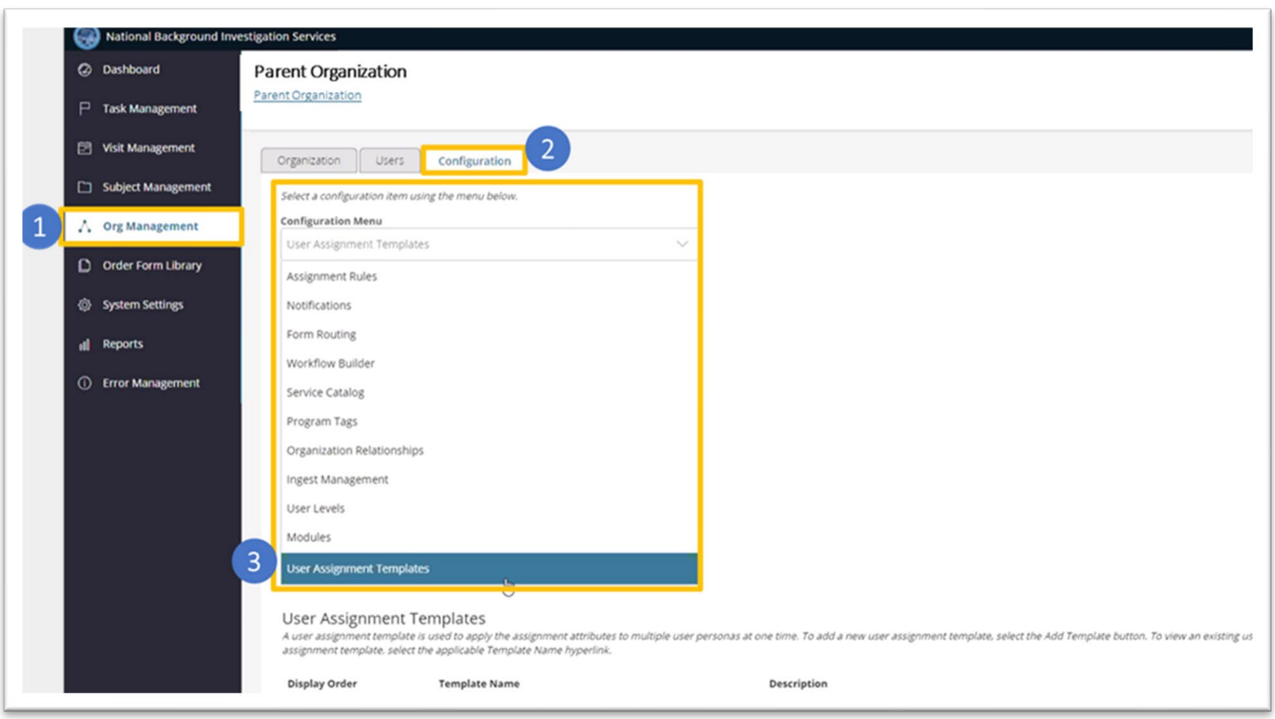
HOW TO CREATE AND VIEW A USER ASSIGNMENT TEMPLATE

Users with the User Manager role can create standard templates to use when completing a user's assignment capabilities in their user profile for a more efficient way of completing that information. Once created, User Assignment Templates are used to apply assignment attributes to an individual user in one persona and multiple assignments can be added within one template. This can be particularly helpful/timesaving if you have many users that require the same assignment logic.

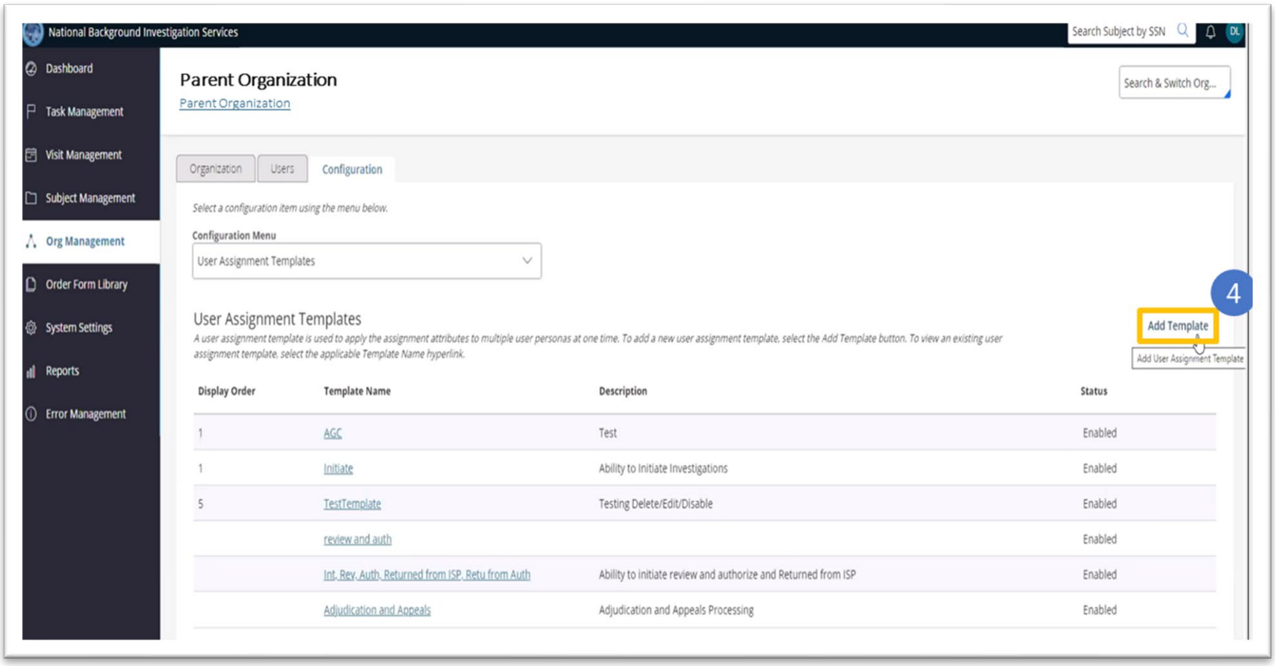
CREATE A USER ASSIGNMENT TEMPLATE

Below is the 12-step process for how to Create a User Assignment Template.

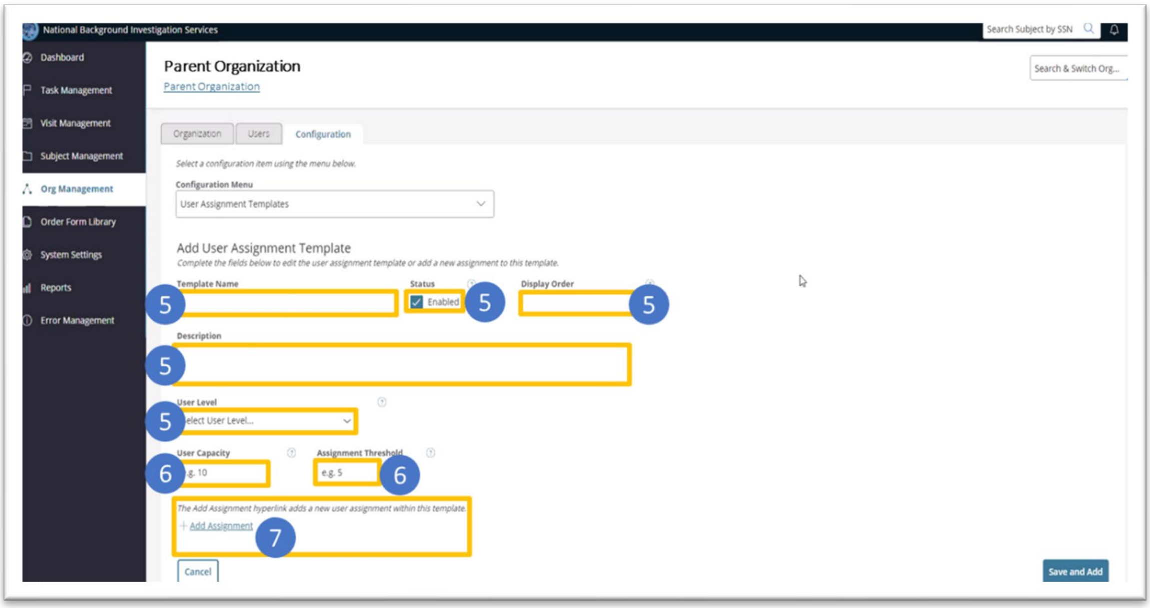
1. From log in, select **Org Management** from the navigation menu on the left.
2. Switch to the designated Org (if needed) and select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **User Assignment Templates**.



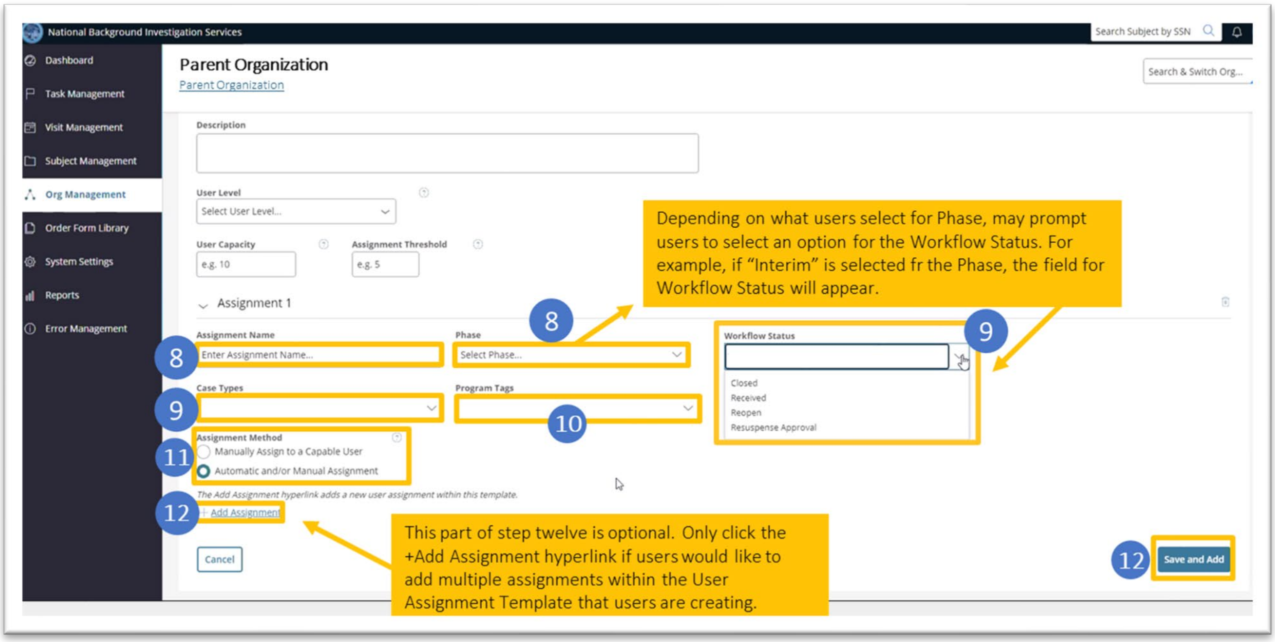
4. To create a new template, select **Add Template**.



5. Provide the Template Name, Status, Display Order, Description, and User Level.
6. If the user will be receiving automatically assigned work, configure the **User Capacity** and **Assignment Threshold** Values. Note: The User Capacity defines the maximum number of assignments a user can automatically be assigned; however, users can still be assigned a case manually, which may exceed the user's capacity. The Assignment Threshold defines the number of assignments a user owns before the system automatically assigns additional tasks. These fields are required if Automatic and/or Manual Assignment method is selected for an assignment.
7. Select **Add Assignment** to add an assignment within the User Assignment Template. Multiple assignments can be added.



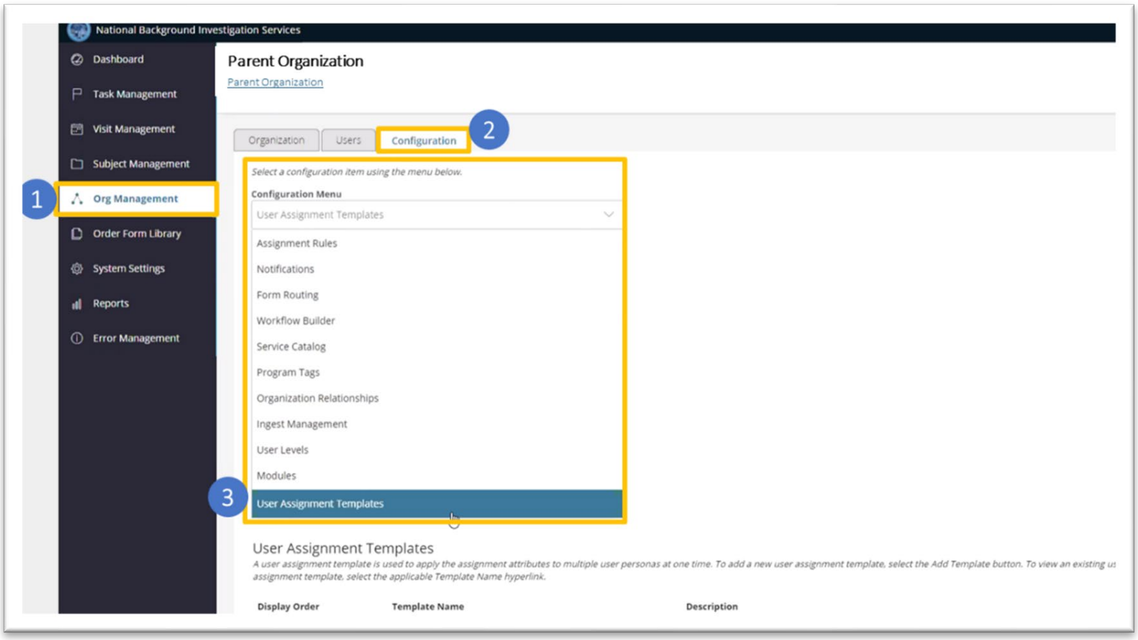
8. Enter the **Assignment Name**. Select the Phase for the assignment from the drop-down menu. The phase determines what phase of the case the user can work on. Additional fields will populate depending on the phase selected.
9. From the drop-down menus, select the appropriate **Case Type(s)** and **Workflow Status** for the user. These sections indicate the types of cases or tasks users want a user to be capable of working.
10. From the drop-down menu, select any applicable **Program Tags** needed for this assignment configuration.
11. Select the **Assignment Method**. Select either Manually Assign to a Capable User or Automatic and/or Manual Assignment.
12. Select **+Add Assignment** to add another assignment within the same template or click **Save and Add** if users do not need to add another assignment.



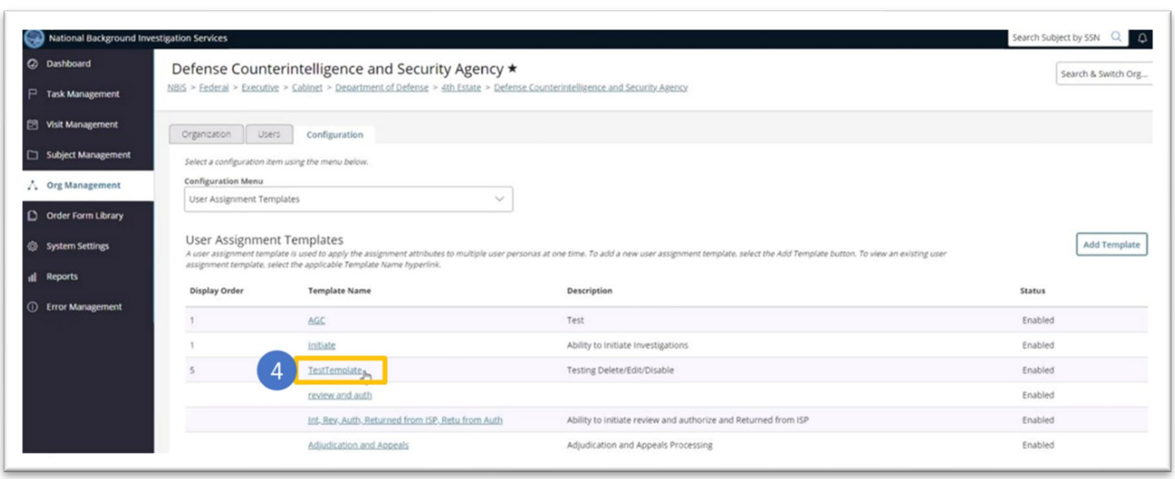
VIEW A USER ASSIGNMENT TEMPLATE

Users with the User Manager role can also view User Assignment Templates. Below is the 4-step process for how to View User Assignment Templates.

1. From log in, select **Org Management** from the navigation menu on the left.
2. Switch to the designated Org (if needed) and select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **User Assignment Templates**. This will prompt users with the list of existing User Assignment Templates.



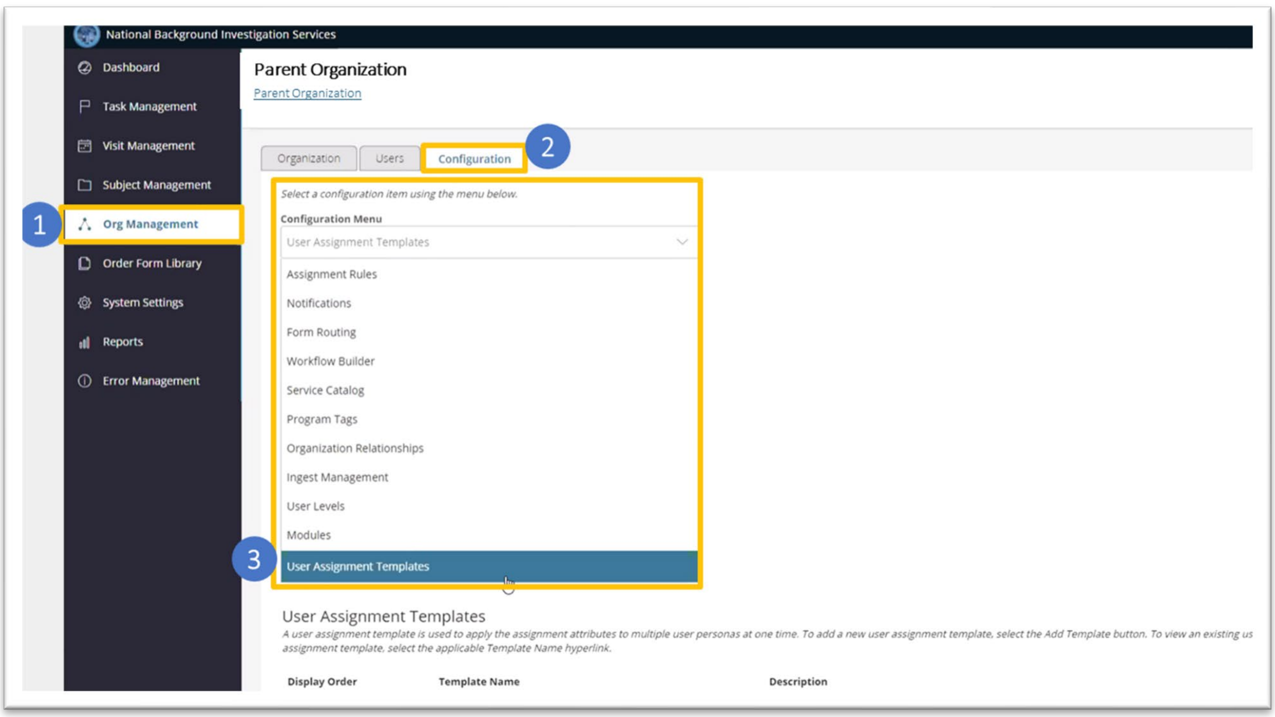
4. Select the **hyperlink** within the Template Name column to view the details of any specific User Assignment template.



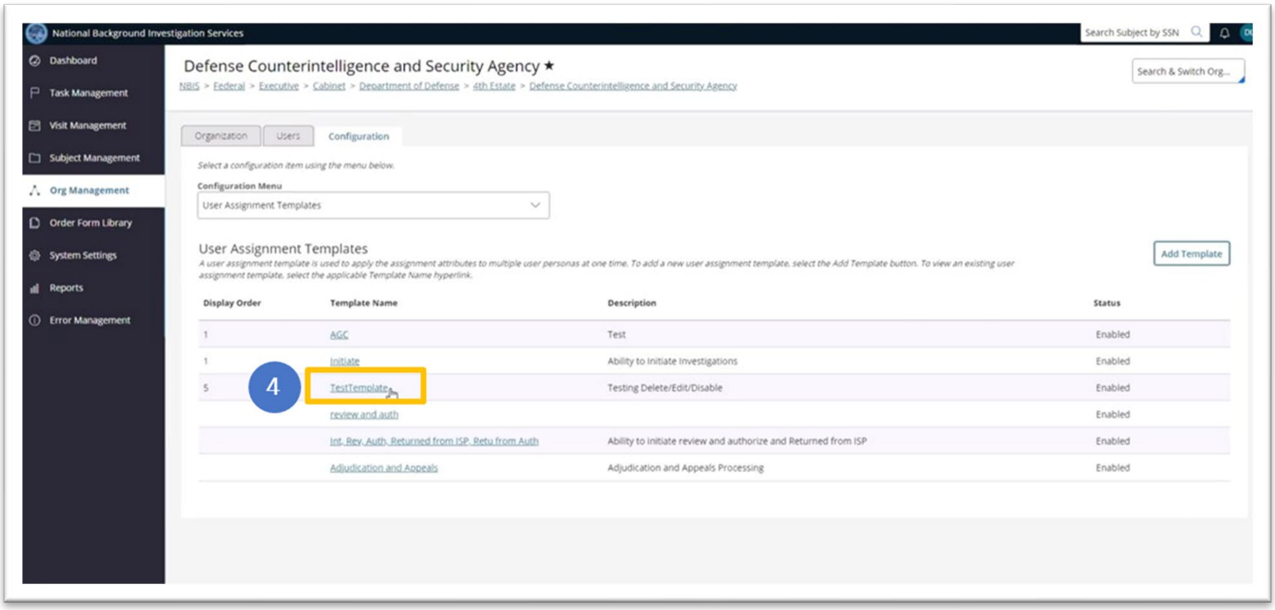
HOW TO EDIT, DISABLE, OR DELETE USER ASSIGNMENT TEMPLATES

Users with the User Manager role can Delete a User Assignment Template if a user's assignment changes or if the team's assignments change. Additionally, users with the User Manager role can Disable a User Assignment Template just in case users may not need to use the template now but will want to use it later. A Disabled User Assignment Template can always be enabled at any time. However, once the User Assignment Template has been deleted it cannot be retrieved and is permanently deleted. Below outlines the 6-step process to Edit, Disable, or Delete a User Assignment Template.

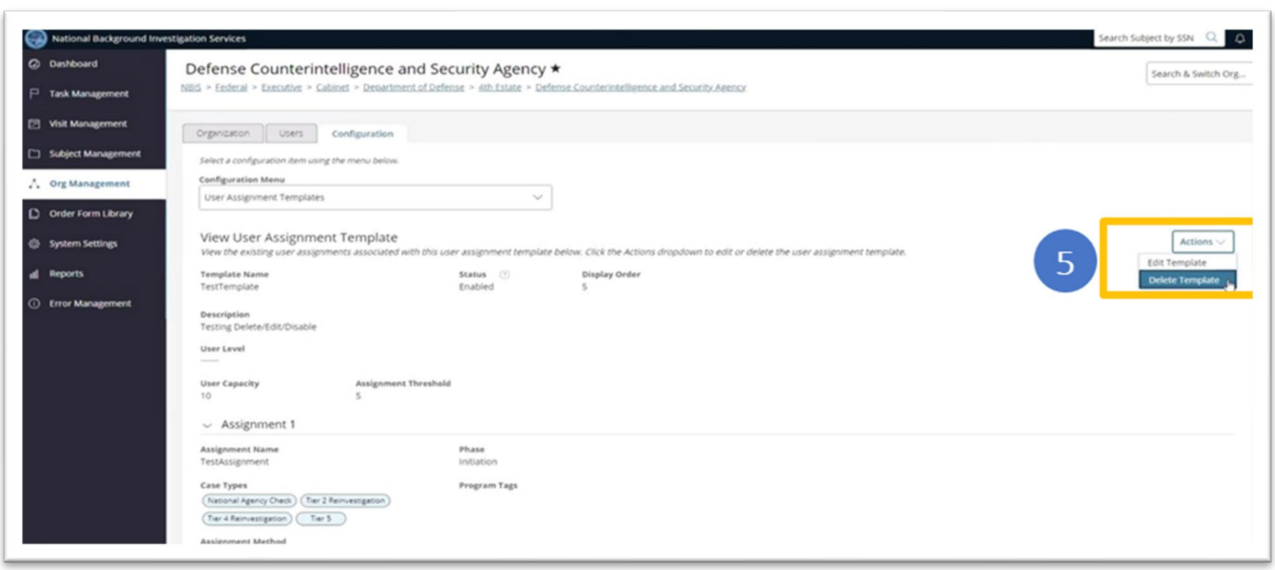
1. From log in, select **Org Management** from the navigation menu on the left.
2. Switch to the designated Org (if needed) and select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **User Assignment Templates**.



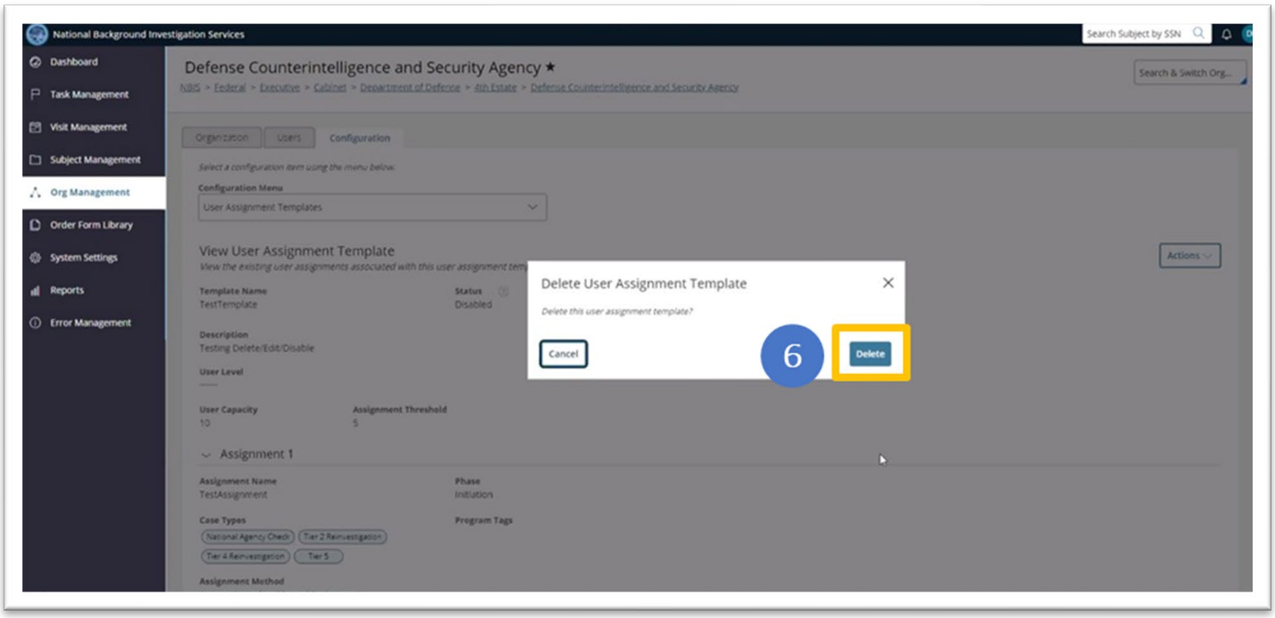
4. From the list of User Assignment Templates, select the actual template users would like to edit under the Template Name column.



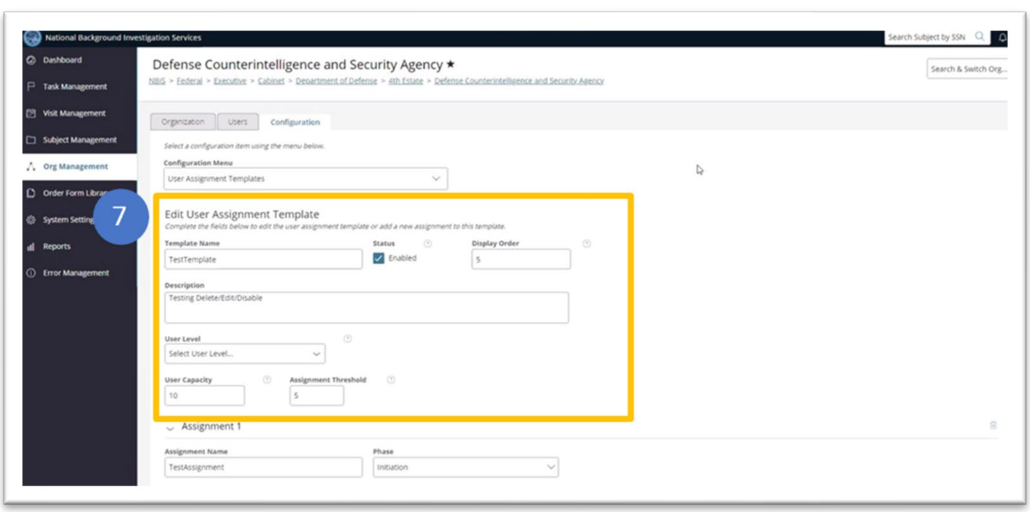
5. Select the **Actions** drop-down menu. Users will be prompted with Edit and Delete options.



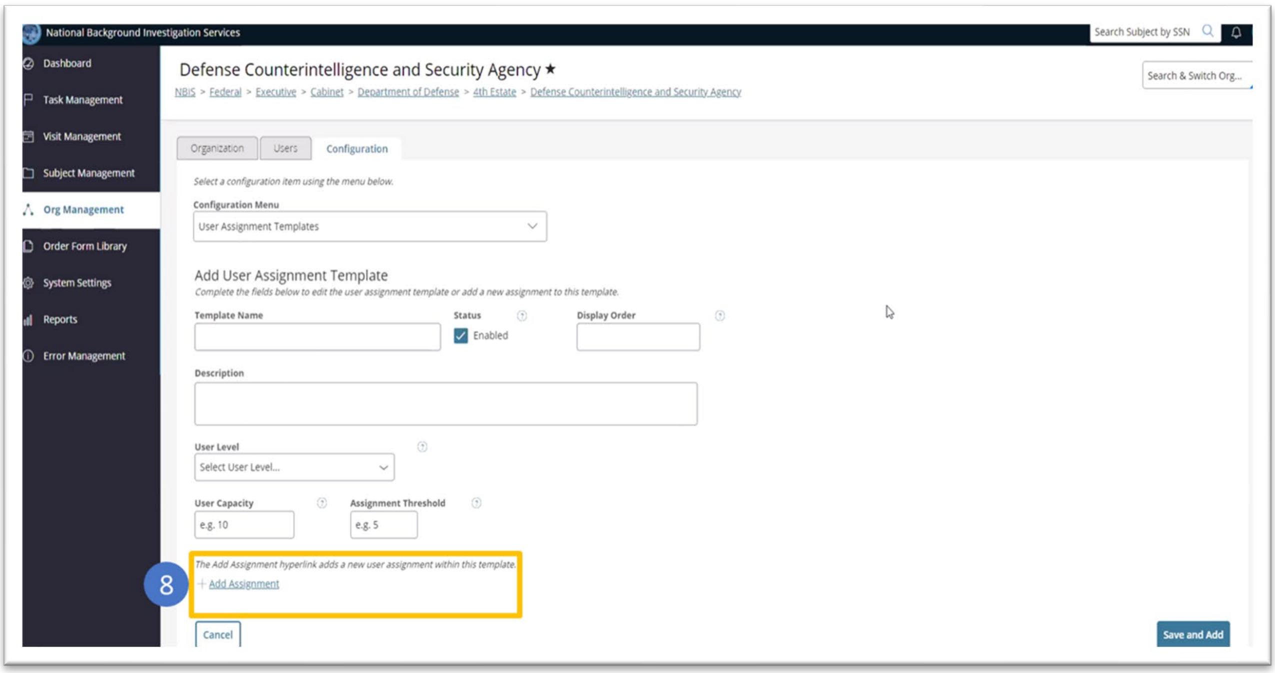
6. To delete the User Assignment Template, select **Delete Template**. Users will be prompted with a warning screen. Select Delete again. The deleted User Assignment Template will not appear in the list of existing User Assignment Templates screen; this will be confirmation that users successfully deleted the User Assignment Template.



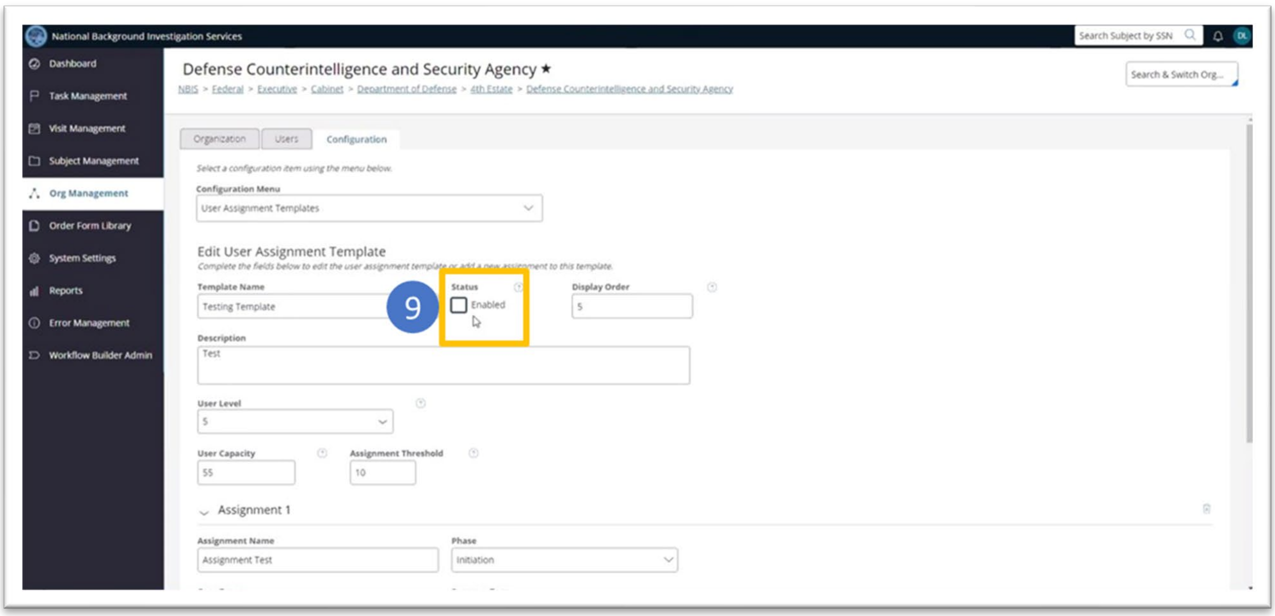
7. To edit or disable the User Assignment Template, select **Edit Template**; this will bring users to the Edit User Assignment Templates page. From the Edit User Assignment Templates page, users can configure and edit any User Assignment Template details.



8. Select the **+Add Assignment hyperlink** to a add a new assignment within the existing User Assignment Template. Complete all required fields including Assignment Name, Phase, Case Types, Program Tags and Assignment Method. Click Save at the bottom right corner. After users click Save, users will return to User Assignment Templates home screen/User Assignment Templates list.



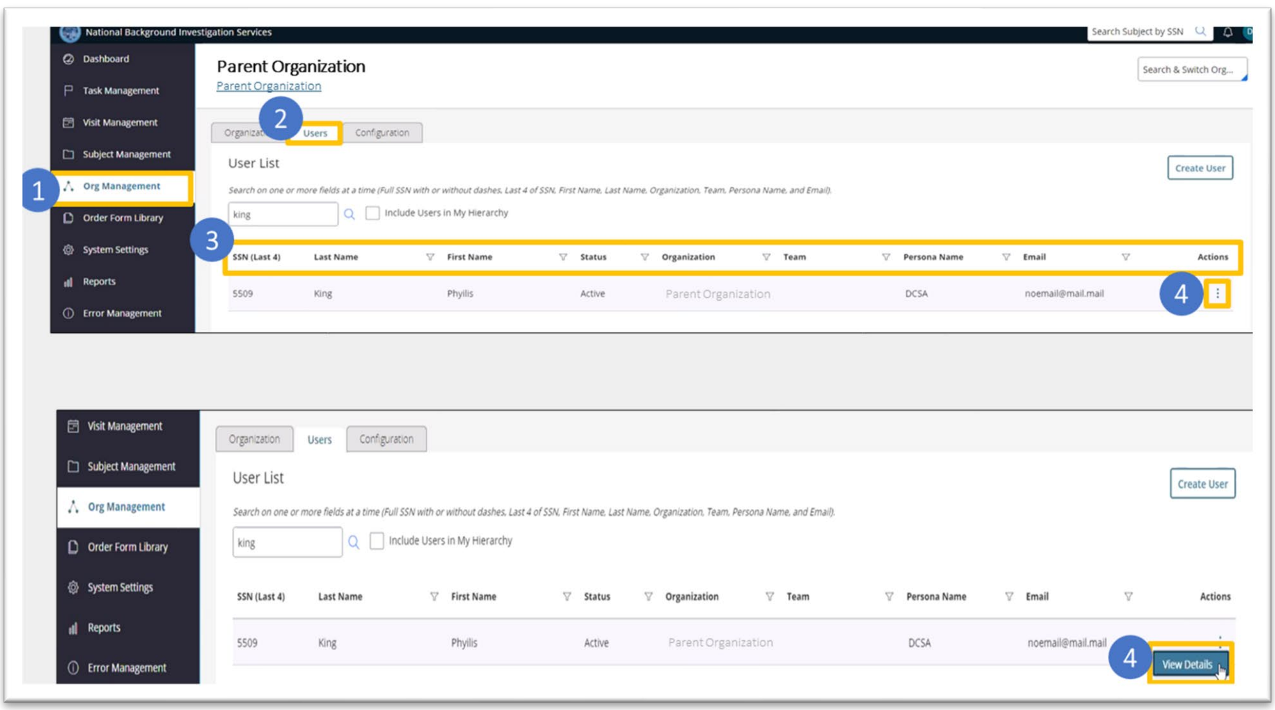
9. To **Disable** the User Assignment Template, make sure the **Enabled box** beneath status is unchecked in order to disable the User Assignment Template. Click **Save** in the bottom right corner. Users will return to the list of existing User Assignment Templates displaying all User Assignment Templates organized by their display order.



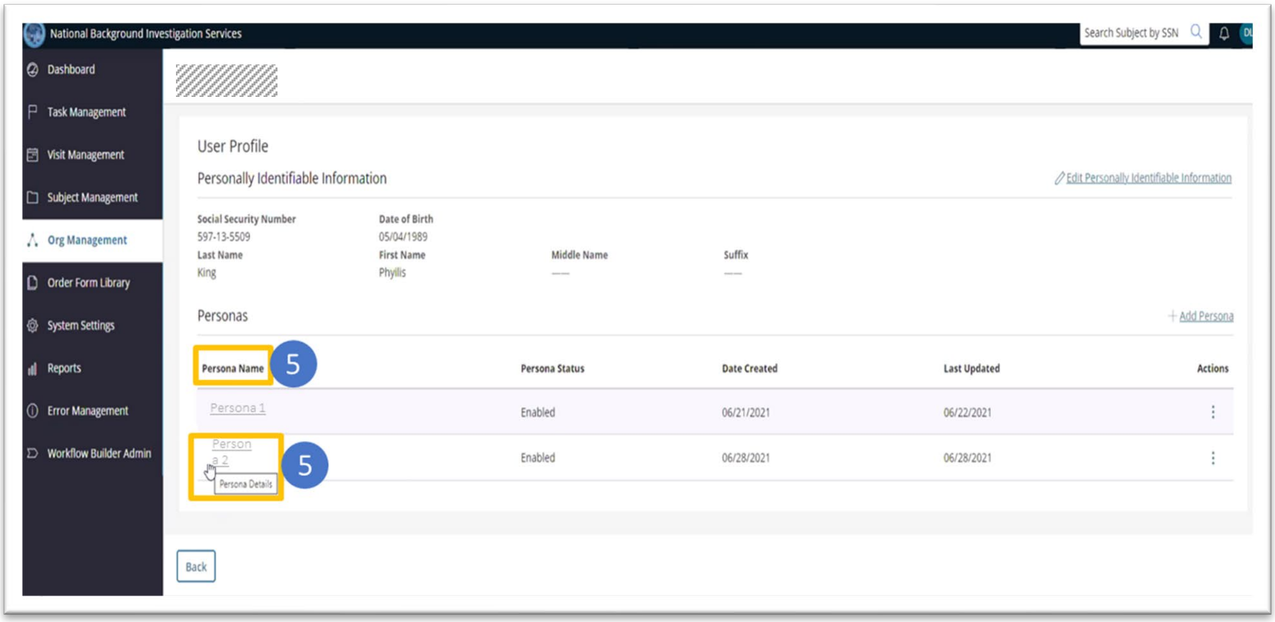
HOW TO ADD A USER ASSIGNMENT TEMPLATE TO A USER

User Assignments manage the number of tasks a user is assigned to perform within the context of the Organization. User Assignments are what allow a user to work on cases with certain attributes. User Assignments can be applied when creating a user from the Manage User Assignments tab and also appears as a notification if a new user created without assigning a user assignment. Below is the 12-step process for how the users with the User Manager role can add a User Assignment to an existing user.

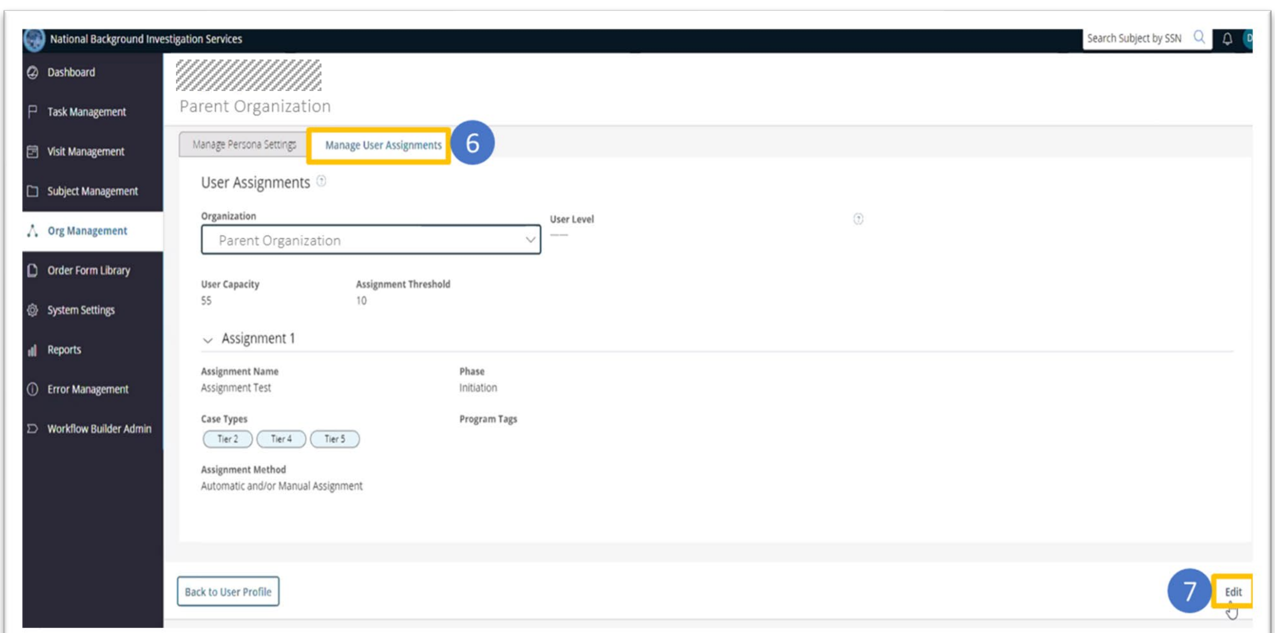
1. From initial log in, select the **Org Management** tab from the navigation menu on the left.
2. Switch to the designated Org (if needed) and select the **Users** tab.
3. Scroll through the existing users from the User List to **identify the user** to add/apply an assignment template to.
4. From the Actions column, select the ellipses (three vertical dots) and select **View Details** to be prompted with the User Profile screen.



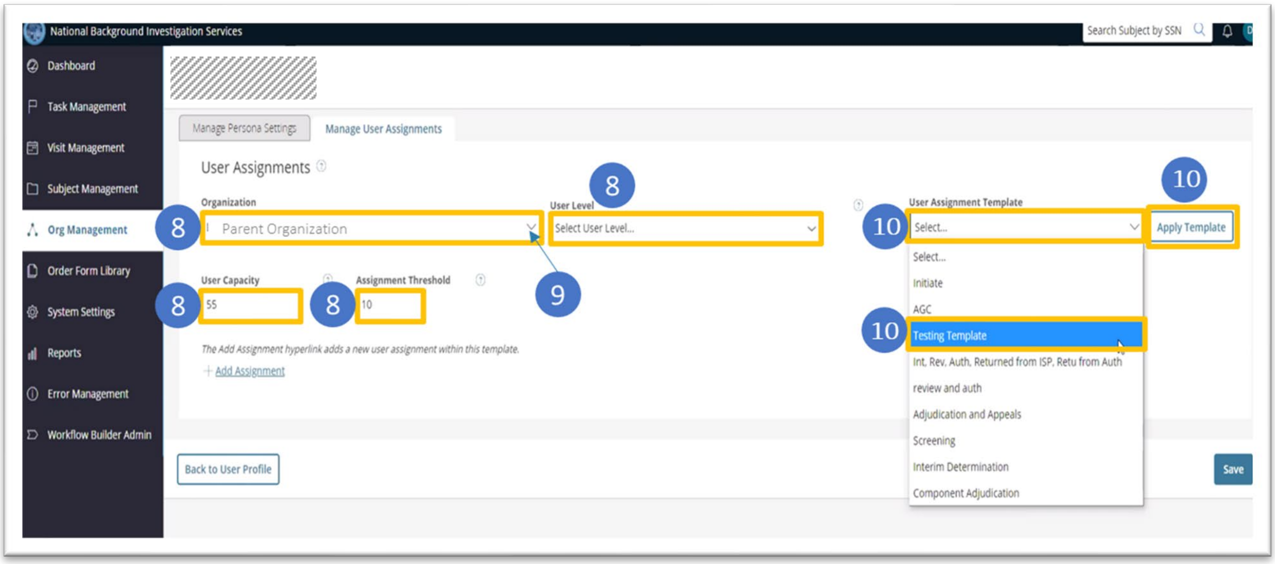
5. Click the **hyperlink** for the user's persona under the persona name column. If a user has multiple personas, make sure to select the Persona to edit/work on and be prompted with Persona Settings page.



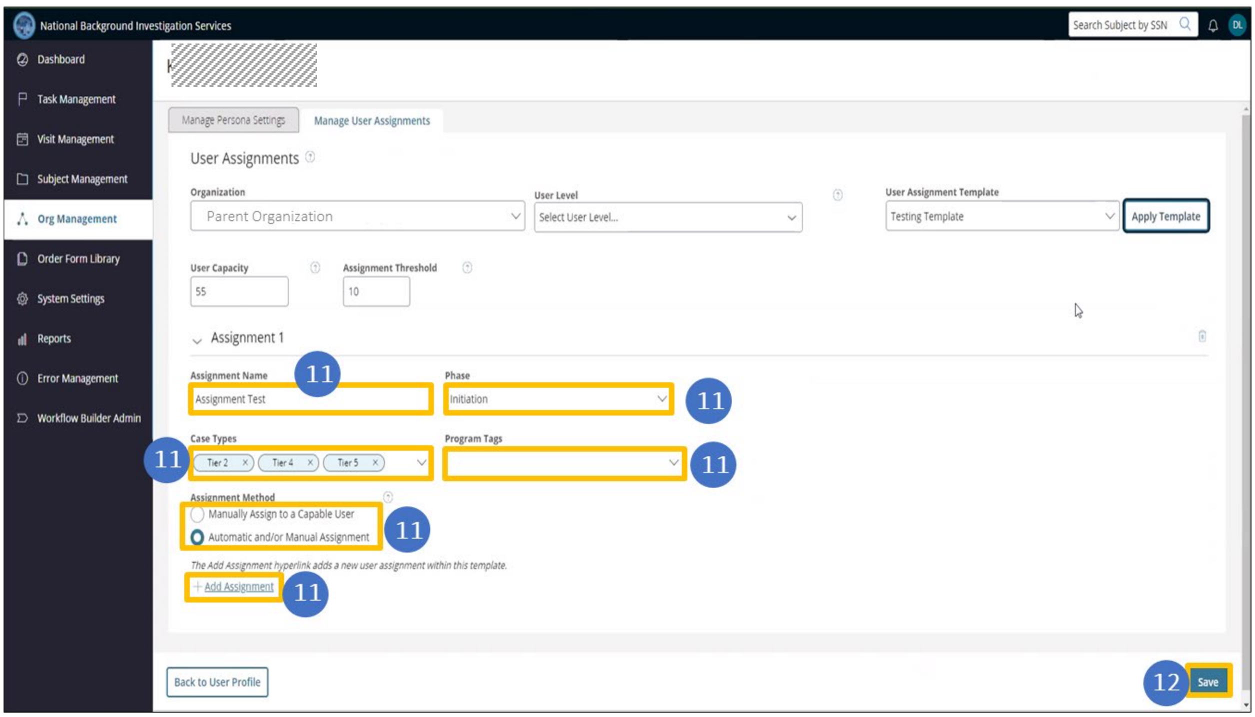
6. Select **Manage User Assignments** tab.
7. Click the **Edit** button on bottom right of screen to be prompted with Organization, User Level and User Assignment Templates fields.



8. Complete all required fields, including those from step 7 in addition to selecting the Organization, User Capacity, and Assignment Threshold.
9. Under the Organization drop-down menu, make sure the organization selected correlate to where the User Assignment template is housed.
10. From the User Assignment Template drop-down options, select the appropriate User Assignment Template to add to the user. Select **Apply Template**.



11. After selecting/applying the appropriate template, the User Assignment Template details will display. Verify that the details of the assignment are accurate (Assignment Name, Phase, Case Types and Assignment Method). It is optional to add multiple assignments to a user by clicking the +Add Assignment button.
12. Once all assignments are added, select **Save** at the bottom right of the User Profile.



ACRONYMS AND DEFINITIONS.

ACCM - alternative compensatory control measures

AEA - Atomic Energy Act of 1954, as amended

AUS - Australia

CAGE - commercial and government entity

CCIPP - classified critical infrastructure protection program

CDC - cleared defense contractor

CFIUS - Committee on Foreign Investment in the United States

CFR - Code of Federal Regulations

CI - Counterintelligence

CIA - Central Intelligence Agency

CNSS - Committee on National Security Systems

CNWDI - critical nuclear weapons design information

COMSEC - communications security

COR - central office of record

CSA - cognizant security agency

CSO - cognizant security office

CUSR - Central United States Registry

DCSA - Defense Counterintelligence and Security Agency

DD - Department of Defense (forms only)

DDTC - Directorate of Defense Trade Controls

DGR - designated government representative

DHS - Department of Homeland Security

DNI - Director of National Intelligence

DoD - Department of Defense

DoDD - Department of Defense Directive

DoDI - Department of Defense Instruction

DoDM - Department of Defense Manual

DOE - Department of Energy

ECP - electronic communications plan

E.O. - Executive order

FBI - Federal Bureau of Investigation

FCL - facility (security) clearance

FGI - foreign government information

FOCI - foreign ownership, control, or influence

FRD - Formerly Restricted Data

FSCC - Facility Security Clearance Certificate (NATO)

FSO - facility security officer

GCA - government contracting activity

GCMS - government contractor monitoring station

GSA - General Services Administration

GSC - government security committee

IDE - intrusion detection equipment

IDS - intrusion detection system

IFB - invitation for bid

ISOO - Information Security Oversight Office

ISSM - information system security manager

ISSO - information systems security officer

ITAR - International Traffic in Arms Regulations

ITPSO - insider threat program senior official

KMP - key management personnel

LAA - limited access authorization

MFO - multiple facility organization

NATO - North Atlantic Treaty Organization

NDA - nondisclosure agreement

NIAG - NATO Industrial Advisory Group

NID - national interest determination

NISP - National Industrial Security Program

NISPOM - National Industrial Security Program Operating Manual

NIST - National Institute for Standards and Technology

NNPI - Naval Nuclear Propulsion Information

NNSA - National Nuclear Security Administration

NPLO - NATO Production Logistics Organization

NRC - Nuclear Regulatory Commission

NRTL - nationally recognized testing laboratory

NSA - National Security Agency

NSI - national security information

NTIB - National Technology and Industrial Base

OCA - original classification authority

OMB - Office of Management and Budget

OPM – Office of Personnel Management

PA - proxy agreement

PCL - personnel (security) clearance

RD - Restricted Data

RFP - request for proposal

RFQ - request for quotation

SAP - special access program

SCA - security control agreement

SCI - sensitive compartmented information

SD - Secretary of Defense (forms only)

SEAD - Security Executive Agent directive

SF - standard form

SMO – Security Management Office

SMO - senior management official

SSA - special security agreement

SSP - systems security plan

TCP - technology control plan

TFNI - Transclassified Foreign Nuclear Information

TP - transportation plan

UK - United Kingdom

UL - Underwriters' Laboratories

U.S.C. - United States Code

USD (I&S) - Under Secretary of Defense for Intelligence and Security

USG - United States Government

USML - United States Munitions List

VAL - visit authorization letter

VT - voting trust

Access means the ability and opportunity to gain knowledge of classified information.

Access Permittee means the holder of an Access Permit issued pursuant to the regulations set forth in 10 CFR part 725, “Permits For Access to Restricted Data.”

ACCM are security measures used by USG agencies to safeguard classified intelligence or operations when normal measures are insufficient to achieve strict need-to-know controls and where SAP controls are not required.

Adverse information means any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes an insider threat.

Affiliate means each entity that directly or indirectly controls, is directly or indirectly controlled by, or is under common control with, the ultimate parent entity.

Agency[ies] means any “Executive agency” as defined in 5 U.S.C. 105; any “Military department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that releases classified information to private sector entities. This includes component agencies under another agency or under a cross-agency oversight office (such as ODNI with CIA), which are also agencies for purposes of this rule.

Alarm service company means an entity or branch office from which all of the installation, service, and maintenance of alarm systems are provided, and the monitoring and investigation of such systems are either provided by its own personnel or with personnel assigned by this location.

Alarm system description form means a form describing an alarm system and monitoring information.

Approved security container means a GSA approved security container originally procured through the Federal Supply system. The security containers bear the GSA Approval label on the front face of the container, which identifies them as meeting the testing requirements of the assigned federal specification and having been maintained according to Federal Standard 809.

Approved vault means a vault built to Federal Standard 832 and approved by the CSA.

AUS community consists of the Government of Australia entities and Australian non-governmental facilities identified on the DDTC website (https://pmddtc.state.gov/) at the time of export or transfer.

Authorized person means a person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know.

Branch office means an office of an entity which is located somewhere other than the entity's main office location. A branch office is simply another location of the same legal business entity and is still involved in the business activities of the entity.

CCIPP means security sharing of classified information under a designated critical infrastructure protection program with such authorized individuals and organizations as determined by the Secretary of Homeland Security.

CDC means a subset of contractors cleared under the NISP who have classified contracts with the DoD.

Certification means comprehensive evaluation of an information system component that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

Classification guide means a document issued by an authorized original classifier that identifies the elements of information regarding a specific subject that must be classified and prescribes the level and duration of classification and appropriate declassification instructions.

Classified contract means any contract, license, agreement, or grant requiring access to classified information by a contractor and its employees for performance. A contract is referred to in this rule as a “classified contract” even when the contract document and the contract provisions are not classified. The requirements prescribed for a “classified contract” also are applicable to all phases of precontract, license or grant activity, including solicitations (bids, quotations, and proposals), precontract negotiations, post-contract activity, or other government contracting activity (GCA) programs or projects which require access to classified information by a contractor.

Classified covered information system means an information system that is owned or operated by or for a cleared defense contractor and that processes, stores, or transmits information created by or for the DoD with respect to which such contractor is required to apply enhanced protection (e.g., classified information). A classified covered information system is a type of covered network consistent with the requirements of Section 941 of Public Law 112-239 and 10 U.S.C. 391.

Classified information means information that has been determined, pursuant to E.O. 13526, or any predecessor or successor order, and the AEA of 1954, as amended, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. The term includes NSI, RD, and FRD.

Classified meetings mean a conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified information is disclosed.

Classified visit means a visit during which a visitor will require, or is expected to require, access to classified information.

Classifier means any person who makes a classification determination and applies a classification category to information or material. The determination may be an original classification action or it may be a derivative classification action. Contractors make derivative classification determinations based on classified source material, a security classification guide, or a contract security classification specification, or equivalent.

Cleared commercial carrier means a carrier that is authorized by law, regulatory body, or regulation to transport SECRET and CONFIDENTIAL material and has been granted a SECRET facility clearance in accordance with the NISP.

Cleared employees means all employees of industrial or commercial contractors, licensees, certificate holders, or grantees of an agency, as well as all employees of subcontractors and personal services contractor personnel, and who are granted favorable eligibility determinations for access to classified information by a CSA or are being processed for eligibility determinations for access to classified information by a CSA. A contractor may give an employee access to classified information in accordance with the provisions of § 117.10(a)(1)(iii).

Closed area means an area that meets the requirements of this rule for safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

CNWDI means a DoD category of TOP SECRET RD or SECRET RD information that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fusion-able, and high explosive materials by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test or replace.

Compromise means an unauthorized disclosure of classified information.

COMSEC means the protective measures taken to deny unauthorized persons information derived from USG telecommunications relating to national security and to ensure the authenticity of such communications.

CONFIDENTIAL means the classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority (OCA) is able to identify or describe.

Consignee means a person, firm, or Government (i.e., USG or foreign government) activity named as the receiver of a shipment; one to whom a shipment is consigned.

Consignor means a person, firm, or Government (i.e., USG or foreign government) activity by which articles are shipped. The consignor is usually the shipper.

Constant surveillance service means a transportation protective service provided by a commercial carrier qualified by the Surface Deployment and Distribution Command to transport CONFIDENTIAL shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative; however, an FCL is not required for the carrier. The carrier providing the service must maintain a signature and tally record for the shipment.

Consultant means an individual under contract, and compensated directly, to provide professional or technical assistance to a contractor in a capacity requiring access to classified information.

Continuous evaluation as defined in SEAD 6 is a personnel security investigative process to review the background of a covered individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. Continuous evaluation leverages a set of automated records checks and business rules, to assist in the ongoing assessment of an individual's continued eligibility. It supplements, but does not replace, the established personnel security program for scheduled periodic reinvestigations of individuals for continuing eligibility.

Continuous monitoring program means a system that facilitates ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.

Contracting officer means a USG official who, in accordance with departmental or agency procedures, has the authority to enter into and administer contracts, licenses or grants and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his or her authority.

Contractor means any industrial, educational, commercial, or other entity that has been granted an entity eligibility determination by a CSA. This term also includes licensees, grantees, or certificate holders of the USG with an entity eligibility determination granted by a CSA. As used in this rule, “contractor” does not refer to contractor employees or other personnel.

Cooperative agreement means a legal instrument which, consistent with 31 U.S.C. 6305, is used to enter into the same kind of relationship as a grant (see definition of "grant" in this subpart), except that substantial involvement is expected between USG and the recipient when carrying out the activity contemplated by the cooperative agreement. The term does not include "cooperative research and development agreements" as defined in 15 U.S.C. 3710a.

Cooperative research and development agreement means any agreement between one or more Federal laboratories and one or more non-Federal parties under which the Government, through its laboratories, provides personnel, services, facilities, equipment, intellectual property, or other resources with or without reimbursement (but not funds to non-Federal parties) and the non-Federal parties provide funds, personnel, services, facilities, equipment, intellectual property, or other resources toward the conduct of specified research or development efforts which are consistent with the missions of the laboratory; except that such term does not include a procurement contract or cooperative agreement as those terms are used in sections 6303, 6304, and 6305 of title 31.

Corporate family means an entity, its parents, subsidiaries, divisions, and branch offices.

Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.

Courier means a cleared employee, designated by the contractor, whose principal duty is to transmit classified material to its destination, ensuring that the classified material remains under their constant and continuous protection and that they make direct point-to-point delivery.

CRYPTO means the marking or designator that identifies unencrypted COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive USG or USG-derived information. This includes non-split keying material used to encrypt or decrypt COMSEC critical software and software-based algorithms.

CSA means an agency designated as having NISP implementation and security responsibilities for its own agencies (including component agencies) and any entities and non-CSA agencies under its cognizance. The CSAs are: DoD; DOE; NRC; ODNI; and DHS.

CSO means an organizational unit to which the head of a CSA delegates authority to administer industrial security services on behalf of the CSA.

CUI means information the USG creates or possesses, or that an entity creates or possesses for or on behalf of the USG, that a law, regulation, or USG-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

Custodian means an individual who has possession of, or is otherwise charged with, the responsibility for safeguarding classified information.

Cybersecurity means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cyber incident means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

Declassification means a date or event which coincides with the lapse of the information's national security sensitivity, as determined by the OCA. Declassification occurs when the OCA has determined that the classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, and the information has had its classification designation removed or cancelled.

Defense articles means those articles, services, and related technical data, including software, in tangible or intangible form, which are listed on the United States Munitions List (USML) of the International Traffic in Arms Regulations (ITAR), as modified or amended. Defense articles exempt from the scope of ITAR section 126.17 are identified in Supplement No. 1 to Part 126 of the ITAR.

Defense services means:

(1) Furnishing assistance (including training) to foreign persons, whether in the United States or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles;

(2) Furnishing to foreign persons any controlled technical data, whether in the United States or abroad; or

(3) Providing military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

Derivative classification means the incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes classifying information based on classification guidance. Duplicating or reproducing existing classified information is not derivative classification.

Document means any recorded information, regardless of the nature of the medium, or the method or circumstances of recording.

Downgrade means a determination by a declassification authority that information classified and safeguarded at a specified level will be classified and safeguarded at a lower level.

Embedded system means an information system that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem, such as, ground support equipment, flight simulators, engine test stands, or fire control systems.

Empowered official is defined in 22 CFR part 120.

Entity is a generic and comprehensive term which may include sole proprietorships, partnerships, corporations, limited liability companies, societies, associations, institutions, contractors, licensees, grantees, certificate holders, and other organizations usually established and operating to carry out a commercial, industrial, educational, or other legitimate business, enterprise, or undertaking, or parts of these organizations. It may reference an entire organization, a prime contractor, parent organization, a branch or division, another type of sub-element, a sub-contractor, subsidiary, or other subordinate or connected entity (referred to as "sub-entities" when necessary to distinguish such entities from prime or parent entities). It may also reference a specific location or facility, or the headquarters or official business location of the organization, depending upon the organization's business structure, the access needs involved, and the responsible CSA's procedures. The term "entity" as used in this rule refers to the particular entity to which an agency might release, or is releasing, classified information, whether that entity is a parent or subordinate organization. The term "entity" in this rule includes contractors.

Entity eligibility determination means an assessment by the CSA as to whether an entity is eligible for access to classified information of a certain level (and all lower levels). Entity eligibility determinations may be broad or limited to specific contracts, sponsoring agencies, or circumstances. A favorable entity eligibility determination results in eligibility to access classified information under the cognizance of the responsible CSA to the level approved. When the entity would be accessing categories of information such as RD or SCI for which the CSA for that information has set additional requirements, CSAs must also assess whether the entity is eligible for access to that category of information. Some CSAs refer to their favorable entity eligibility determinations as FCLs. However, a favorable entity eligibility determination for the DHS CCIPP is not equivalent to an FCL and does not meet the requirements for FCL reciprocity. A favorable entity eligibility determination does not convey authority to store classified information.

Escort means a cleared person, designated by the contractor, who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort.

Extent of protection means the designation (such as "Complete") used to describe the degree of alarm protection installed in an alarmed area.

Facility means a plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity.

FCL means an administrative determination that, from a security viewpoint, an entity is eligible for access to classified information of a certain level (and all lower levels) (e.g., a type of favorable entity eligibility determination used by some CSAs). An entity eligibility determination for the DHS CCIPP is not the equivalent of an FCL and does not meet the requirements for FCL reciprocity.

FGI means information that is:

(1) Provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) Produced by the United States pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

Foreign interest means any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its territories, and any person who is not a citizen or national of the United States.

Foreign national means any person who is not a citizen or national of the United States.

Foreign person is defined in 31 CFR 800.224 for CFIUS purposes.

FRD means classified information removed from the Restricted Data category upon a joint determination by the DOE and DoD that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information.

Freight forwarder (transportation agent) means any agent or facility designated to receive, process, and transship U.S. material to foreign recipients. In the context of this rule, it means an agent or facility cleared specifically to perform these functions for the transfer of U.S. classified material to foreign recipients.

GCA means an element of an agency that the agency head has designated and delegated broad authority regarding acquisition functions. A foreign government may also be a GCA.

Governing board means an entity's board of directors, board of managers, board of trustees, or equivalent governing body.

Grant means a legal instrument which, consistent with 31 U.S.C. 6304, is used to enter into a relationship: (a) Of which the principal purpose is to transfer a thing of value to the recipient to carry out a public purpose of support or stimulation authorized by a law of the United States, rather than to acquire property or services for the USG's direct benefit or use; or, (b) In which substantial involvement is not expected between DoD and the recipient when carrying out the activity contemplated by the award. Throughout this rule, the term grant will include both the grant and cooperative agreement.

Grantee means the entity that receives a grant or cooperative agreement.

Hand carrier means a cleared employee, designated by the contractor, who occasionally hand carries classified material to its destination in connection with a classified visit or meeting. The classified material remains in the personal possession of the hand carrier except for authorized overnight storage.

Home office means the headquarters of a multiple facility entity.

Industrial security means that portion of information security concerned with the protection of classified information in the custody of U.S. industry.

Information means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information security means the system of policies, procedures, and requirements established pursuant to executive order, statute, or regulation to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public.

Information system means an assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.

Insider means cleared contractor personnel with authorized access to any USG or contractor resource, including personnel, facilities, information, equipment, networks, and systems.

Insider threat means the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified NSI.

Joint venture means an association of two or more persons or entities engaged in a single defined project with all parties contributing assets and efforts, and sharing in the management, profits and losses, in accordance with the terms of an agreement among the parties.

KMP means an entity's senior management official (SMO), facility security officer (FSO), insider threat program senior official (ITPSO), and all other entity officials who either hold majority interest or stock in or have direct or indirect authority to influence or decide issues affecting the management or operations of, the entity or classified contract performance.

L access authorization means an access determination that is granted by DOE or NRC based on a Tier 3 or successor background investigation as set forth in applicable national-level requirements and DOE directives. Within DOE and NRC, an "L" access authorization permits an individual who has an official "need to know" to access Confidential Restricted Data, Secret and Confidential Formerly Restricted Data, Secret and Confidential Transclassified Foreign Nuclear Information, or Secret and Confidential National Security Information, required in the performance of official duties. An "L" access authorization determination is required for individuals with a need to know outside of DOE, NRC, DoD, and in limited cases NASA, to access Confidential Restricted Data.

LAA means security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring only limited access in the course of their regular duties.

Material means any product or substance on or in which information is embodied.

Matter means anything in physical form that contains or reveals classified information.

Media means physical devices or writing surfaces including but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

MFO means a legal entity (single proprietorship, partnership, association, trust, or corporation) composed of two or more entities (facilities).

National of the United States means a person who owes permanent allegiance to the United States. All U.S. citizens are U.S. nationals; however, not all U.S. nationals are U.S. citizens (for example, persons born in American Samoa or Swains Island).

NATO information means information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless NATO authority has been obtained to release outside of NATO.

NATO visits means visits by personnel representing a NATO entity and relating to NATO contracts and programs.

Need-to-know means a determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.

Network means a system of two or more information systems that can exchange data or information.

NNPI is classified or unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities.

Non-DoD executive branch agencies means the non-DoD agencies that have entered into agreements with DoD to receive NISP industrial security services from DoD. A list of these agencies is on the Defense Counterintelligence and Security Agency website at https://www.dcsa.mil.

Non-Federal information system is defined in 32 CFR part 2002.

NRTL means a private sector organization recognized by the Occupational Safety and Health Administration to perform certification for certain products to ensure that they meet the requirements of both the construction and general industry Occupational Safety and Health Administration electrical standards. Each NRTL is recognized for a specific scope of test standards.

NSI means information that has been determined pursuant to E.O. 13526 or predecessor order to require protection against unauthorized disclosure and marked to indicate its classified status.

NTIB means the industrial bases of the United States and Australia, Canada, and the United Kingdom.

NTIB entity means a person that is a subsidiary located in the United States for which the ultimate parent entity and any intermediate parent entities of such subsidiary are located in a country that is part of the national technology and industrial base (as defined in section 2500 of title 10, United States Code); and that is subject to the foreign ownership, control, or influence requirements of the National Industrial Security Program.

Nuclear weapon data means Restricted Data or Formerly Restricted Data concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance and effects) of nuclear explosives, nuclear weapons or nuclear weapon components, including information incorporated in or related to nuclear explosive devices. Nuclear weapon data is matter in any combination of documents or material, regardless of physical form or characteristics.

OCA means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

Original classification means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Only USG officials who have been designated in writing may apply an original classification to information.

Parent means an entity that owns at least a majority of another entity's voting securities.

PCL means an administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

Prime contract means a contract awarded by a GCA to a contractor for a legitimate USG purpose.

Prime contractor means the contractor who receives a prime contract from a GCA.

Privileged user means a user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Proscribed information means:

(1) TOP SECRET information;

(2) COMSEC information or material, excluding controlled cryptographic items when unkeyed or utilized with unclassified keys.

(3) RD;

(4) SAP information; or.

(5) SCI.

Protective security service means a transportation protective service provided by a cleared commercial carrier qualified by DoD's Surface Deployment and Distribution Command to transport SECRET shipments.

Q access authorization means an access determination that is granted by DOE or NRC based on a Tier 5 or successor background investigation as set forth in applicable national-level requirements and DOE directives. Within DOE and the NRC, a "Q" access authorization permits an individual with an official "need to know" to access Top Secret, Secret and Confidential Restricted Data, Formerly Restricted Data, Transclassified Foreign Nuclear Information, National

Security Information, or special nuclear material in Category I or II quantities, as required in the performance of official duties. A “Q” access authorization is required for individuals with a need to know outside of DOE, NRC, DoD, and in a limited case NASA, to access Top Secret and Secret Restricted Data.

Remote terminal means a device communicating with an automated information system from a location that is not within the central computer facility.

Restricted area means a controlled access area established to safeguard classified material that, because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

RD means all data concerning

(1) design, manufacture, or utilization of atomic weapons;

(2) the production of special nuclear material; or

(3) the use of special nuclear material in the production of energy, but does not include data declassified or removed from the RD category pursuant to section 142 of the AEA.

SAP means any program that is established to control access and distribution and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A SAP can be created or continued only as authorized by a senior agency official delegated such authority pursuant to E.O. 13526.

Schedule 13D means a form required by the Securities and Exchange Commission when a person or group of persons acquires beneficial ownership of more than 5% of a voting class of a company's equity securities registered under Section 12 of the “Securities Exchange Act of 1934” (available at: https://www.sec.gov/fast-answers/answerssched13htm.html).

SCI means a subset of classified national intelligence concerning or derived from intelligence sources, methods or analytical processes that is required to be protected within formal access control systems established by the DNI.

SECRET means the classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe.

Security in depth means a determination made by the CSA that a contractor's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring, or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

Security violation means failure to comply with the policy and procedures established by this part that reasonably could result in the loss or compromise of classified information.

Shipper means one who releases custody of material to a carrier for transportation to a consignee. (See also “Consignor.”)

SMO is the contractor's official responsible for the entity policy and strategy. The SMO is an entity employee occupying a position in the entity with ultimate authority over the facility's operations and the authority to direct actions necessary for the safeguarding of classified information in the facility. This includes the authority to direct actions necessary to safeguard classified information when the access to classified information by the facility's employees is solely at other contractor facilities or USG locations.

Source document means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Standard practice procedures mean a document prepared by a contractor that implements the applicable requirements of this rule for the contractor's operations and involvement with classified information at the contractor's facility.

Subcontract means any contract entered into by a contractor to furnish supplies or services for performance of a prime contract or a subcontract. It includes a contract, subcontract, purchase order, lease agreement, service agreement, request for quotation (RFQ), request for proposal (RFP), invitation for bid (IFB), or other agreement or procurement action between contractors that requires or will require access to classified information to fulfill the performance requirements of a prime contract.

Subcontractor means a supplier, distributor, vendor, or firm that enters into a contract with a prime contractor to furnish supplies or services to or for the prime contractor or another subcontractor. For the purposes of this rule, each subcontractor will be considered as a prime contractor in relation to its subcontractors.

Subsidiary means an entity in which another entity owns at least a majority of its voting securities.

System software means computer programs that control, monitor, or facilitate use of the information system; for example, operating systems, programming languages, communication, input-output controls, sorts, security packages, and other utility-type programs. Also includes off-the-shelf application packages obtained from manufacturers and commercial vendors, such as for word processing, spreadsheets, data base management, graphics, and computer-aided design.

Technical data means:

(1) Information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.

(2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List.

(3) Information covered by an invention secrecy order.

(4) Software directly related to defense articles.

TFNI means classified information concerning the nuclear energy programs of other nations (including subnational entities) removed from the RD category under section 142(e) of the AEA after the DOE and the Director of National Intelligence jointly determine that it is necessary to carry out intelligence-related activities under the provisions of the National Security Act of 1947, as amended, and that it can be adequately safeguarded as NSI instead. This includes information removed from the RD category by past joint determinations between DOE and the CIA. TFNI does not include information transferred to the United States under an Agreement for Cooperation under the Atomic Energy Act or any other agreement or treaty in which the United States agrees to protect classified information.

TOP SECRET means the classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.

Transmission means sending information from one place to another by radio, microwave, laser, or other non-connective methods, as well as by cable, wire, or another connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

Transshipping activity means a government activity to which a carrier transfers custody of freight for reshipment by another carrier to the consignee.

UK community consists of the UK Government entities with facilities and UK non-governmental facilities identified on the DDTC website (https://www.pmddtc.state.gov/) at the time of export.

Unauthorized person means a person not authorized to have access to specific classified information in accordance with the requirements of this rule.

United States means the 50 states and the District of Columbia.

United States and its territorial areas mean the 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, Wake Island, Johnston Atoll, Kingman Reef, Palmyra Atoll, Baker Island, Howland Island, Jarvis Island, Midway Islands, Navassa Island, and Northern Mariana Islands.

Upgrade means a determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a change to the classification designation to reflect the higher degree.

U.S. classified cryptographic information means a cryptographic key and authenticators that are classified and are designated as TOP SECRET CRYPTO or SECRET CRYPTO. This means all cryptographic media that embody, describe, or implement classified cryptographic logic, to include, but not limited to, full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic software, firmware, or repositories of such software such as magnetic media or optical disks.

U.S. person means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

Voting securities means any securities that presently entitle the owner or holder thereof to vote for the election of directors of the issuer or, with respect to unincorporated entities, individuals exercising similar functions.

Working hours means the period of time when:

(1) There is present in the specific area where classified material is located, a work force on a regularly scheduled shift, as contrasted with employees working within an area on an overtime basis outside of the scheduled work shift; and

(2) The number of employees in the scheduled work force is sufficient in number and so positioned to be able to detect and challenge the presence of unauthorized personnel. This would, therefore, exclude janitors, maintenance personnel, and other individuals whose duties require movement throughout the facility.

Working papers means documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention.