DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

JOB AID

NBIS CONSOLIDATED JOB AIDS

Volume 1 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

BASIC NAVIGATION

HOW TO ACCESS THE NBIS SYSTEM

There are two steps to access NBIS for first time users. The first is Certificate Enrollment, which occurs once access to the NBIS system has been granted. The second is logging into the NBIS Enterprise Portal.

COMPLETE CERTIFICATE ENROLLMENT

Enrolling your certificate is the first step to accessing the NBIS Agency IM application. When your Organization Manager creates your NBIS Agency IM user account, you will receive an email with Welcome to NBIS IdAM Certificate Enrollment Program information. Enrolling your certificate is a one-time action required for each Owning Organization. If you have already enrolled the organization certificate, navigate to "Accessing the NBIS Enterprise Portal" below to access the NBIS Agency IM application.

1. From the Welcome to NBIS IdAM Certificate Enrollment Program email, select the link **Click here to begin Certificate Enrollment**.
2. After reading the Terms of Service, select **I Accept** to agree to the service terms.
3. Enter your Persona ID and Enrollment Key and select **Begin Enrollment**. Persona ID and Enrollment Key should have been received in two separate emails. Contact your supervisor for additional support.
4. Choose **Select Certificate** to be validated. Note: Ensure the certificate being selected is for ID or Authentication Purposes. Other certificates will not work.
5. A Certificate enrollment processing review is conducted to check for authenticity and validation of the submission.
6. Review the returned certificate information and select **Review Complete**.
7. Next enter your SSN (no dashes) and DOB (YYYY-MM-DD) and select **Submit Enrollment** to complete your certificate enrollment. Note: The SSN and DOB must match the data entered by the User Manager that created your account. If incorrect data is entered here, your certificate will need to be re-enrolled with the correct data.
8. Select **Logout** to complete the Certificate enrollment process.

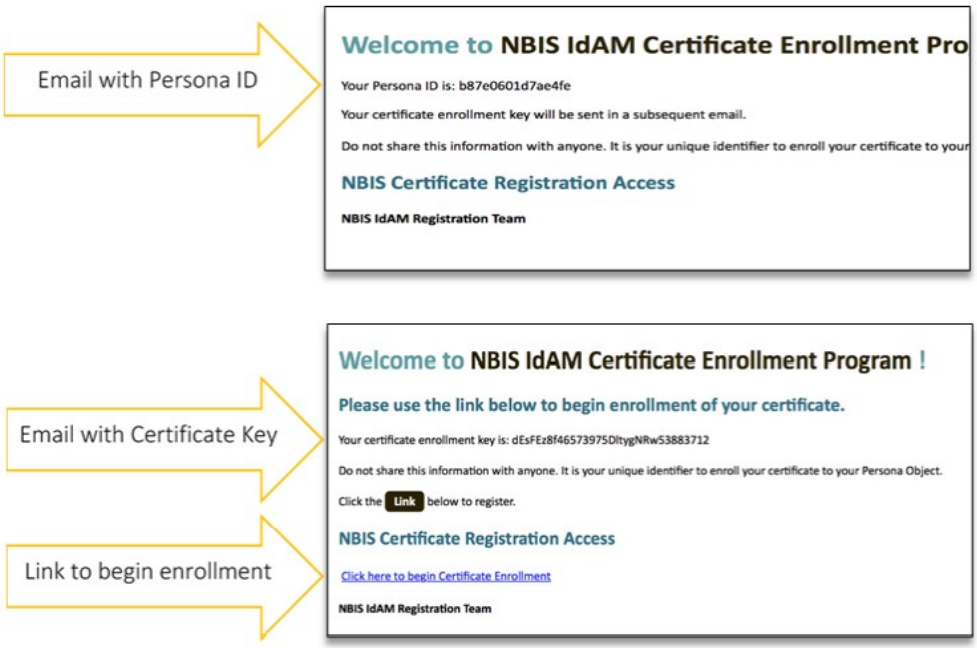
ACCESSING THE NBIS ENTERPRISE PORTAL

Once Certificate Enrollment is complete, you will receive an email confirming your enrollment completion with a link to access the NBIS Enterprise Portal. If you have more than one enrolled Persona you will have an option to choose which enrolled certificate to log into.

1. From the Welcome to NBIS Investigation Management System email, select the link **Click here to access NBIS Enterprise Portal**. Bookmark the link as needed.
2. Review the Terms of Service and select **I Accept**.
3. Choose **Select Certificate**.

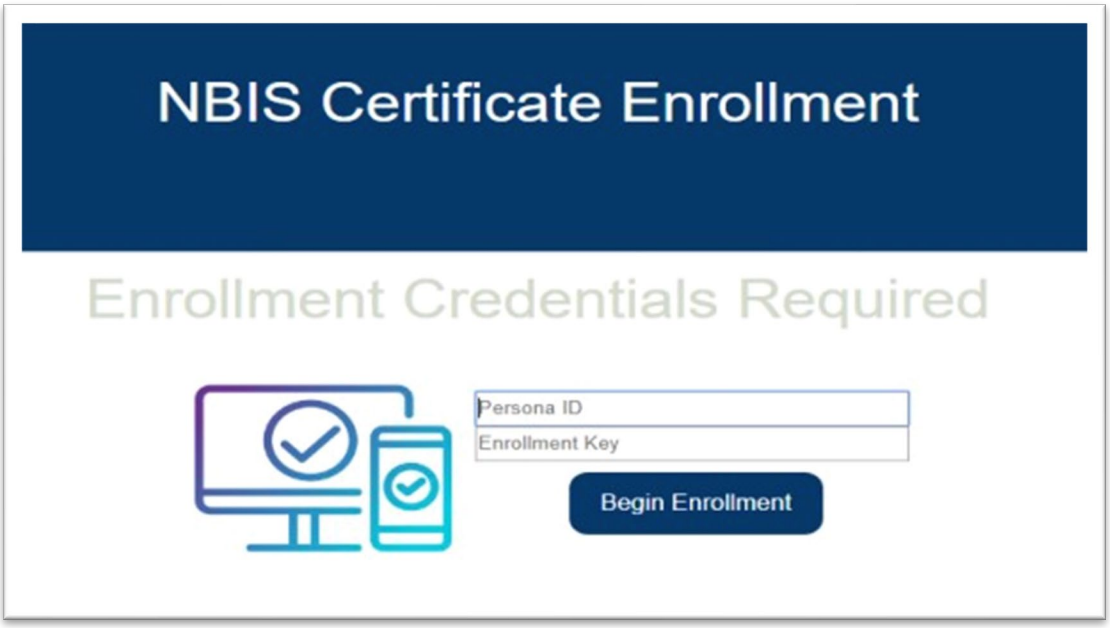
4. Select the certificate from the Choose a certificate to present as identification: drop-down to login to your assigned organization. Note: Certificate selected must match the previous certificate used in the enrollment process.
5. If your certificate is associated to a single Agency user account (Organization) you will be directly logged into the NBIS Enterprise Portal and have access to your assigned organization and role assignment.
    - Note: If you have more than one enrolled Persona you will have an option to choose which enrolled certificate to log into. You are then routed to the assigned Organization(s) to choose the Organization to access within the NBIS Enterprise Portal. If your certificate is associated with more than one Agency user account (different Organization), you will be presented with Organization selections (multiple personas). After selecting an organization, you will be logged into the NBIS Enterprise Portal and have access to the selected organization and role assignment.

Complete Certificate Enrollment (Step 1)

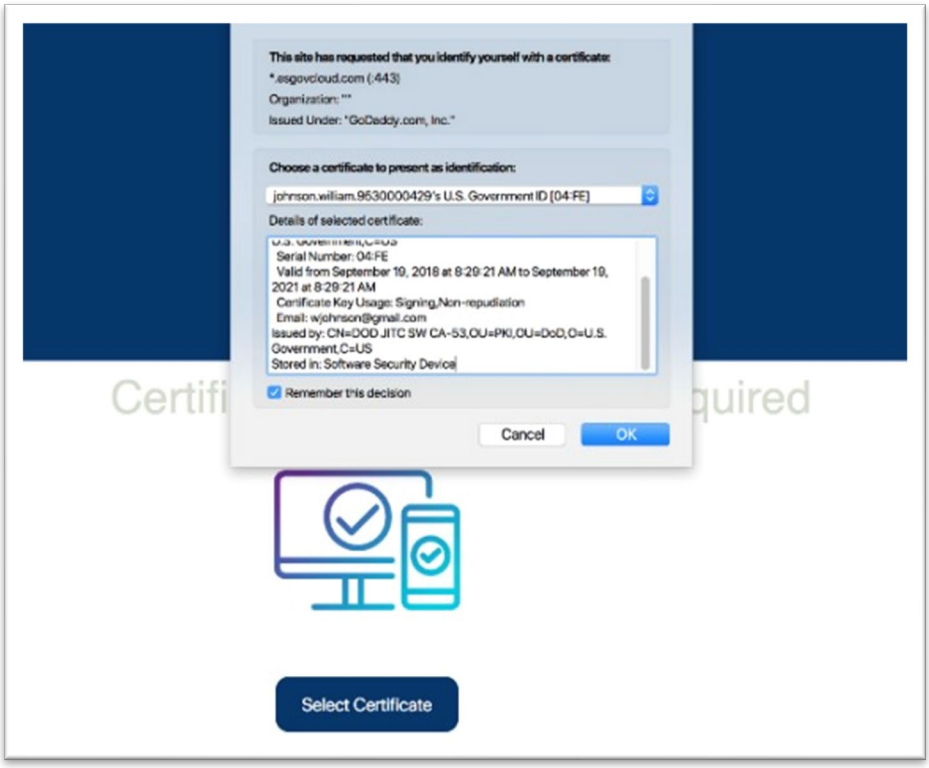


Complete Certificate Enrollment (Step 2)

Complete Certificate Enrollment (Step 3)

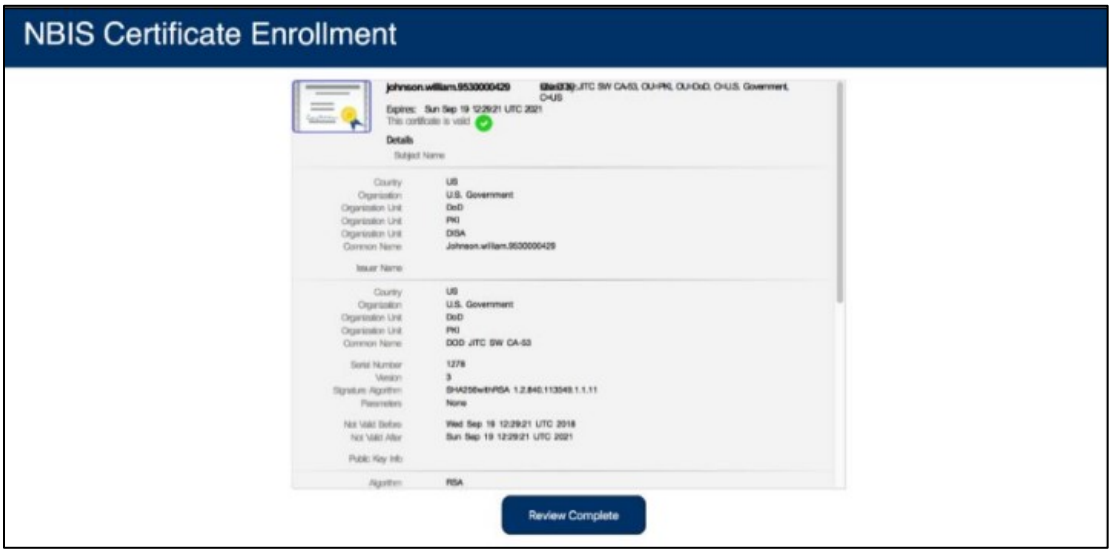


Complete Certificate Enrollment (Step 4)

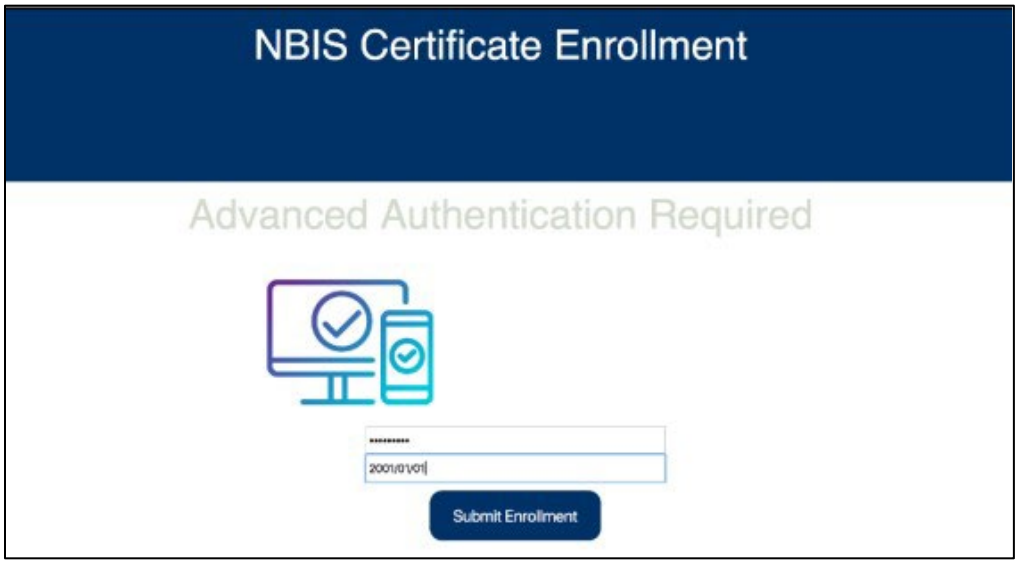


Complete Certificate Enrollment (Step 5)

Complete Certificate Enrollment (Step 6)

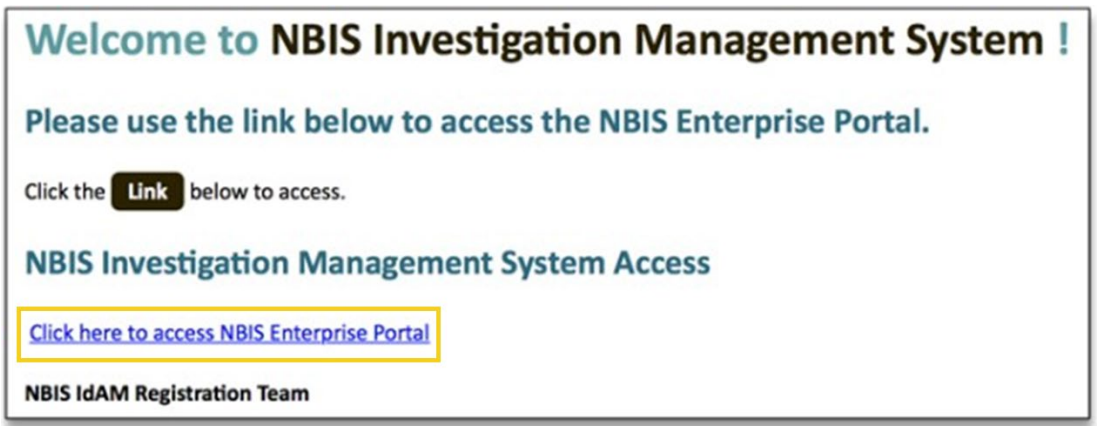


Complete Certificate Enrollment (Step 7)



Complete Certificate Enrollment (Step 8)

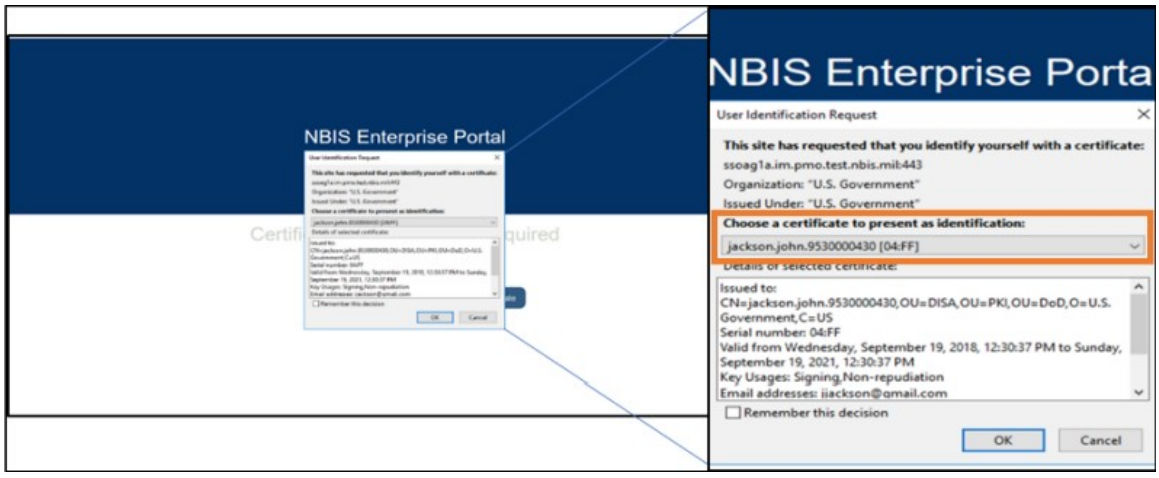
Accessing the NBIS Enterprise Portal (Step 1)



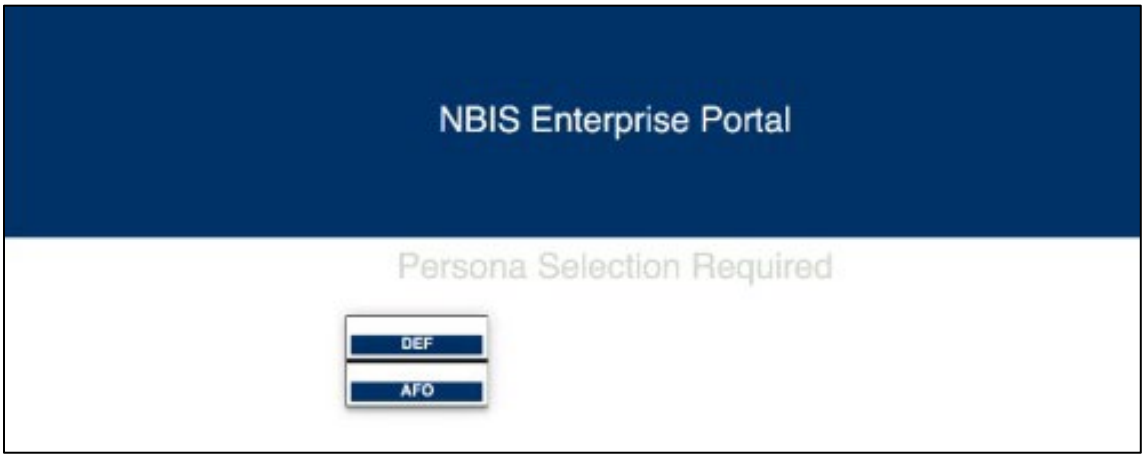
Accessing the NBIS Enterprise Portal (Step 2)

Accessing the NBIS Enterprise Portal (Step 3)

Accessing the NBIS Enterprise Portal (Step 4)



Accessing the NBIS Enterprise Portal (Step 5)

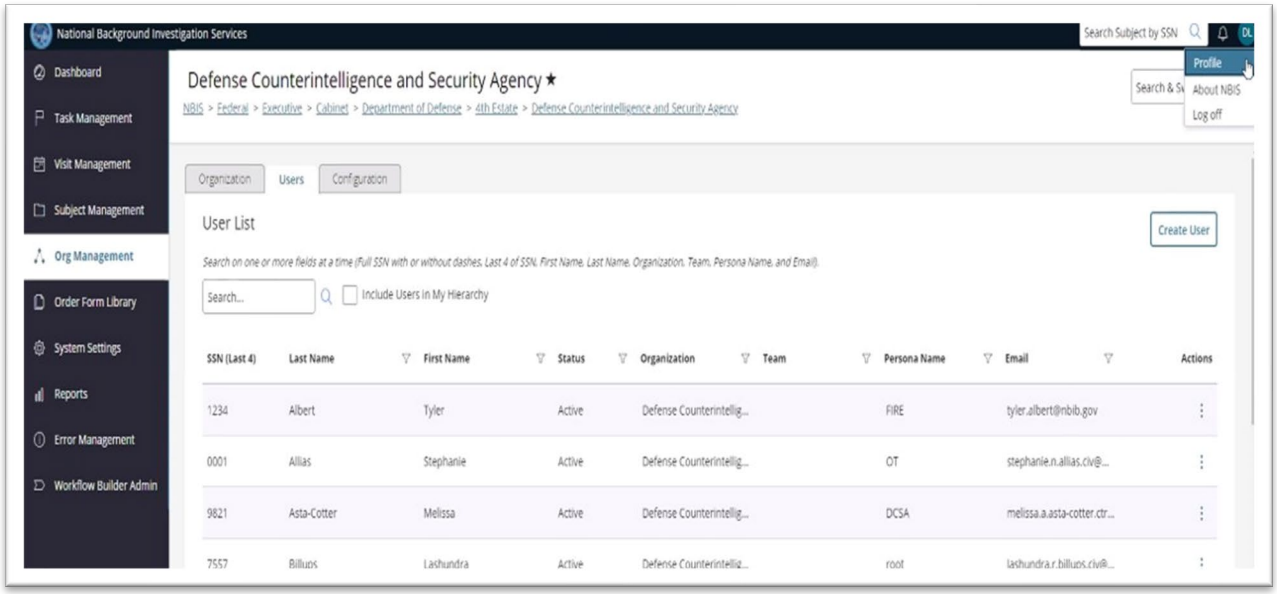


HOW TO ACCESS USER PROFILE

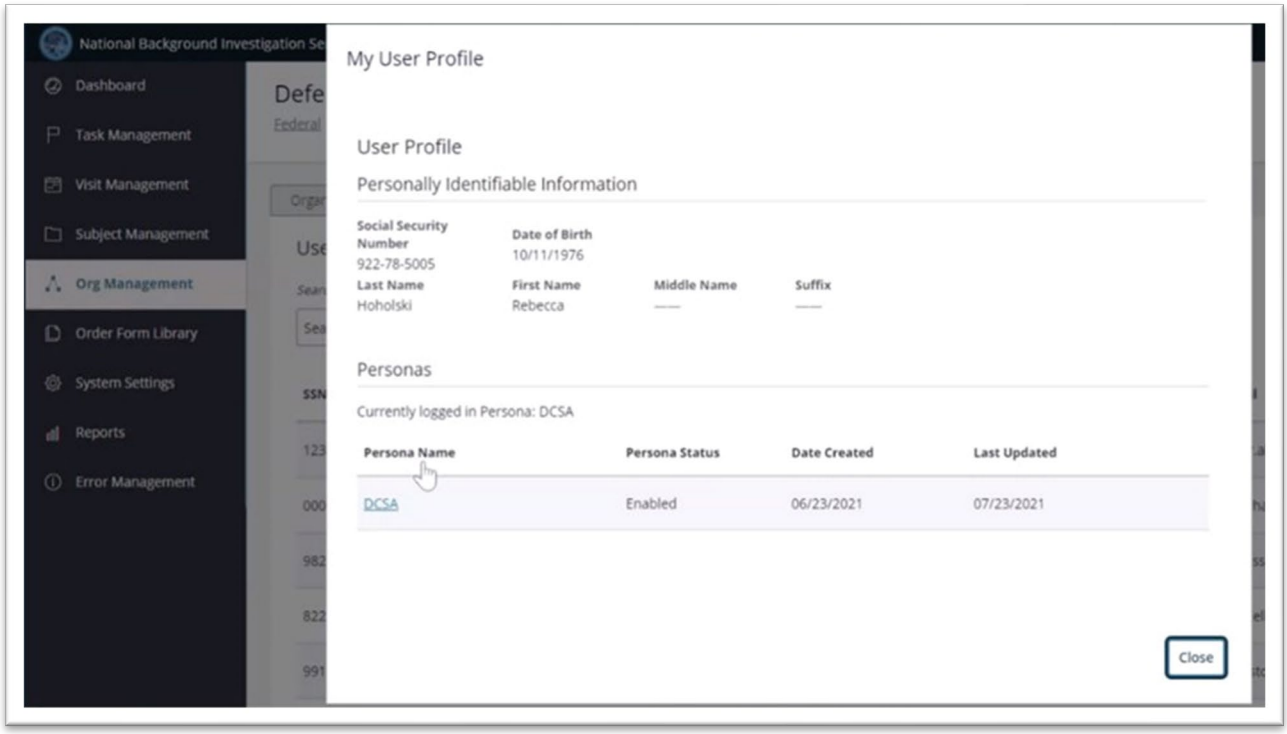
Users have access to view their profile details; however, a user cannot make edits to their own profile. Users with the User Manager role can perform edits to another user's profile including managing persona settings, user assignments, and adding/removing roles within associated orgs. Below is the 3-step process that users can follow to View their Profile details.

1. After initial log in, users can **select their initials** in the upper right-hand portion of the screen.
2. After users select their initials, a drop-down menu will appear displaying "Profile," "About NBIS," and "Log Off." Select **Profile**.
3. After users select Profile, the My User Profile screen will appear displaying the user's Personal Identifiable Information (PII) and the Persona(s) linked to the user's account.

Steps 1-2



Step 3


National Background Investigation Se
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
My User Profile
User Profile
Personally Identifiable Information
Social Security Number
922-78-5005
Date of Birth
10/11/1976
Last Name
Hoholski
First Name
Rebecca
Middle Name
Suffix
Personas
Currently logged in Persona: DCSA
Persona Name
Persona Status
Date Created
Last Updated
DCSA
Enabled
06/23/2021
07/23/2021
Close

HOW TO ACCESS NOTIFICATIONS

Users have access to view a list of their own user notifications. Please note that case related notifications may have the link disabled if the user does not have the correct roles/permissions to view the case. Below is the 3-step process to access user notifications.

1. After initial log in, users can select the **bell notification icon** button in the upper right-hand portion of the screen next to their initials.
2. After users click on the notification icon, a drop-down menu will appear displaying a list of notifications sent to the user.
3. If enabled, **click the link** below the notification to view the associated case request.

HOW TO ACCESS THE USER NAVIGATION MENU

To access the navigation menu, users will either see the black navigation bar or a small icon on their screen that will expand into the navigation menu.

NAVIGATION MENU

The navigation menu is visible to all users in the application, though the content visible in the menu will vary based on a user's screen size and/or browser zoom percent setting. As a result, users may see the hamburger icon (a three-line column) instead of the black navigation bar. The options available to the user within the navigation menu vary based on their assigned roles.

Select a tab on the navigation bar to be able to perform or view the following actions.

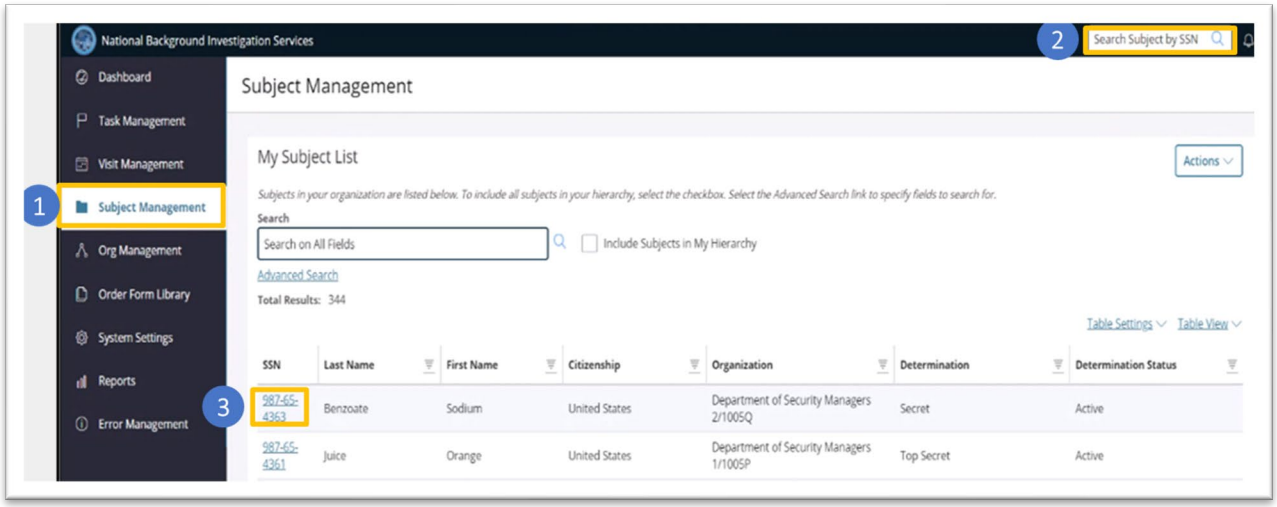
1. **Task Management** is where users can view the work assigned to them and review cases they have worked on previously. You can access the Task Management tab from the navigation menu on the left side of the screen.
2. **Visit Management** allows Subject Managers and FSOs to create visits and invite organizations to attend meetings and events. Visits can be created through the Visit Management tab and from the subject profile. Only Subject Managers and FSOs can create, request, and approve visits. The Subject viewer role can view the visits on the Visit Management tab and on the subject profile.
3. **Subject Management** component of NBIS is designed to help maintain relationships between Subjects and organizations, and then to ultimately use this relationship to manage Subjects' access and visits. Subject Management in NBIS provides one central platform to manage Subjects.
4. **Organization (Org) Management** refers to an organization hierarchy structure and its alignment of user roles throughout its organizational levels. Org Management is the creation and sustainment of an organization's hierarchy to ensure user roles and system accesses are properly aligned and monitored.
5. **Order Form Template**
6. **Reports**
7. **Error Management**

HOW TO UTILIZE GLOBAL SUBJECT SEARCH

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. Initiating a case request requires the user to first search for a Subject using their SSN, which will be covered in further detail in Subject Management. Below is the 3-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.
    - 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. 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. If a Subject exists search results appear in My Subject List. Select the Subject's **SSN hyperlink** to open the Subject's profile.

(Steps 1-3)



MANAGING FORM ROUTING WORKFLOWS

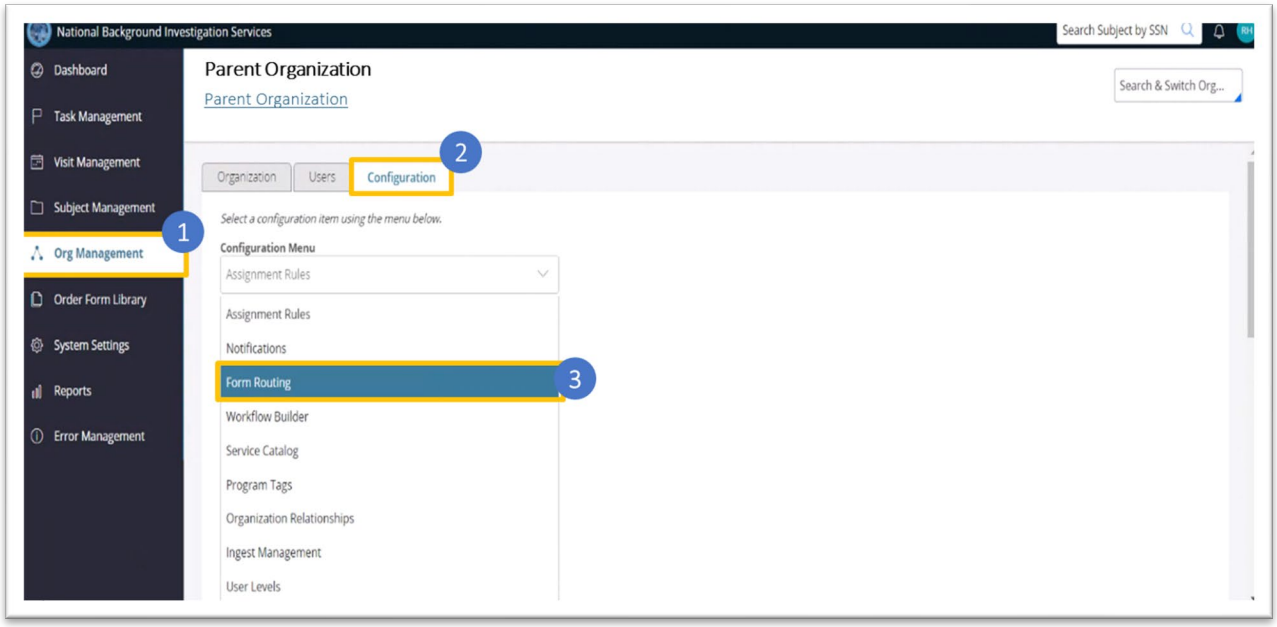
HOW TO ADD A FORM ROUTING WORKFLOW

A Form Routing Workflow consists of a sequence of stages of the investigative process utilized by organizations to allow them to quickly configure and reuse routes for stages within the Initiate, Review and Authorize processes. Users with the Workflow Manager role can add and manage Form Routing Workflows for their Orgs.

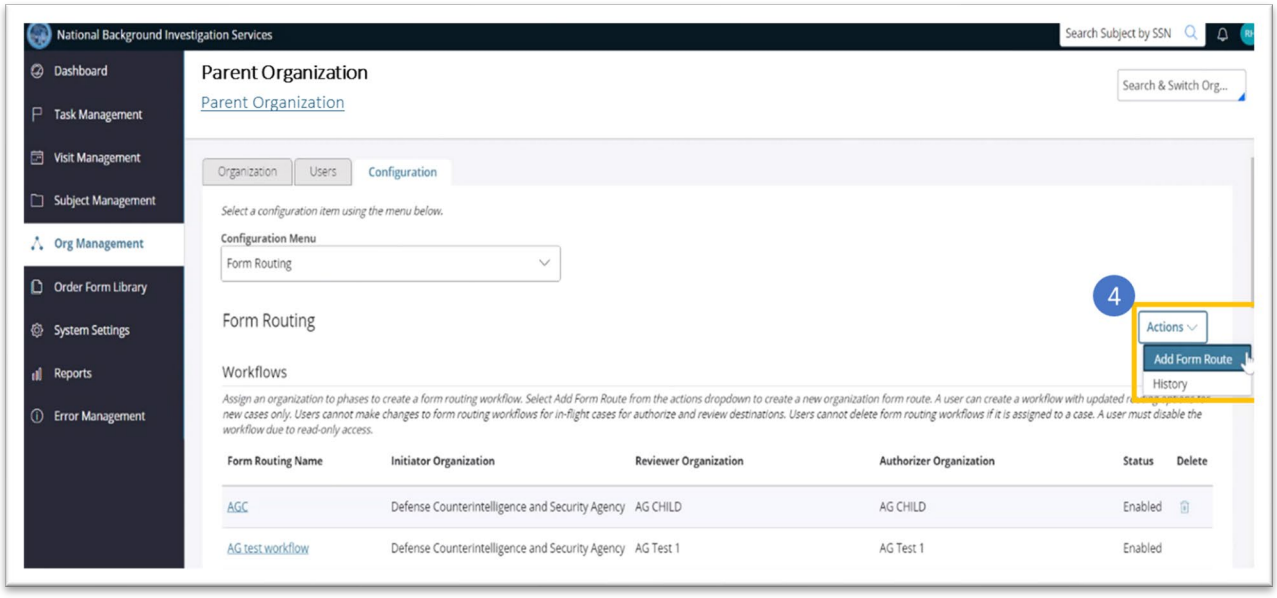
Below is the 8-step process for adding Form Routing Workflows.

1. From initial 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. Click the arrow within the Configuration Menu to reveal the drop-down options and select **Form Routing**.
4. From the Actions drop-down menu on the right, select **Add Form Route**.
5. Complete all required fields starting with entering a Form Routing Name. Note: The designated Org will always be the Initiator.
6. Select a **Reviewer Organization** category and an **Authorizer Organization** category.
    - Users can select Hierarchy to choose their org or another org within their hierarchy to provide Reviewer and Authorizer functionality.
    - Users can select Org Relationship to permit an external Org outside of their Org hierarchy to provide Reviewer and/or Authorizer functionalities. Note that Organizations must have already established an external Organization relationship in order to appear in this selection.
7. Within the fields for Reviewer Organization and Authorizer Organization, start typing in an organization's name to make them Reviewer and/or Authorizer Organizations.
8. Once required fields are completed, select **Submit** to save the new workflow.
    - Note: After saving, the newly created workflow should appear in the list of existing workflows. If the workflow does not appear, locate the workflow in the Form Routing Associations section and select the hyperlink under the Association name column. On the next screen, ensure the status of the workflow is set to Enabled and Save. The workflow should appear in the list of existing workflows.

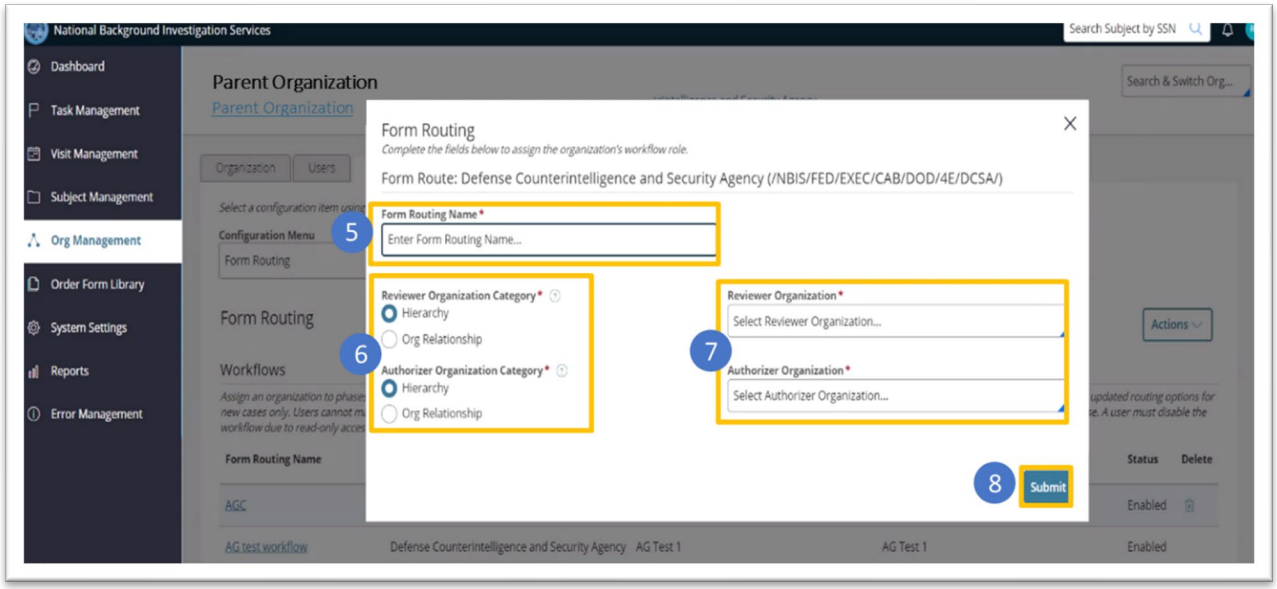
Steps 1-3



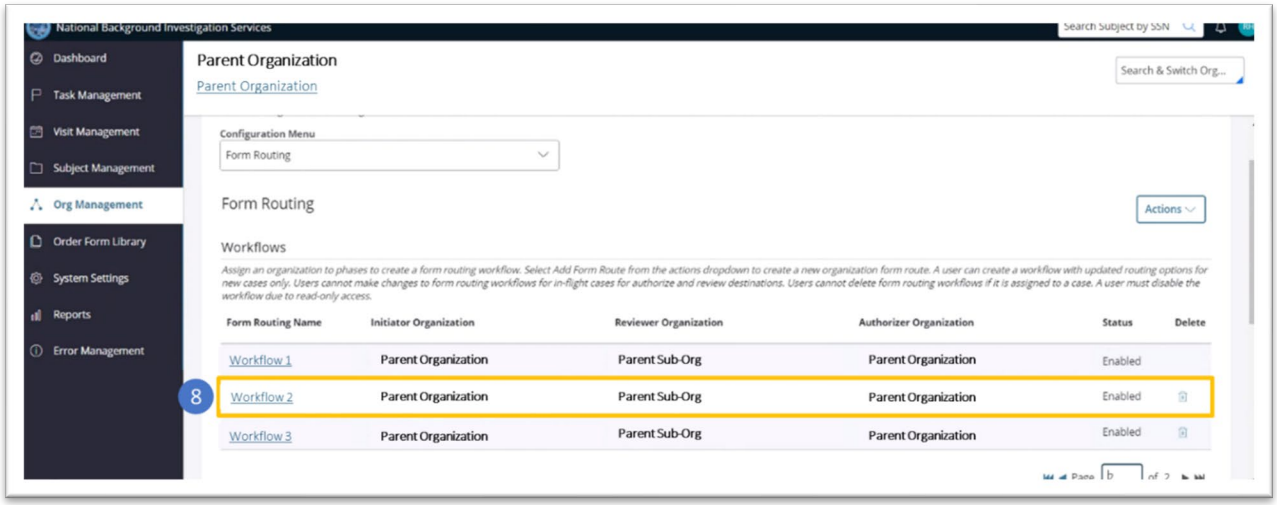
Step 4



Steps 5-8



Step 8 (Continued)



HOW TO MANAGE FORM ROUTING WORKFLOWS

Users with the Workflow Manager role can manage Form Routing Workflows for their Orgs.

VIEW, EDIT, AND ENABLE/DISABLE FORM ROUTING WORKFLOWS

Below is the 6-step process for viewing, editing, enabling, and disabling Form Routing Workflows.

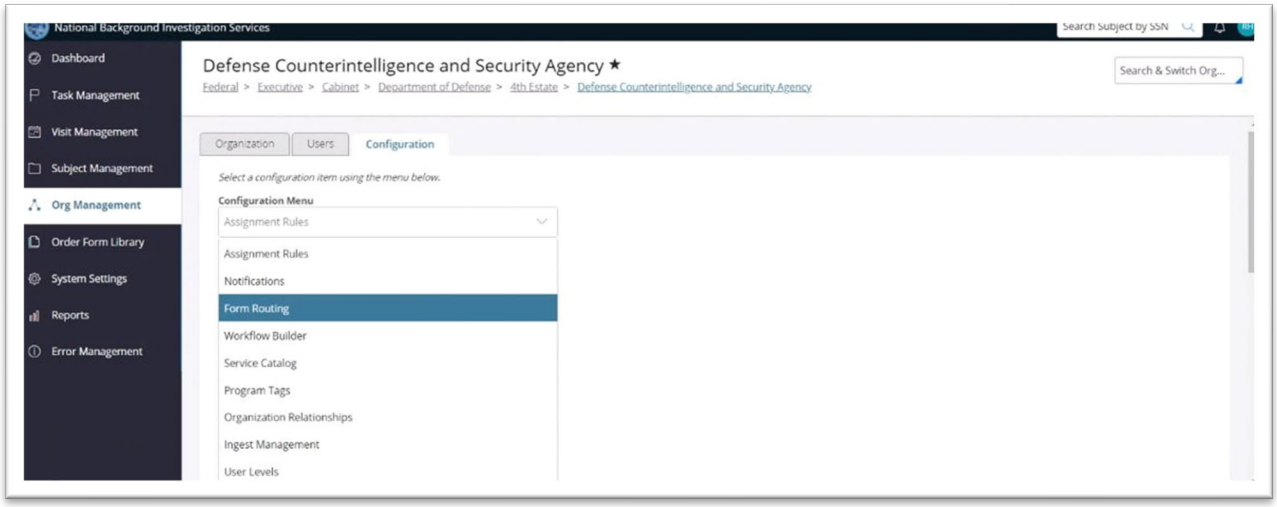
1. Select **Org Management** from the Navigation Menu on the left side of the screen.
2. Switch to the designated Org (if needed) and select the **Configuration tab**.
3. Select **Form Routing** from the Configuration Menu options.
4. The Form Routing Workflows will be listed and will indicate which Org is the Initiator, Reviewer and/or Authorizer. It will also show the status as either Enabled or Disabled. To view the details of a specific Form Routing Workflow, click the **hyperlink** in the Form Routing Name column.
5. Users can make modifications only if the Form Routing Workflow has not been used. If there are cases in-flight that have used or are using the Form Routing Workflow, then users can only edit the Form Routing Name or edit the status to **Enabled/Disabled**.
   - Note: Users may want to Enable a Form Routing Workflow to make sure that they will be able to utilize the routing option for their Org. Users may want to disable a Form Routing Workflow if a case is no longer being used or in-flight.
6. After making edits, select **Submit** to complete the updates.

DELETE FORM ROUTING WORKFLOWS

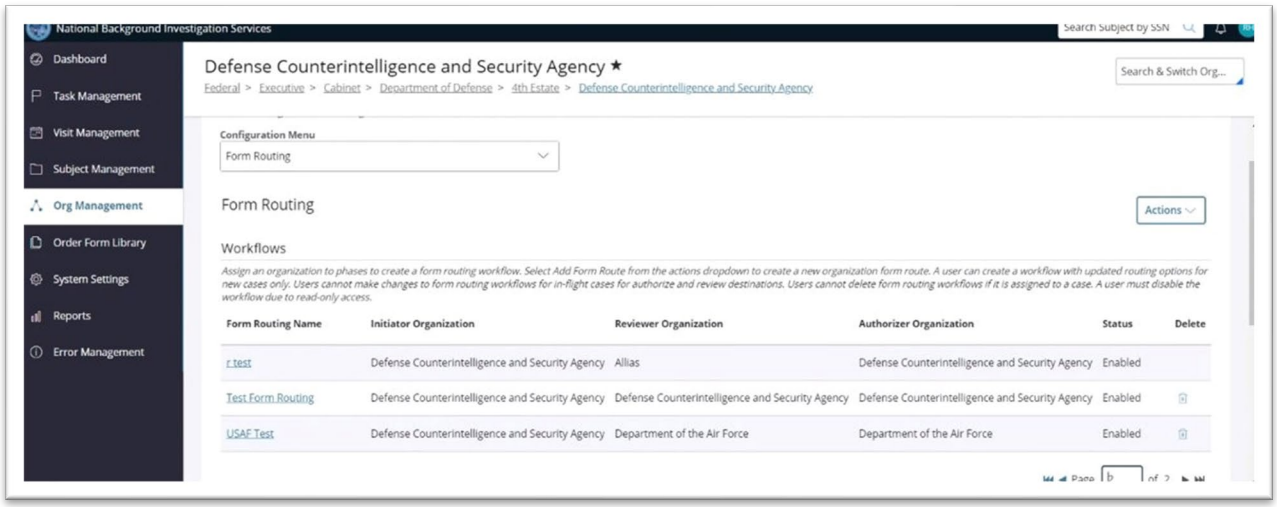
Below is the 6-step process for deleting Form Routing Workflows.

1. Select **Org Management** from the Navigation Menu on the left side of the screen.
2. Switch to the designated Org (if needed) and select the **Configuration tab**.
3. Select **Form Routing** from the Configuration Menu options.
4. Once all existing Form Routing Workflows are displayed, find the row for the specific Form Routing Workflow being deleted.
5. Select the **trashcan icon** under the Delete column to delete the Form Routing Workflow.
6. Select **Continue** to confirm the deletion request. The Form Routing Workflow will not appear on a user's list of existing Form Routing Workflows anymore.
   - Note: Users cannot delete a Form Routing Workflow that is in flight or assigned to a case. The trashcan icon will not be visible. Users may want to delete a Form Routing Workflow if the routing option is no longer assigned to a case or if the routing configuration is no longer applicable to their Org/cases within their Org. Users can view the History of a Form Routing Workflow by clicking the Actions button in the upper right-hand corner and selecting "History."

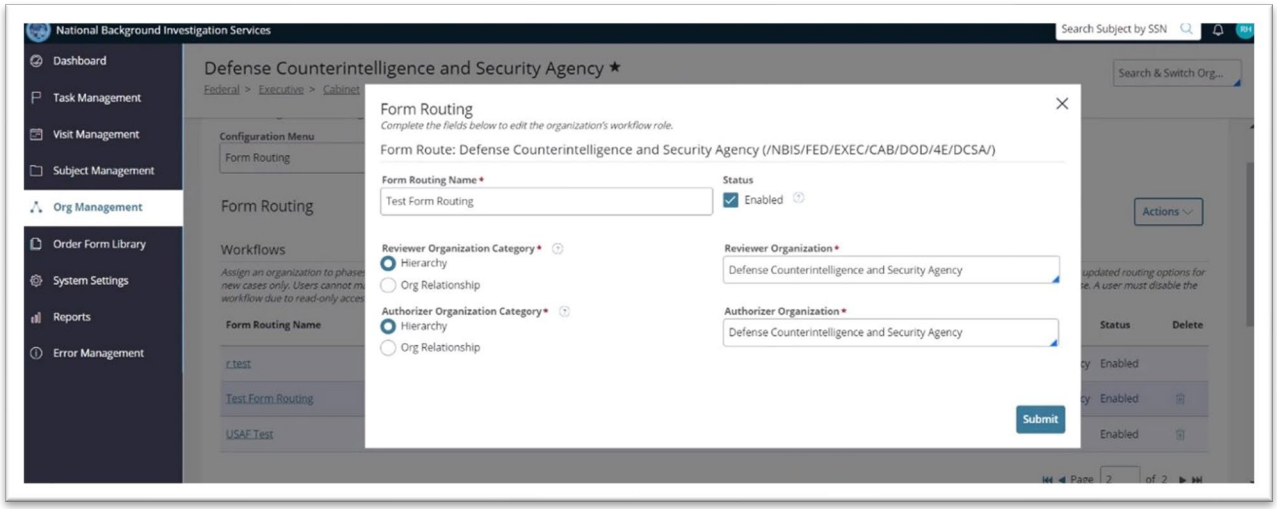
View, Edit, Enable/Disable (Steps 1-3)



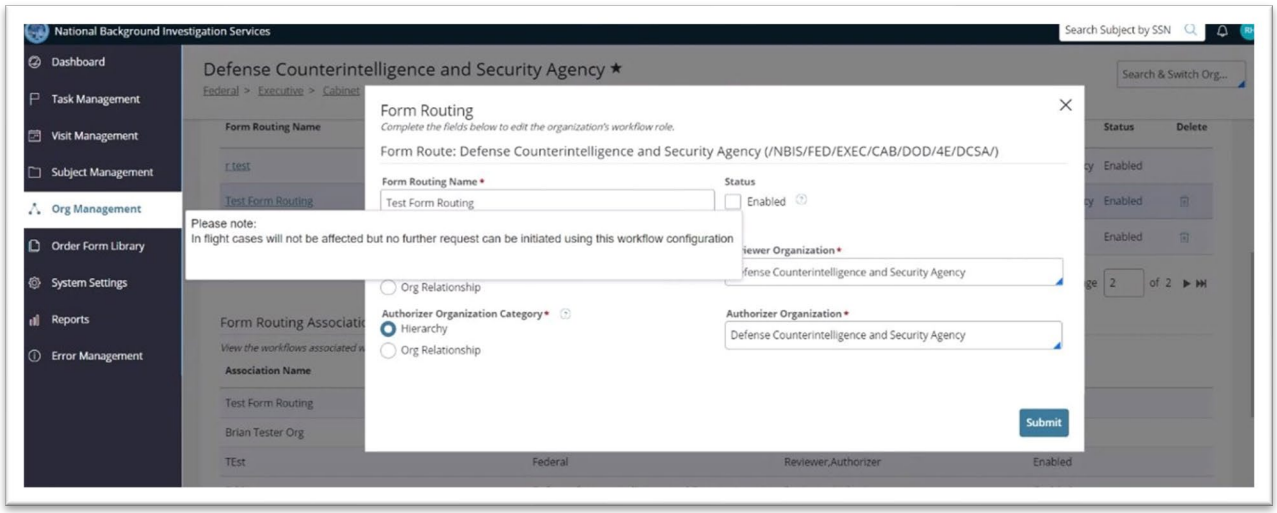
View, Edit, Enable/Disable (Step 4)



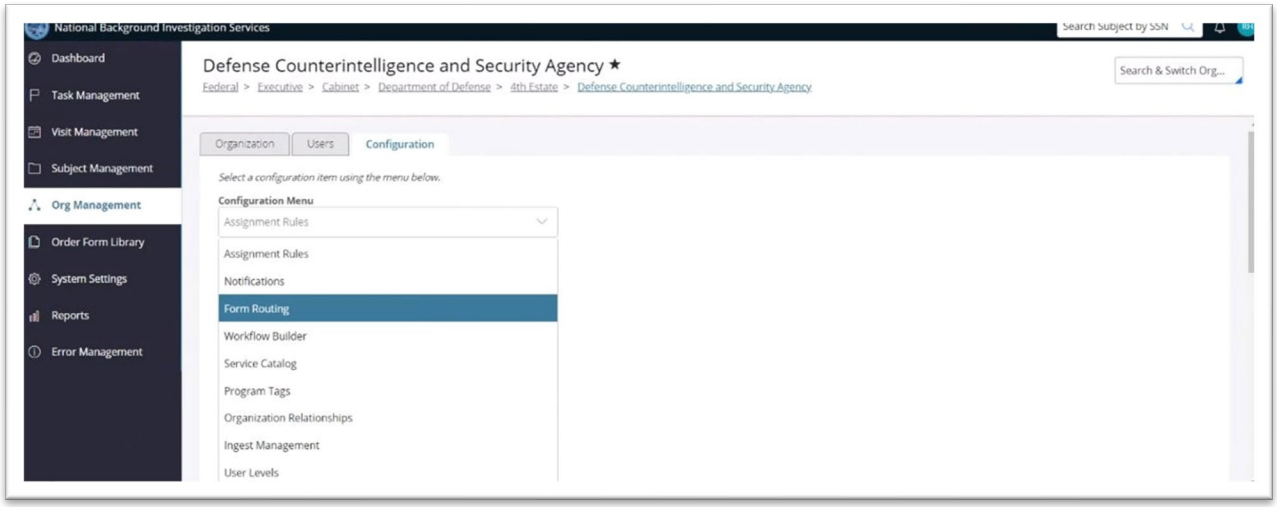
View, Edit, Enable/Disable (Step 5)



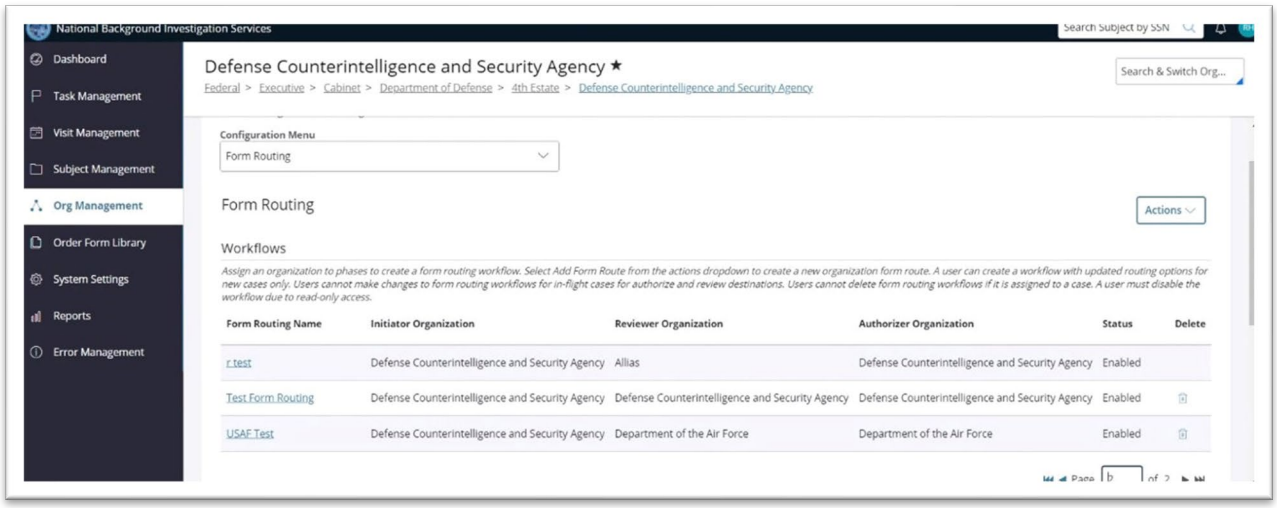
View, Edit, Enable/Disable (Step 6)



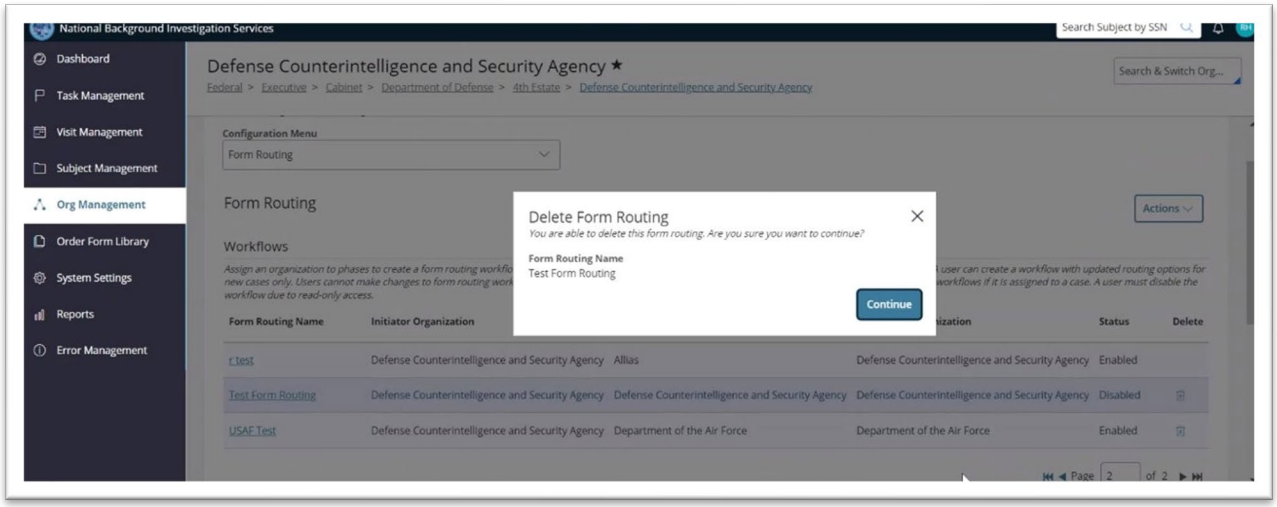
Delete a Form Routing Workflow (Steps 1-3)



Delete a Form Routing Workflow (Step 4)



Delete a Form Routing Workflow (Step 5-6)



ORGANIZATION MANAGEMENT

HOW TO NAVIGATE TO ORGANIZATIONS WITHIN YOUR HIERARCHY

There are two ways to do this. You can either search an organization or Switch Organization Context.

SEARCH AN ORGANIZATION

The Org Management tab can be utilized to view, search, or navigate to different Organizations and/or Sub-Organizations within a hierarchy. After a Parent Org or Sub-Org has been created, users with the Org Manager role can search for an organization's name or Org Code to navigate to different Orgs. Below is the 3-step process for navigation and searching for an Org.

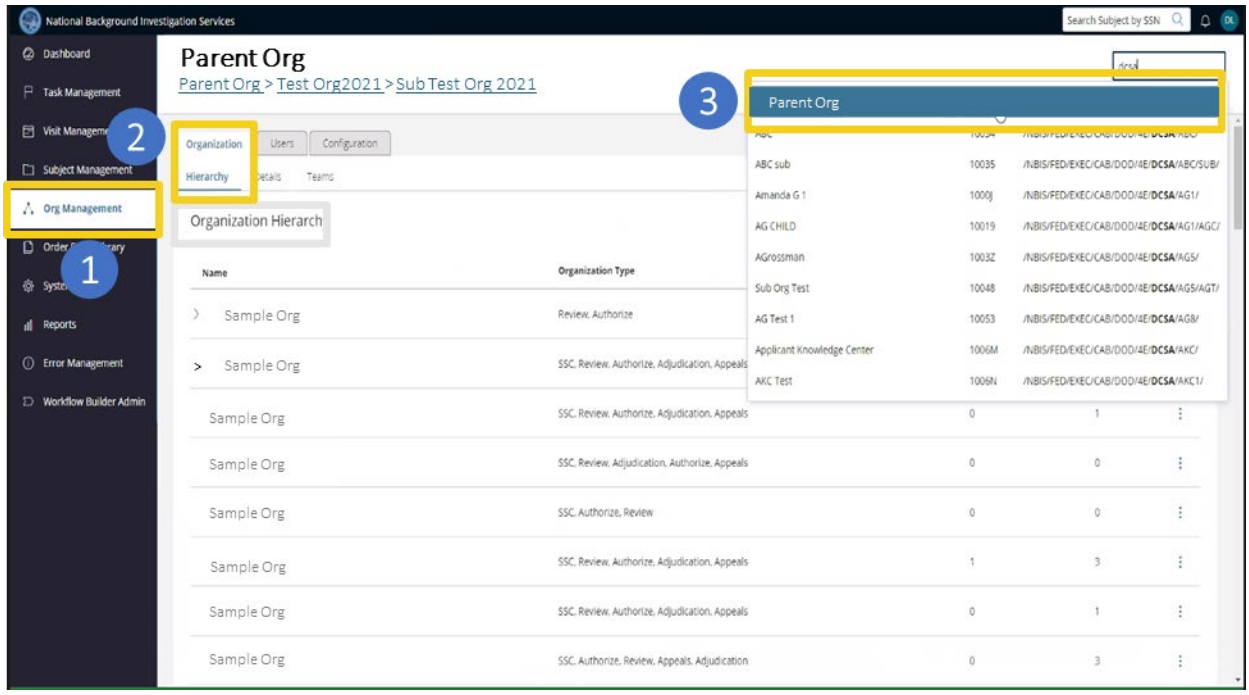
1. Navigate to Org Management on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. Navigate to the Search and Switch Org field in the top-right corner.
3. From the Search & Switch Org field, enter an Organization's Name, abbreviation, or Org Code to find and select a different Organization to view its details, users, and hierarchy.

SWITCH ORGANIZATION CONTEXT

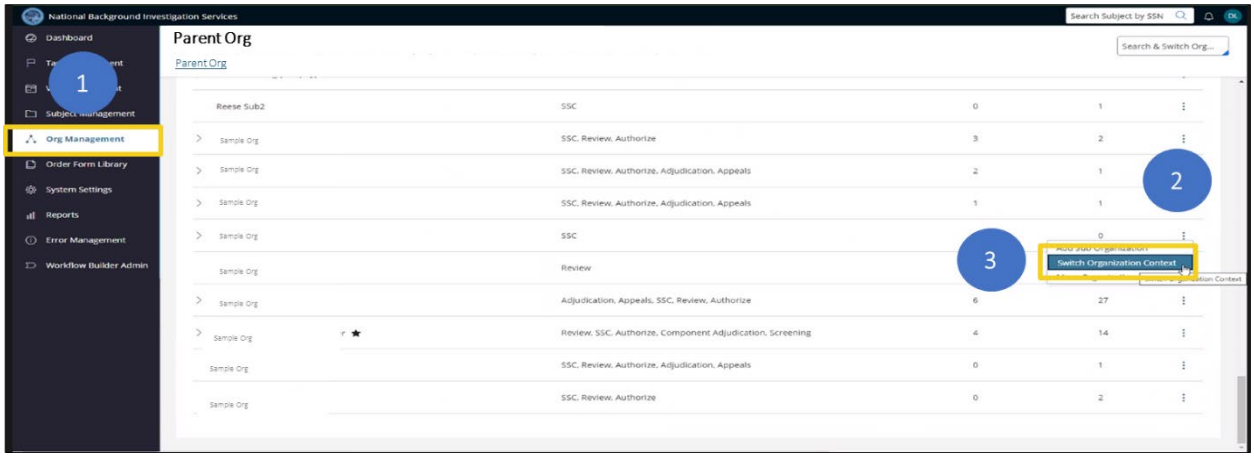
The Switch Organization Context function allows users with the Org Manager role to view a sub-org's details, users, and hierarchy. An example of when to use the Switch Organization Context function would be if a user is currently in an Org and may need to quickly navigate to a different sub-org to view their details. The Switch Organization Context function allows for the seamless navigation between different Sub-Orgs without having to manually search for Org Names and Org Codes. Below is the 3-step process for how to Switch Organization Context.

1. Navigate to Org Management on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. In the Actions column, select the ellipsis to display the Action options for the Sub-Org users wish to view.
3. Select Switch Organization Context to view the sub-org's details, users, and hierarchy.

Search an Organization (Steps 1-3)



Switch Organization Context (Steps 1-3)



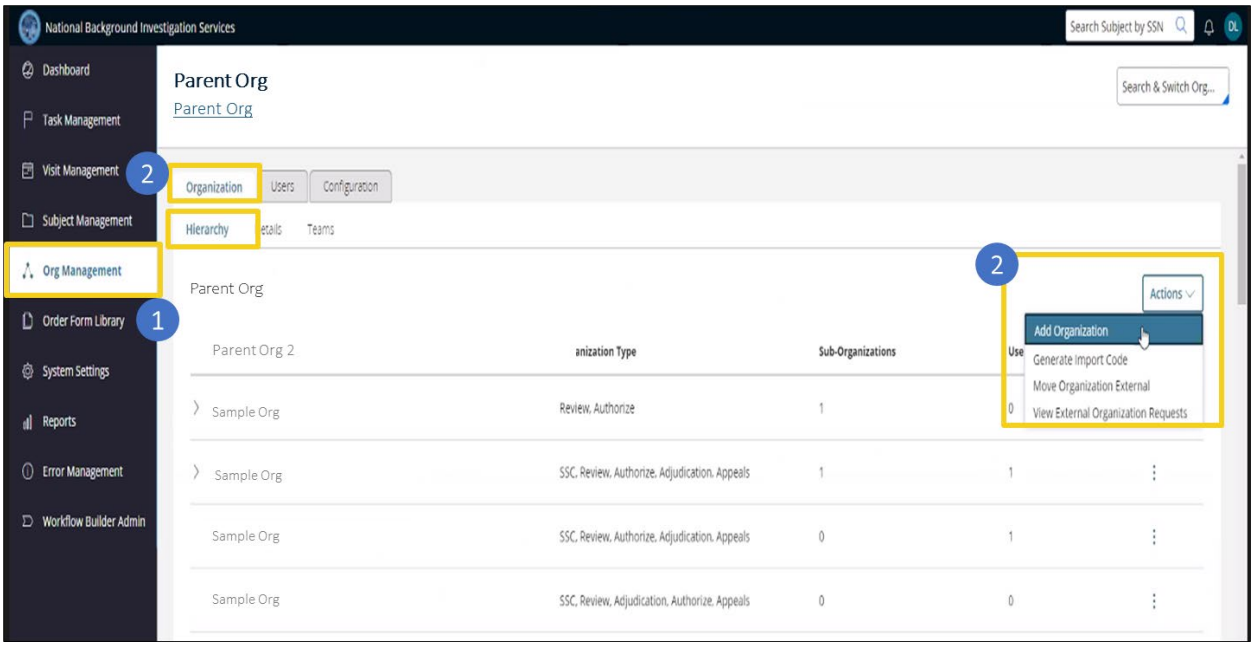
HOW TO ADD AN ORGANIZATION

The below provides the 8-steps that users with the Org Manager role can execute to start building an Org within their hierarchy. The first step in building a hierarchy is creating the Parent Org. The Org Manager role must be added by another user with the User Manager role to the newly created org.

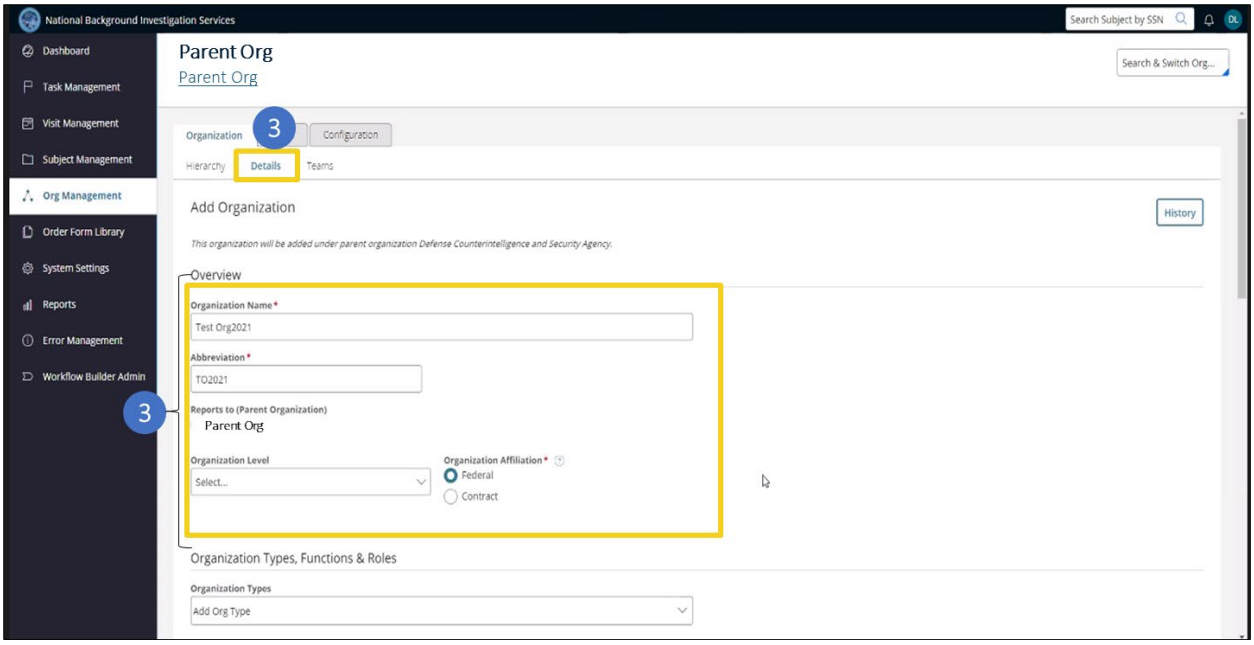
Below is the 8-step process for how to Add and Organization.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and search and switch to the designated Org (if needed).
2. Under the title Organization and the tab Hierarchy, select the Actions drop-down menu and choose **Add Organization**.
3. In the **Organization Details** tab, enter Organization Name, Abbreviation, Org Level, Organization Affiliation. These are required and marked by a red asterisk.
4. Choose the **Org Type(s)** from the drop-down menu. This will auto-populate some of the corresponding Org Functions and Org Roles. Users may choose to "x" out of these to remove the Org Types, Org Functions, and Org Roles. Users may also add applicable Org Types, Org Functions, and Org Roles, as necessary.
5. To view the Role Descriptions/Permissions table, click on the bottom link titled "**View Permissions/Role Descriptions**" and review the latest role descriptions before saving.
6. Users should also enter the **Legacy Systems** information to ensure the data maps correctly in the Org.
7. In the Organization Details tab, enter **Organization Location** and **Mailing Address**. These are required and marked by a red asterisk.
8. Once information is complete, click **Save**.
9. A green success banner will appear at the top stating the newly created Org has been added. The Org that was created will now appear in the hierarchy.

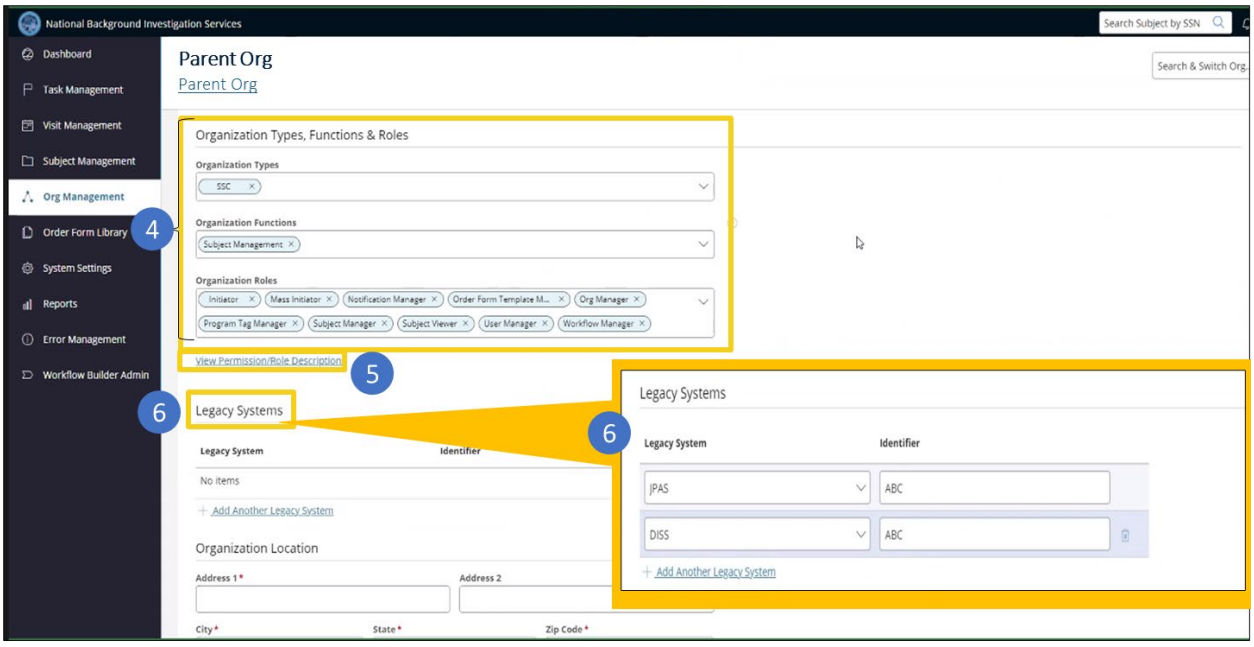
Steps 1-2



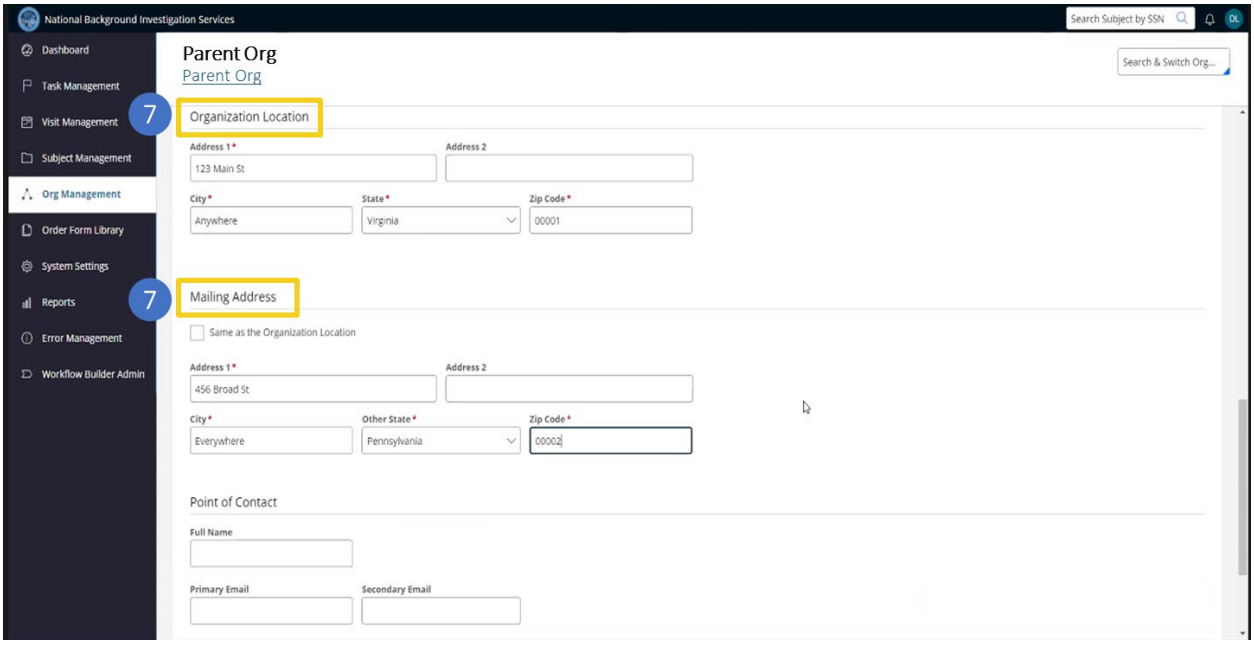
Step 3



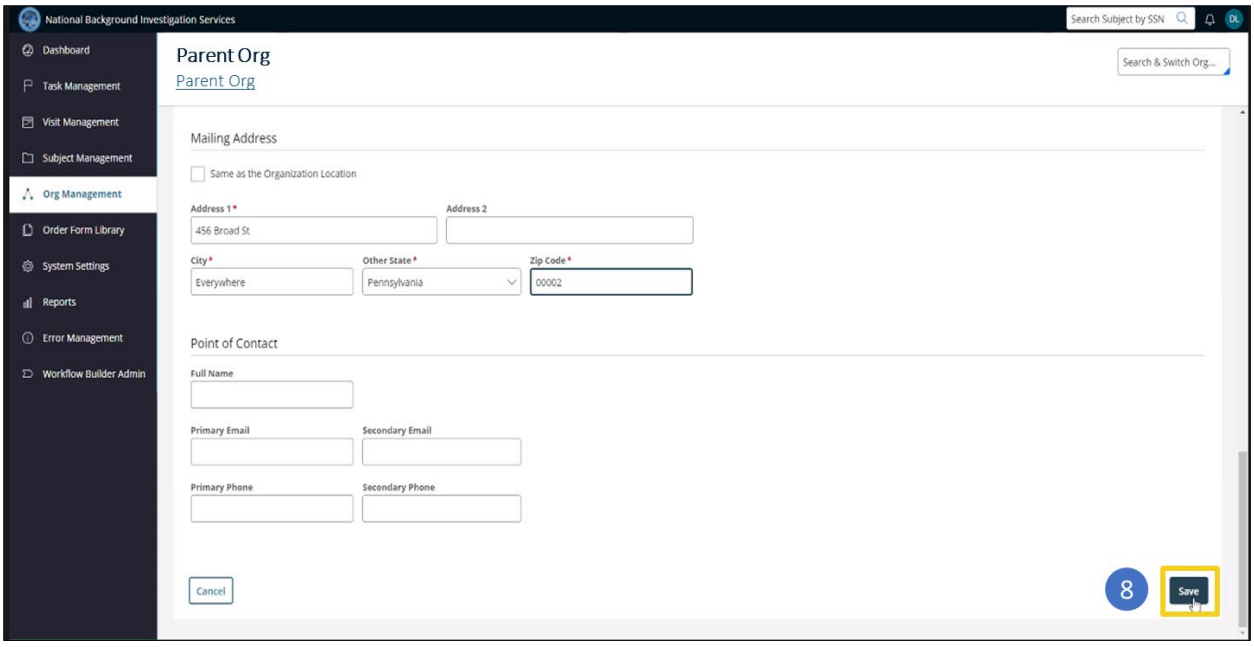
Steps 4-6



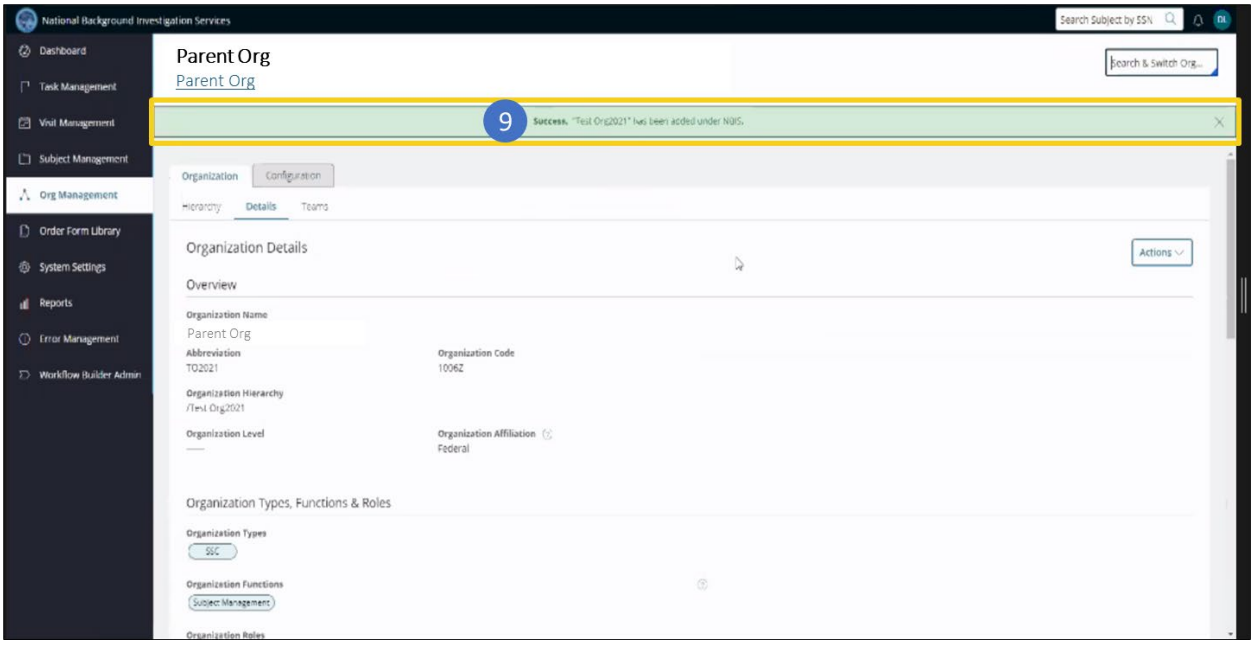
Step 7



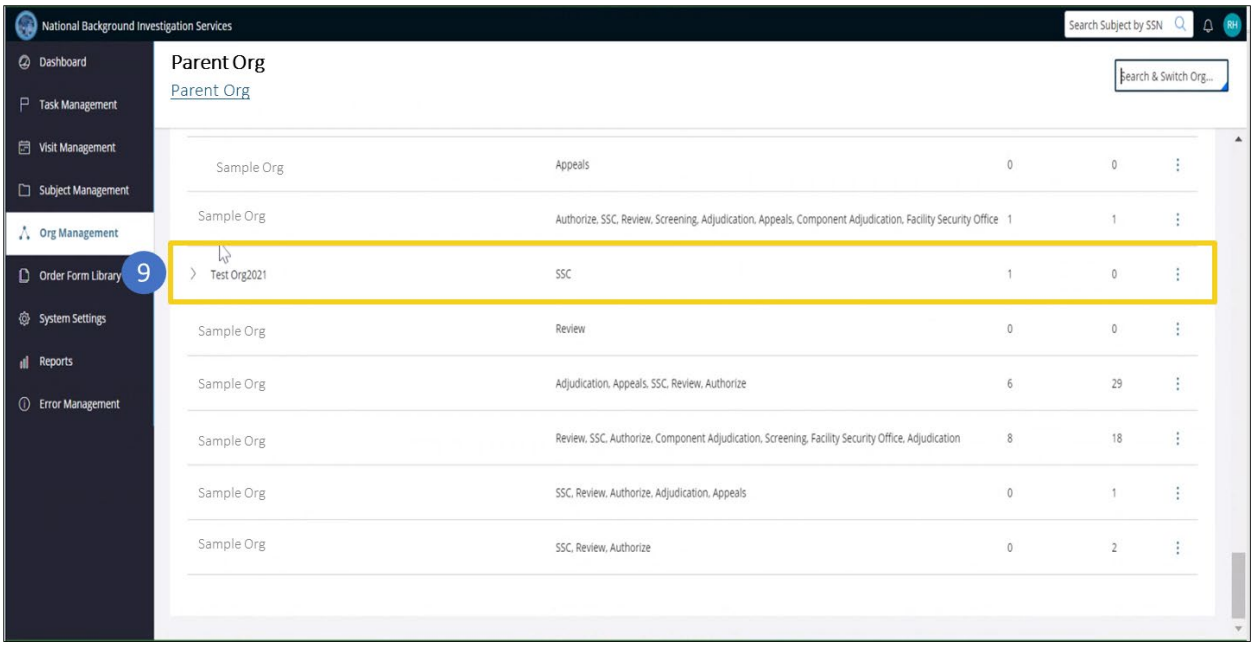
Step 8


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...
Mailing Address
Same as the Organization Location
Address 1 *
456 Broad St
Address 2
City *
Everywhere
Other State *
Pennsylvania
Zip Code *
00002
Point of Contact
Full Name
Primary Email
Secondary Email
Primary Phone
Secondary Phone
Cancel
8
Save

Step 9


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...
9
Success. "Test Org2021" has been added under NBIS.
Organization
Configuration
Hierarchy
Details
Teams
Organization Details
Actions
Overview
Organization Name
Parent Org
Abbreviation
TO2021
Organization Code
1006Z
Organization Hierarchy
/Test Org2021
Organization Level
Organization Affiliation
Federal
Organization Types, Functions & Roles
Organization Types
SSC
Organization Functions
Subject Management
Organization Roles

Step 9 (Continued)



HOW TO MOVE, EDIT, AND DELETE AN ORGANIZATION

MOVE AN ORGANIZATION (INTERNAL MIGRATION)

Users with the Org Manager role can move Sub-Organizations within a hierarchy, which is known as an Internal Migration. Sub-Orgs must have the same identical roles as the Parent Organization. If the moving Organization has certain roles that the receiving Organization does not have, these roles will be automatically dropped during the migration. In some cases, this means the Sub-Org will lose roles. In others, they will have the option to add additional roles that are now available under their new Parent Org. Additionally, an Org cannot be migrated if there are any cases inflight from that Org. Below is the 4-step process for how to Move an organization.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated organization to move.
2. Under the Actions column for the specific organization, select the ellipse icon then select **Move Organization**.
3. Choose the receiving org and select **Move Here**. Users cannot move to the same parent org.
4. The confirmation page displays the preview of the new hierarchy after confirming the organization migration, the impacted roles, and the number of users associated to these impacted roles.
5. Check the box to proceed with the change and select **Confirm** to proceed with the migration.

EDIT AN ORGANIZATION

After navigating to a hierarchy to view the parent organization and its sub-orgs, users with the Org Manager Role can edit their parent-org/sub-org if needed. Examples of why users may want to edit an Org could be to correct a mailing address, add new user roles or input legacy data. Below is the 4-step process for how to edit an organization.

1. Navigate to **Org Management** in the left-hand panel and switch to the designated Org (if needed).
2. Select the Organization tab and the **Details tab** beneath it.
3. Under the Details tab, select **Edit Org from** the Actions drop-down menu in the right-hand box.
4. Edit any information in the fields and click Save. Note: The Organization Level field is editable, with all grouped org levels as available options for the System Manager and Onboarding Manager.

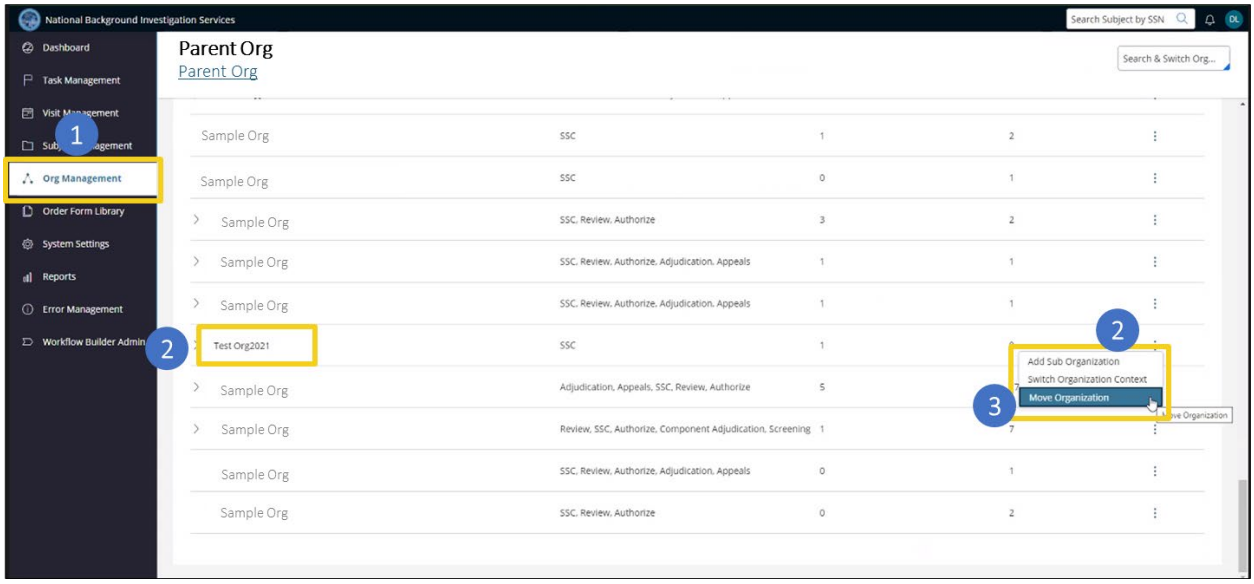
DELETE AN ORGANIZATION

Users with the Org Manager role can delete an organization, if needed. Users can only delete an organization once all users, workflows, teams, and sub-orgs are removed from the organization. The Delete Org option from the Actions drop-down will only appear once all these conditions have been met. Below is the 4-step process for how to delete an Org.

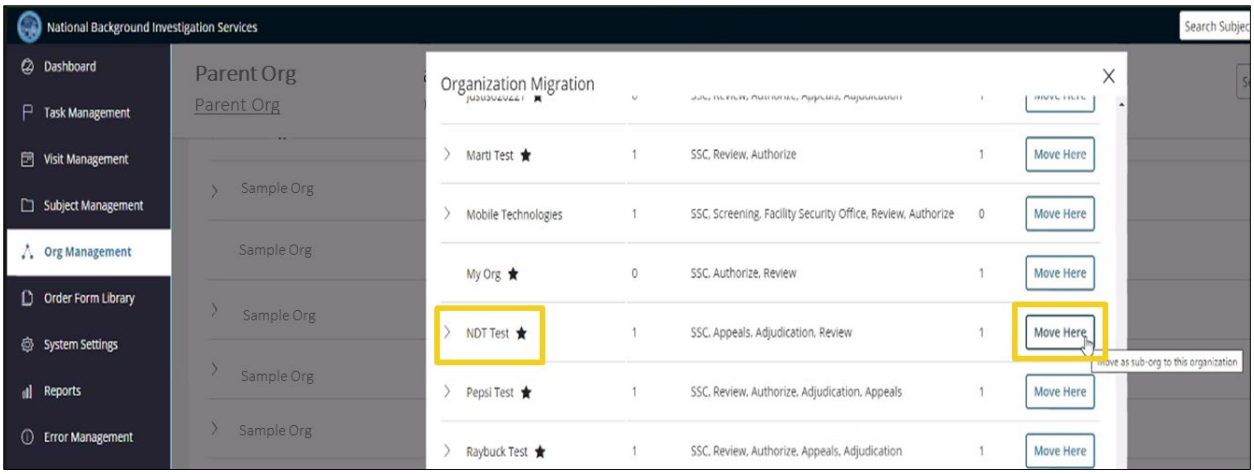
1. Navigate to **Org Management** on the left-hand side and switch to the designated Org (if needed).
2. Select the **Details** tab. From the Actions drop-down, select **Delete Org**.

3. A confirmation screen will pop-up to confirm the deletion of the organization.
4. Select **Confirm** to delete the organization.

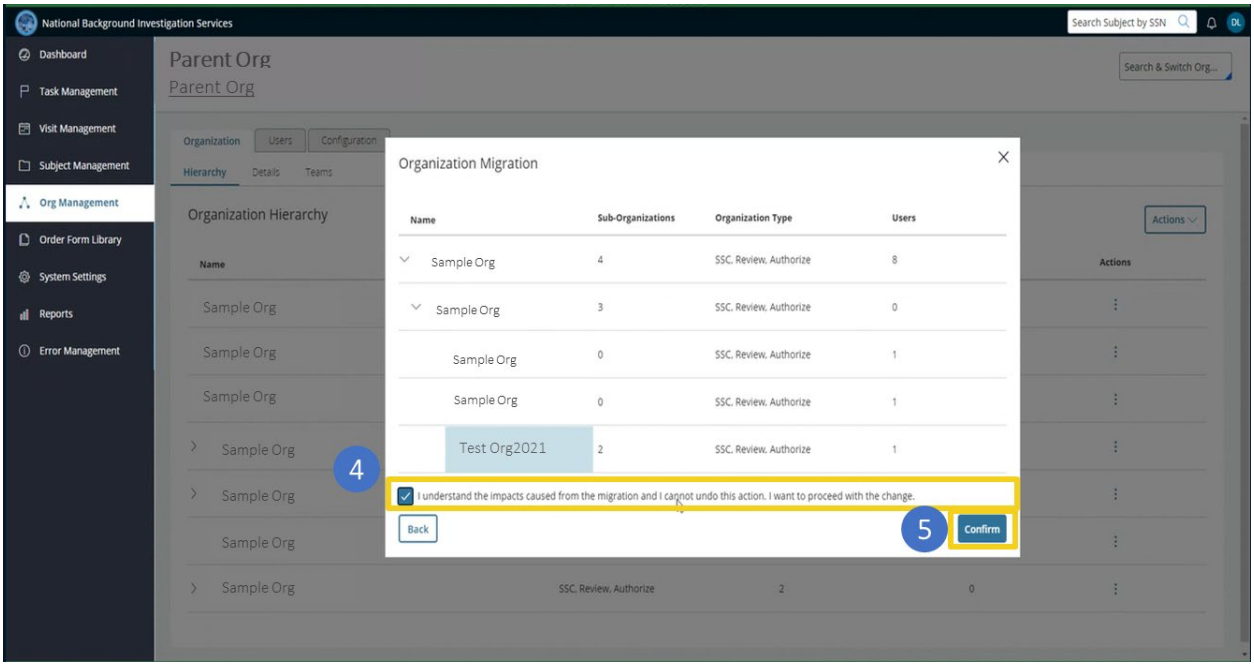
Move an Org (Steps 1-3)



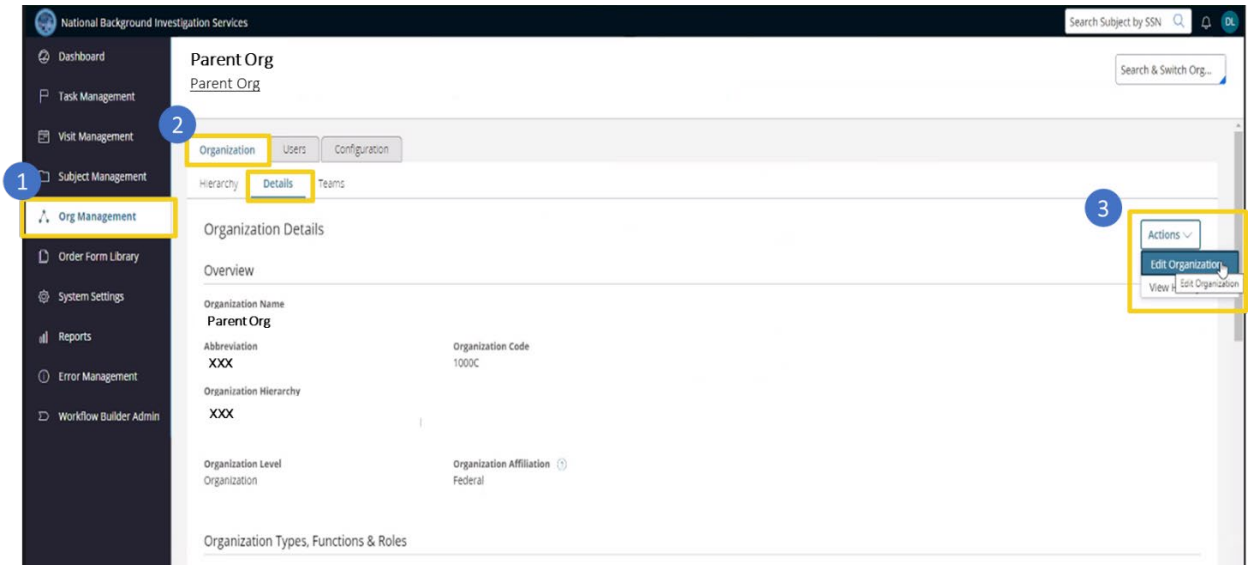
Move an Org (Step 3 Continued)



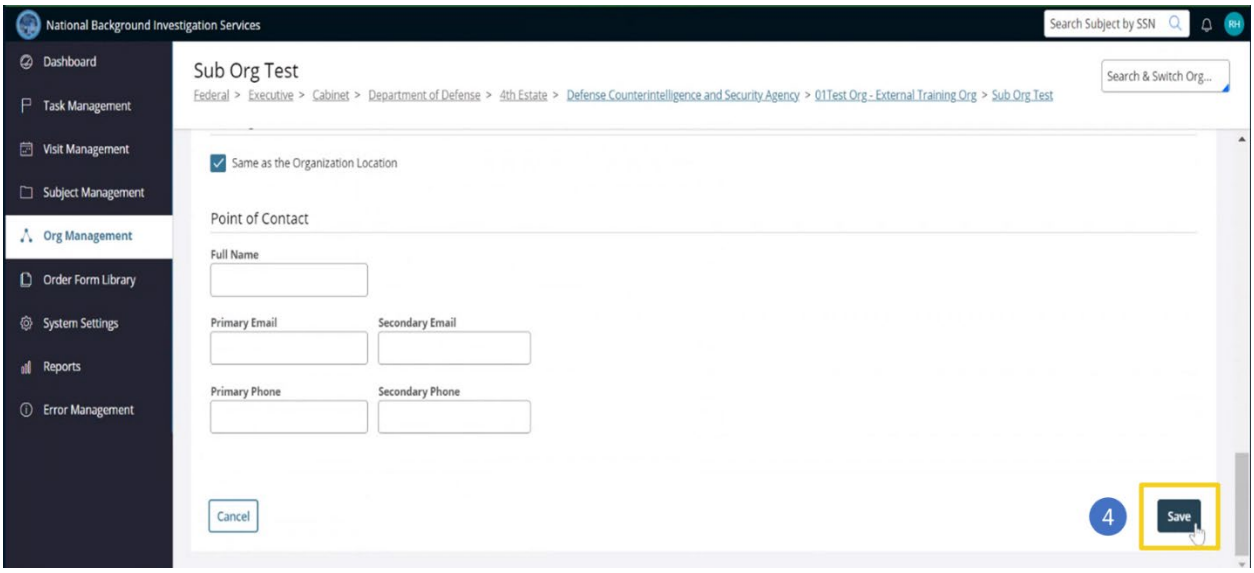
Move an Org (Steps 4-5)



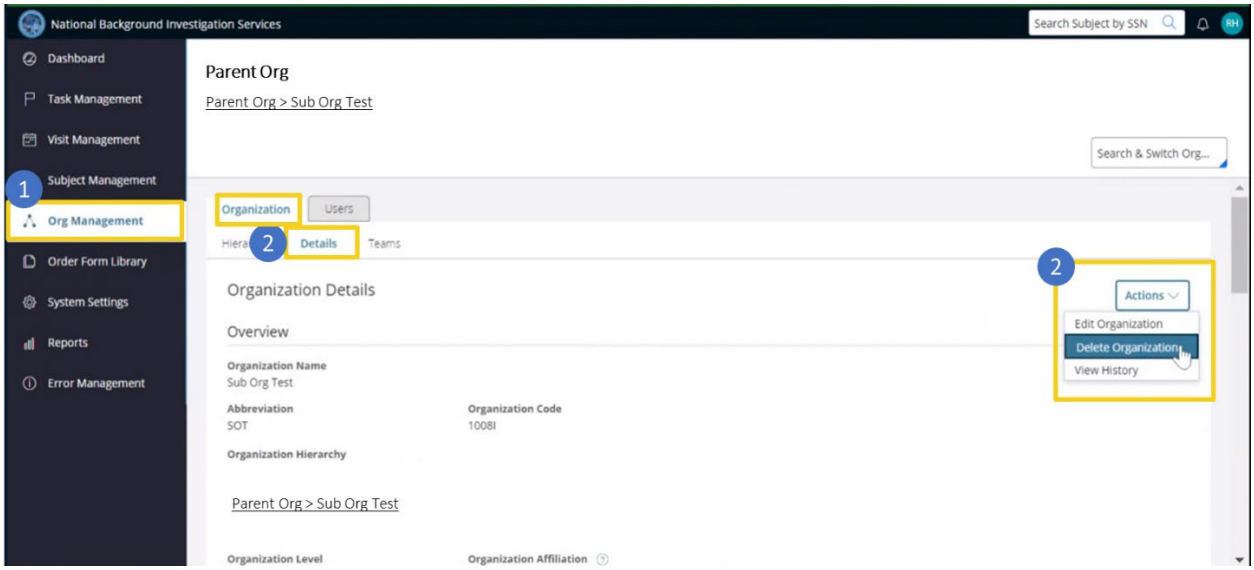
Edit an Org (Steps 1-3)



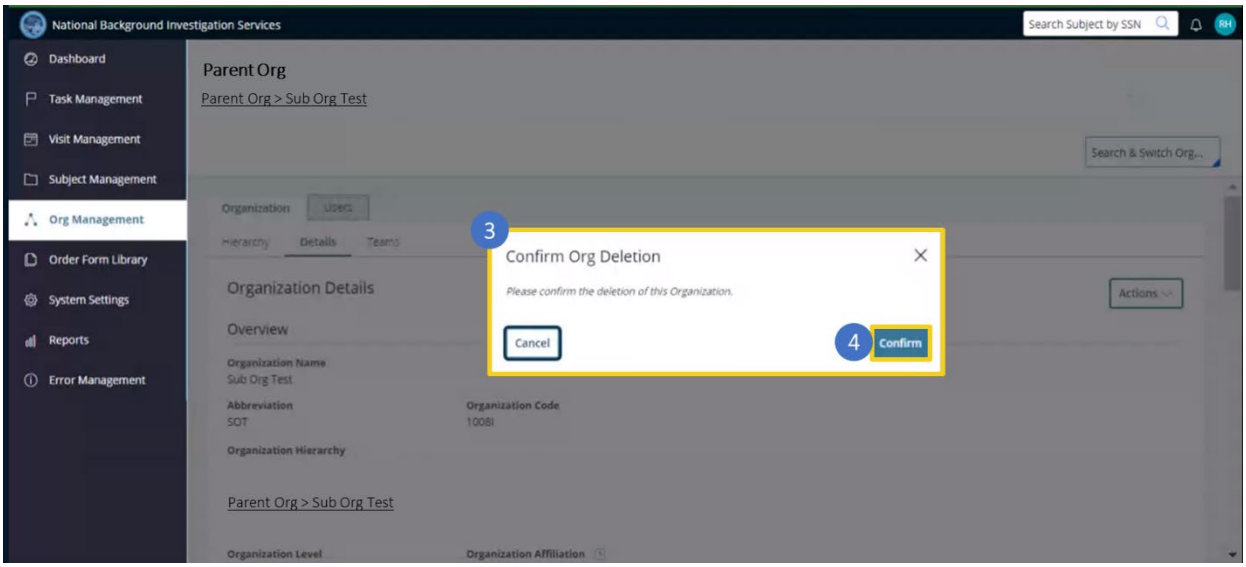
Edit an Org (Step 4)



Delete an Org (Steps 1-2)



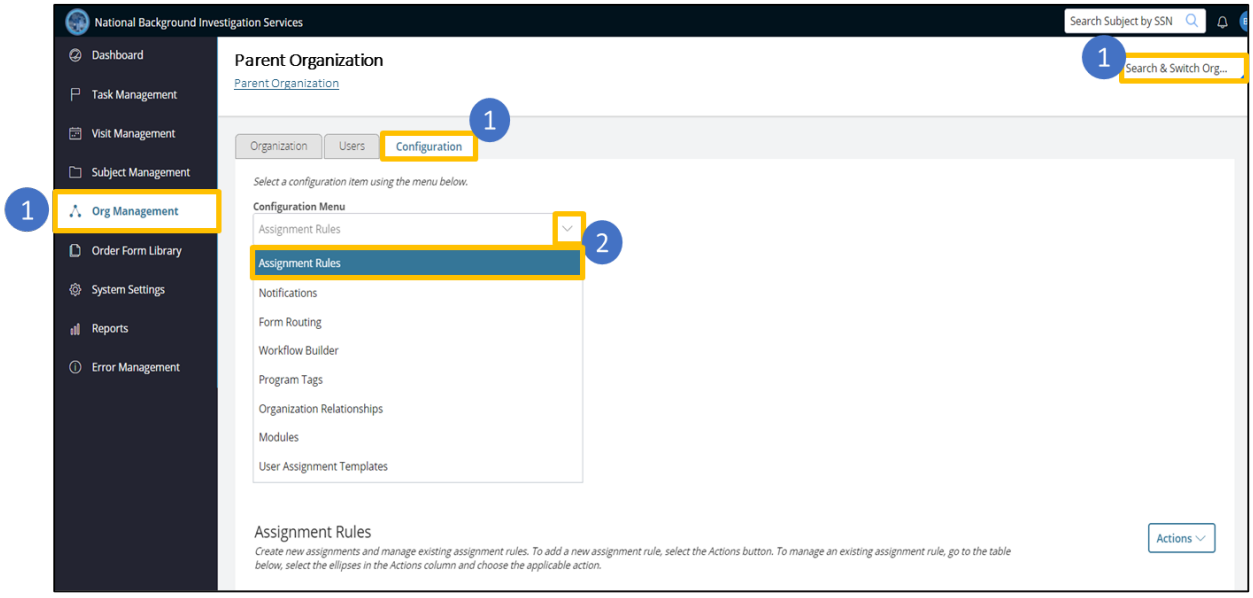
Delete an Org (Steps 3-4)



HOW TO ADD AN ORG ASSIGNMENT RULE

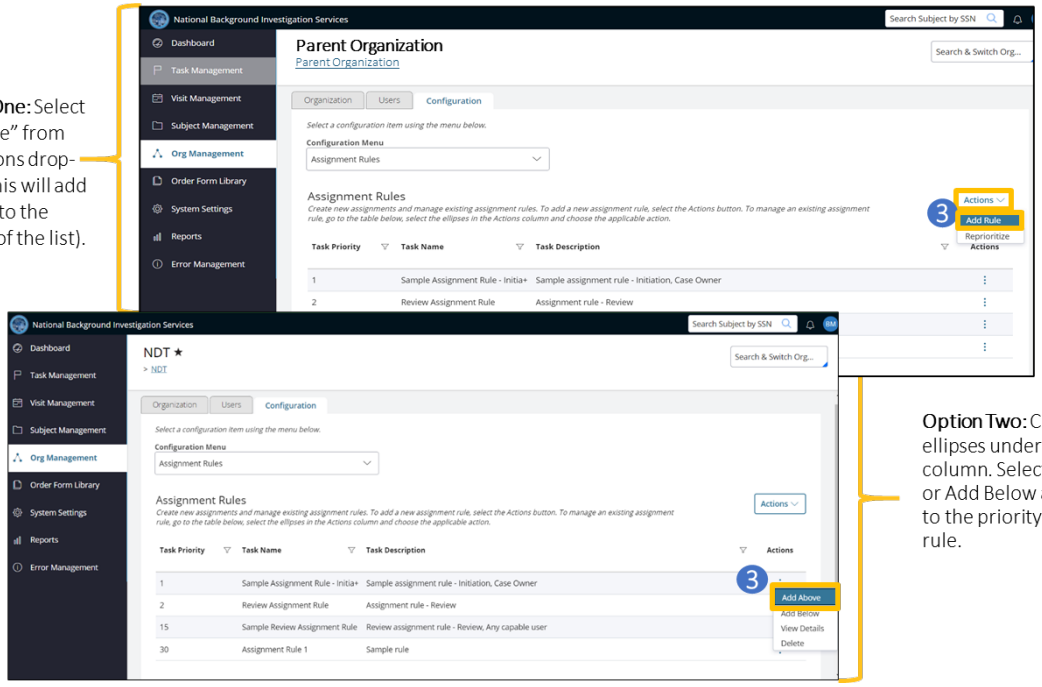
Users with the Org Assignment Manager role can add and manage Assignment Rules for their Org. Below is the 12-step process for how to add an Assignment Rule.

1. From the Navigation Menu on the left, select **Org Management**. Switch to the designated Org (if needed) and select the Configuration tab.
2. From the Configuration drop-down menu, select **Assignment Rules**.



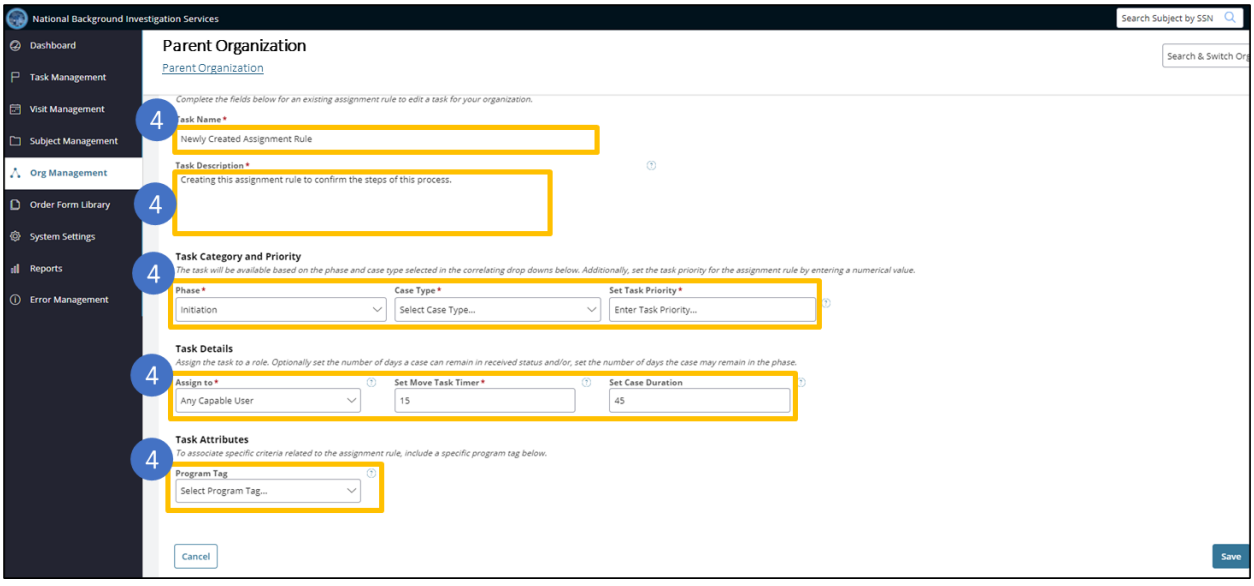
3. There are two ways to add a new Assignment Rule. The first option is to select **"Add Rule"** from the Actions drop-down (this will add the rule to the bottom of the list). The second option is to **click the vertical ellipses** (three vertical dots) under the Actions column. Select Add Above or Add Below according to the priority of the new rule.

Option One: Select "Add Rule" from the Actions drop-down (this will add the rule to the bottom of the list).



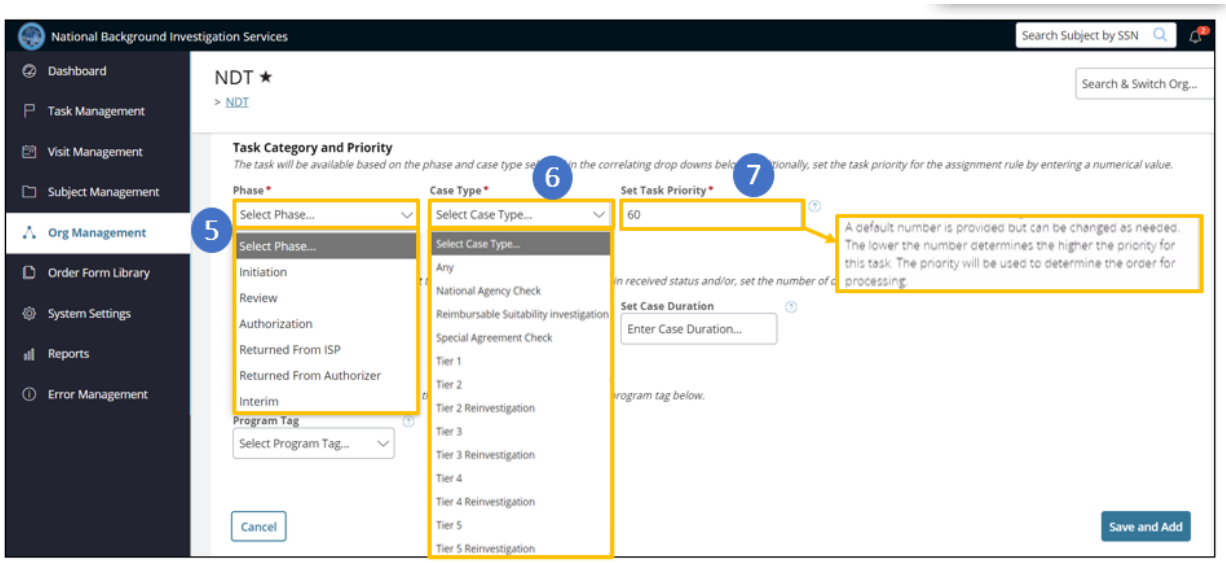
Option Two: Click the ellipses under the Actions column. Select Add Above or Add Below according to the priority of the new rule.

4. **Complete all required fields** marked with an asterisk within the Task Name, Task Description, Task Category and Priority, and Task Details sections of the "Add Assignment Rules" page. Note: Please click the question mark icon for additional information on any given field.

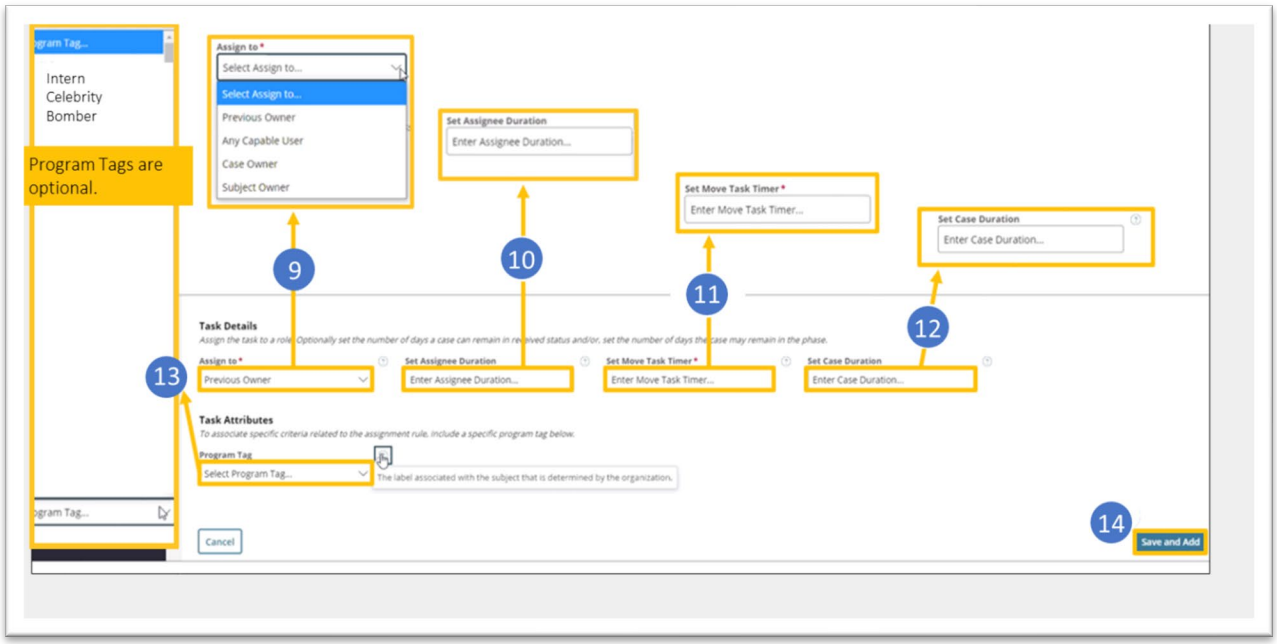


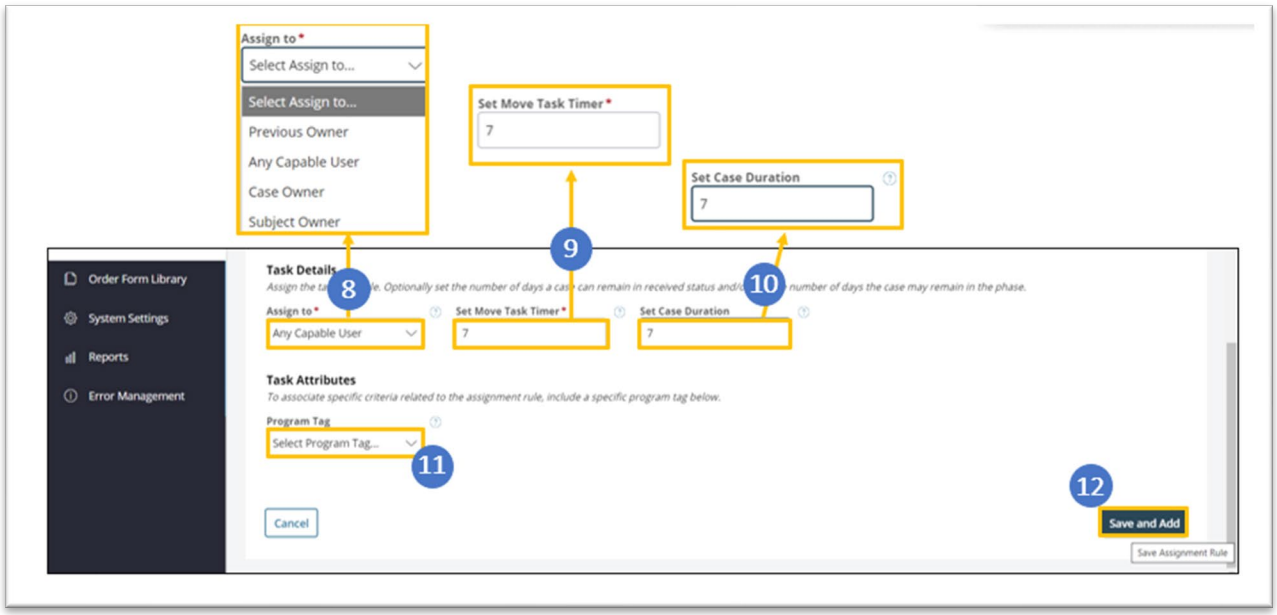
5. In the Phase field, **select the phase** the case is currently in. Phases include Initiation, Screening, Review, Authorization, Returned from ISP, Returned from Authorizer, Adjudication, Appeals, Component Adjudication and Interim.

6. In the Case Type field, **select the appropriate Investigation Tier**. Note: You may only select one case type at a time for a given assignment rule.
7. **Set the Task Priority**. This is a system-generated numeric value used to determine the order of Assignment Rule processing. The lower the number, the higher the priority.



9. Assign the case to a user from the **"Assign To"** drop-down menu. Note: Additional fields may appear, depending on the option selected. Options include Previous Owner, Any Capable User, Case Owner and Subject Owner.
10. **Set the Move Task Timer** to determine how long the task can remain with the current assignee if it is not worked on before it is routed to another user.
11. **Set the Case Duration**, as needed and if applicable. In this field, users enter the number of days to prioritize the case based on when the case was first created or initiated.
12. Select the appropriate **Program Tags**, as needed and if applicable.
13. Select **Save and Add**.


Intern
Celebrity
Bomber
Program Tags are optional.
Assign to *
Select Assign to...
Select Assign to...
Previous Owner
Any Capable User
Case Owner
Subject Owner
Set Assignee Duration
Enter Assignee Duration...
Set Move Task Timer *
Enter Move Task Timer...
Set Case Duration
Enter Case Duration...
9
10
11
12
13
14
Task Details
Assign the task to a role. Optionally set the number of days a case can remain in received status and/or, set the number of days the case may remain in the phase.
Assign to *
Previous Owner
Set Assignee Duration
Enter Assignee Duration...
Set Move Task Timer *
Enter Move Task Timer...
Set Case Duration
Enter Case Duration...
Task Attributes
To associate specific criteria related to the assignment rule, include a specific program tag below.
Program Tag
Select Program Tag...
The label associated with the subject that is determined by the organization.
Cancel
Save and Add


Assign to *
Select Assign to...
Select Assign to...
Previous Owner
Any Capable User
Case Owner
Subject Owner
Set Move Task Timer *
7
Set Case Duration
7
9
8
10
11
12
Order Form Library
System Settings
Reports
Error Management
Task Details
Assign to *
Any Capable User
Set Move Task Timer *
7
Set Case Duration
7
Task Attributes
To associate specific criteria related to the assignment rule, include a specific program tag below.
Program Tag
Select Program Tag...
Cancel
Save and Add
Save Assignment Rule

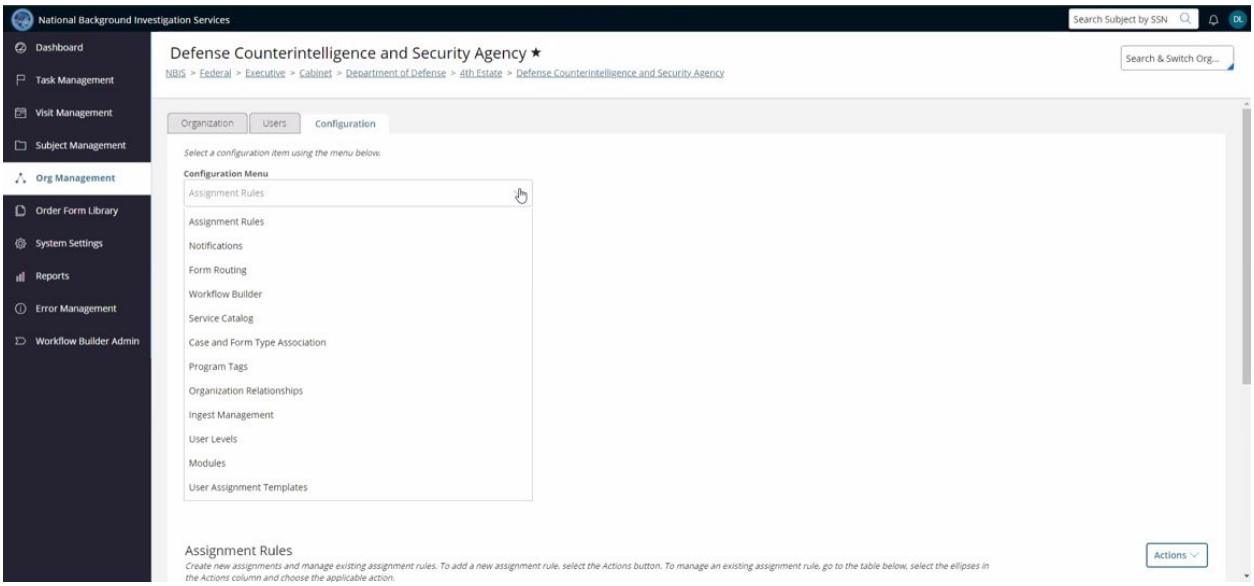
HOW TO MANAGE ORG ASSIGNMENT RULES

Users with the Org Assignment Manager role can manage Assignment Rules using the Configuration drop-down menu. There are multiple ways to manage an Assignment Rule after it has been added including viewing, editing, deleting, and reprioritizing Assignment Rules.

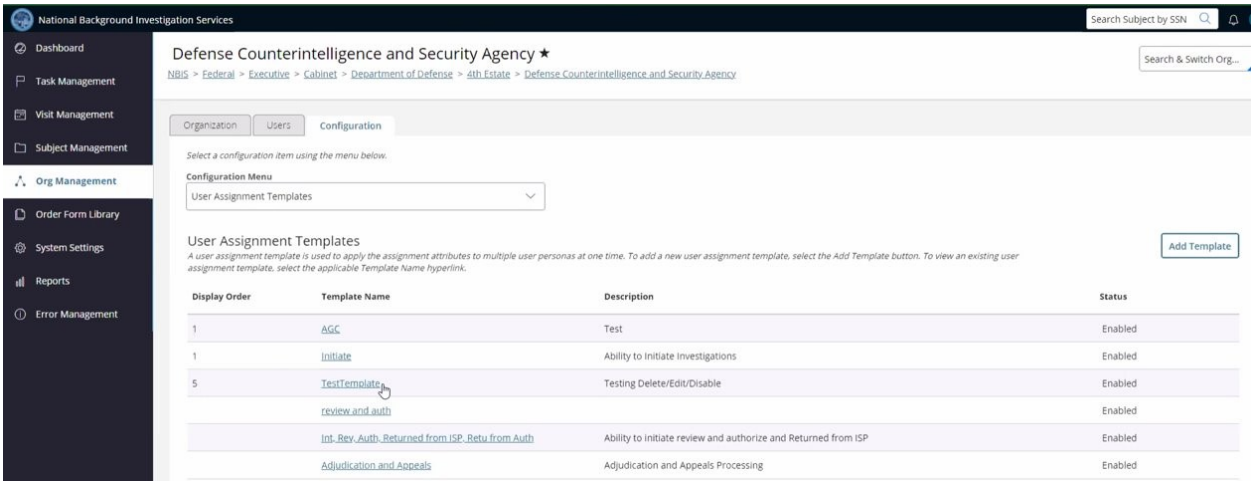
VIEW AN ASSIGNMENT RULE

Below is the 4-step process for how to View an Assignment Rule.

1. From log in, select **Organization Management** from the Navigation Menu on the left. Navigate to your Org (if needed).
2. In the Organization Management window, select the **Configuration** tab. Make sure the Organization you are working in is selected; if not, you will need to select that Organization first.
3. Select the **Assignment Rules** subtitle from the drop-down options from the Configuration menu. The screen will display a prioritized list of existing Assignment Rules.



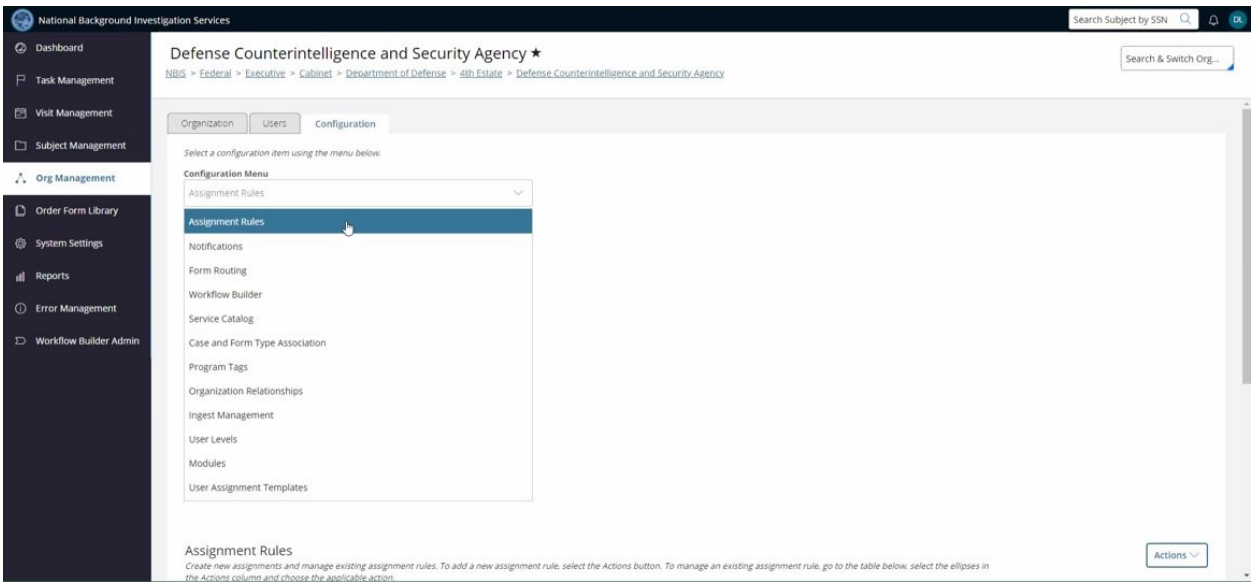
4. In the table of Assignment Rules, under the Actions column, select the ellipses (three vertical dots) for the specific rule and then select **View Details**.



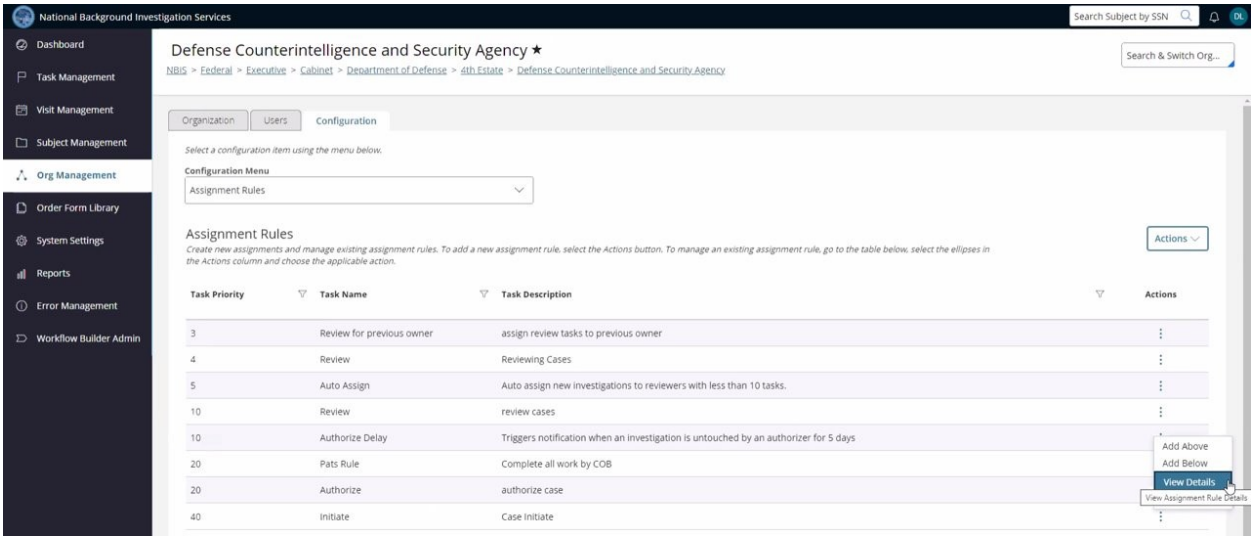
EDIT AN ASSIGNMENT RULE

Below is the 6-step process for how to Edit an Assignment Rule.

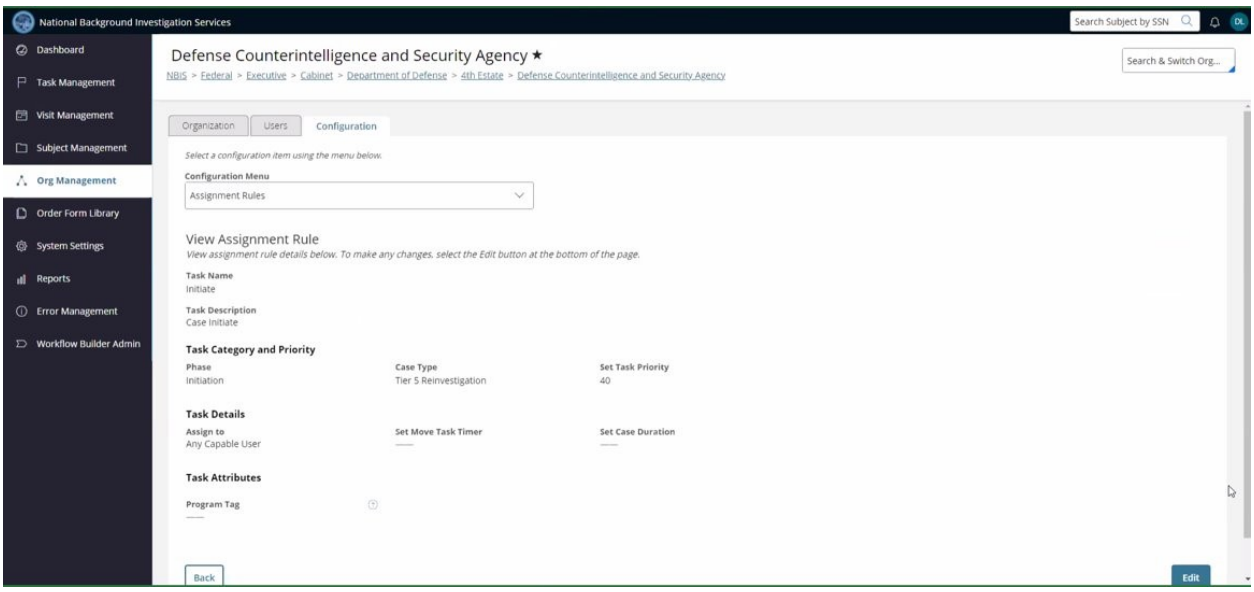
1. From login, select **Organization Management** from the Navigation Menu on the left. Navigate to your Organization (if needed) then select the **Configuration** tab.
2. Select **Assignment Rules** from the Configuration drop down menu.



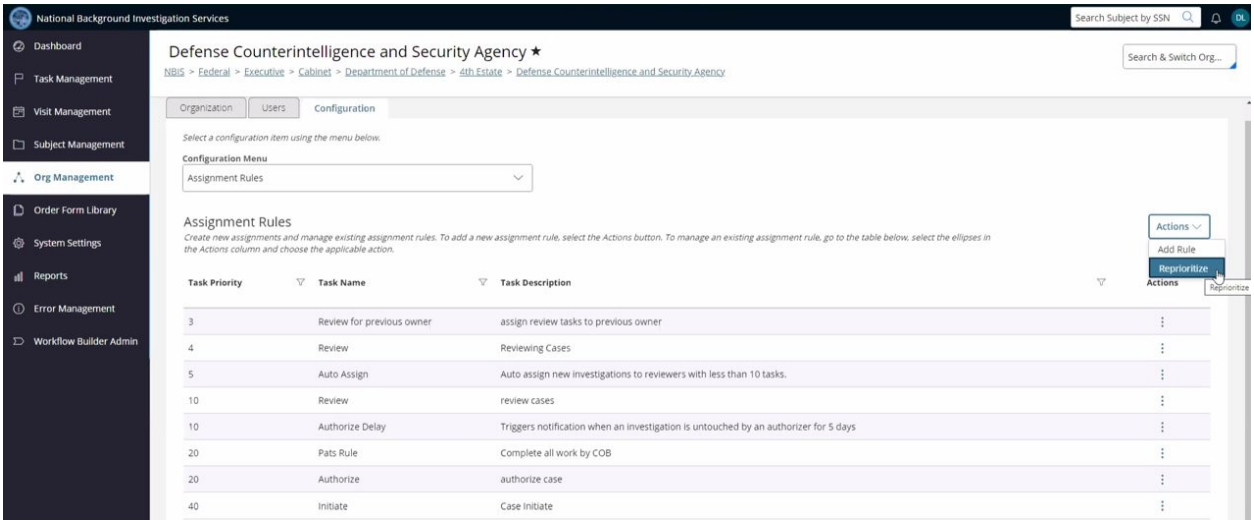
3. The screen will display a prioritized list of existing Assignment Rules. Within the list of Assignment Rules, locate the row you want to edit.
4. In the row that you want to edit, select the ellipses in the Actions column on that row. Select **View Details**.



5. Select Edit then make any changes and select **Save** when completed.



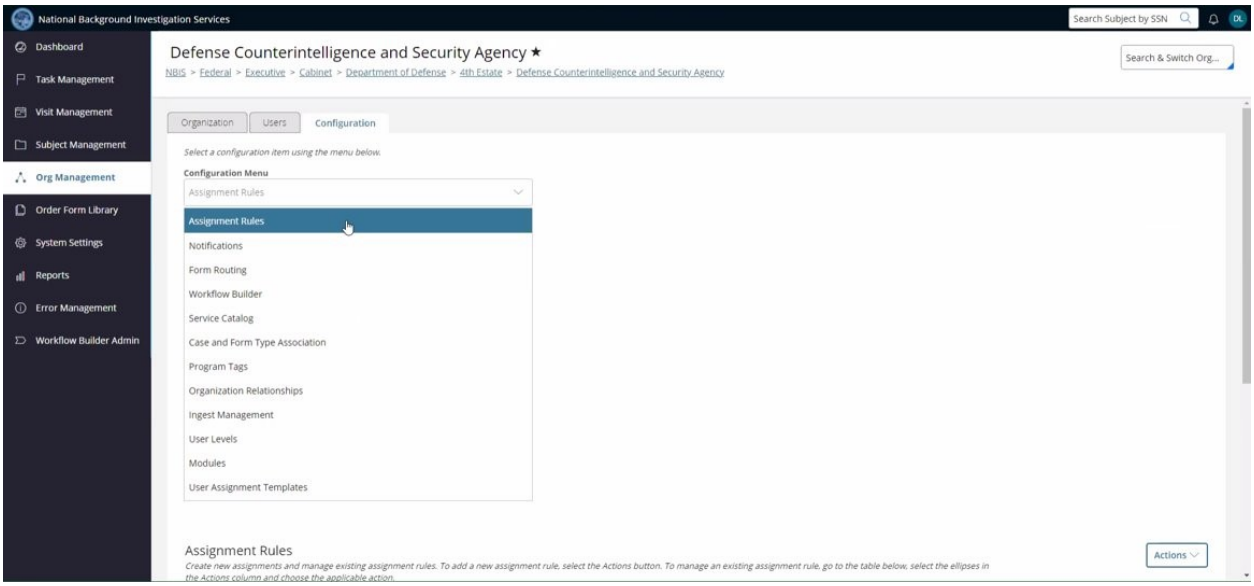
6. From the Actions drop-down, select **Reprioritize**.



DELETE AN ASSIGNMENT RULE

Below is the 6-step process for how to Delete an Assignment Rule.

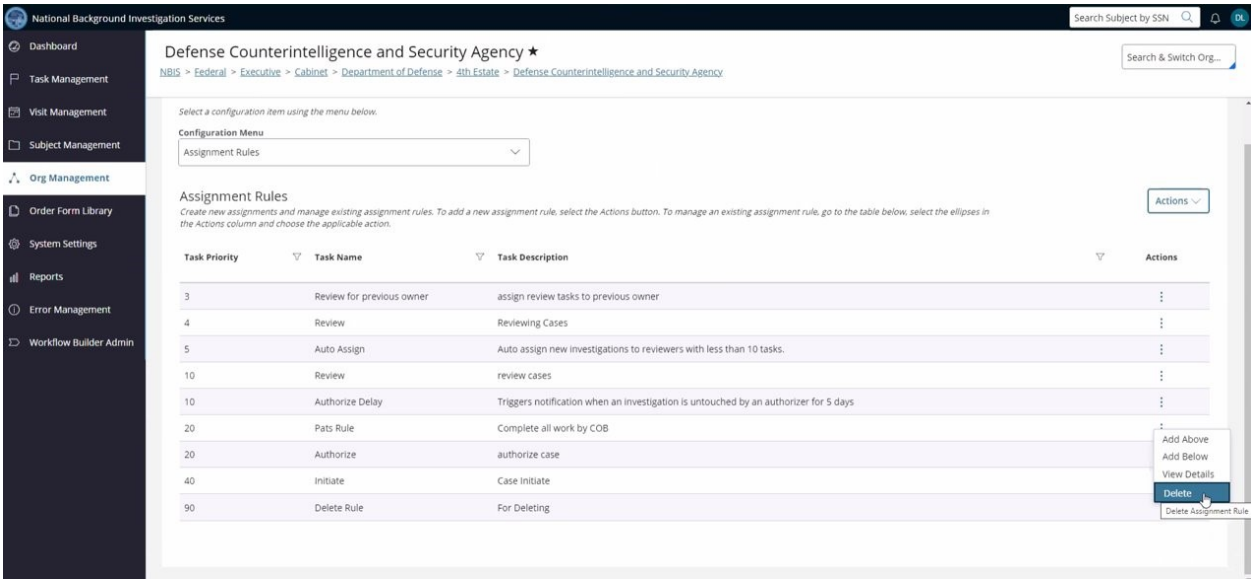
1. From log in, select **Organization Management** from the Navigation Menu on the left. Navigate to your Organization (if needed) then select the **Configuration** tab.
2. Select **Assignment Rules** from the Configuration drop down menu.



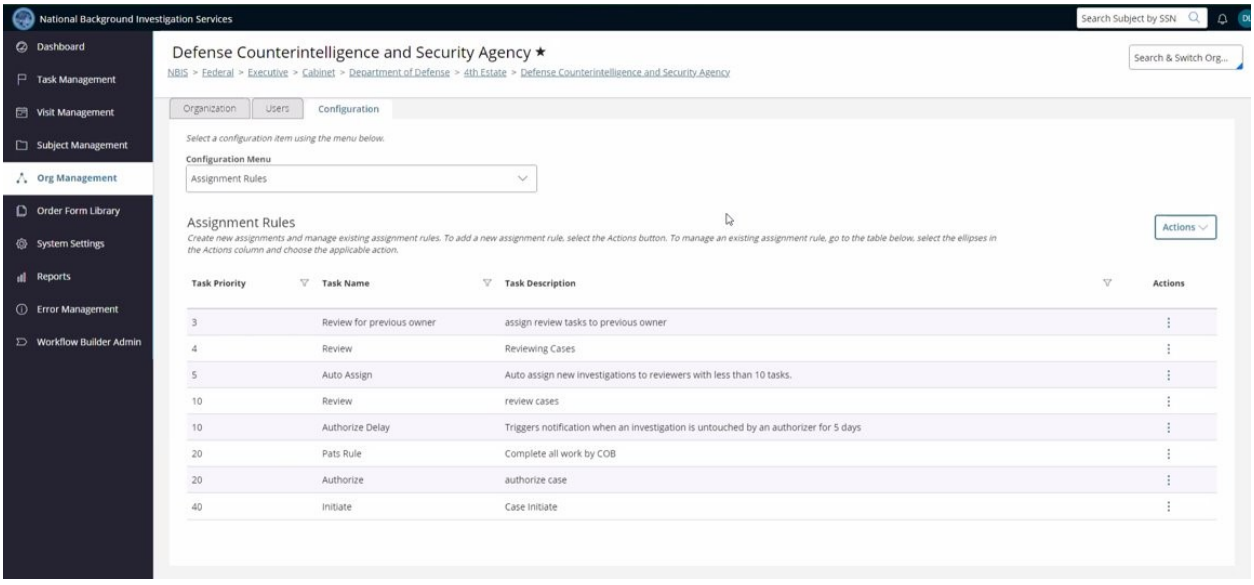
3. The screen will display a prioritized list of existing Assignment Rules; within the list locate the Assignment Rule you want to Delete.

4. In the row of the Assignment Rule that you want to delete, select the **ellipses** under the Actions column.

5. You will be prompted with a mini screen showing four options. Select **Delete** to remove the desired rule.



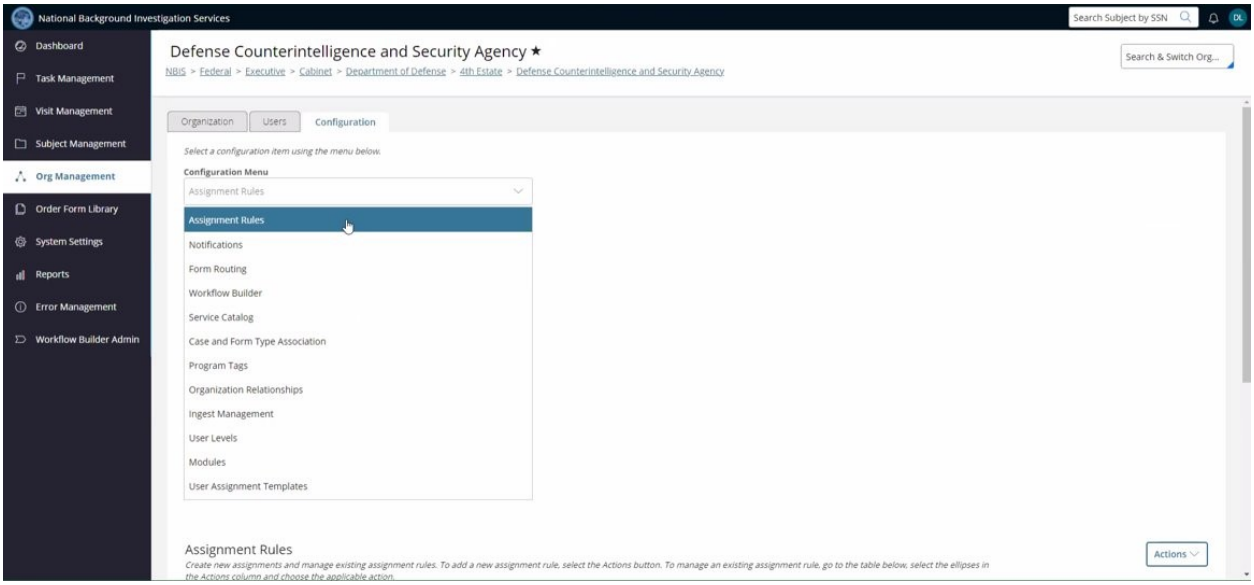
6. Return to the list of existing Assignment Rules. Verify the Assignment Rule was successfully deleted by confirming that it does not appear in the new prioritized list of Assignment Rules.



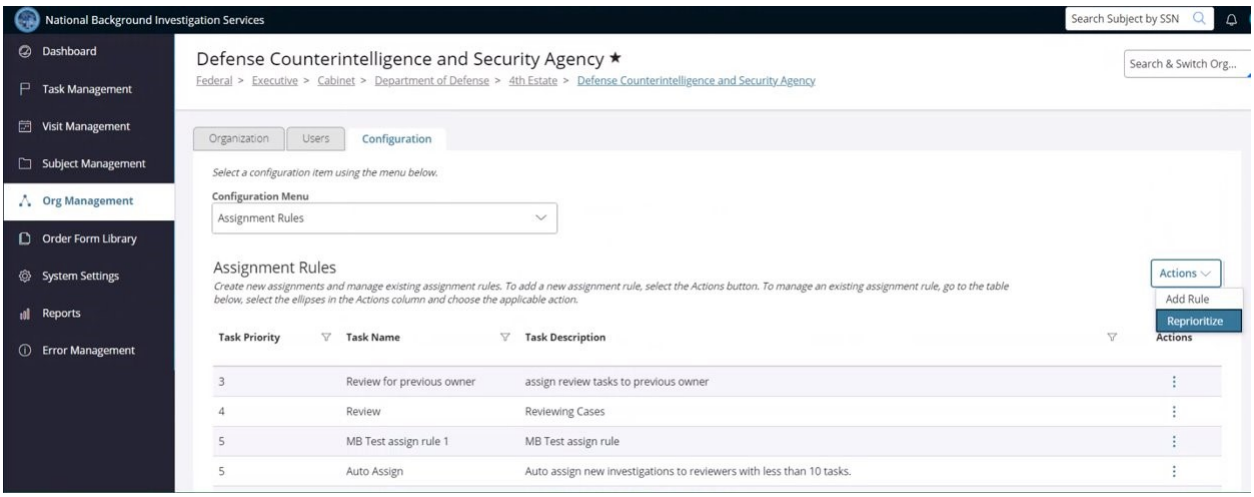
REPRIORITIZE AN ASSIGNMENT RULE

Below is the 5-step process for how to Reprioritize an Assignment Rule.

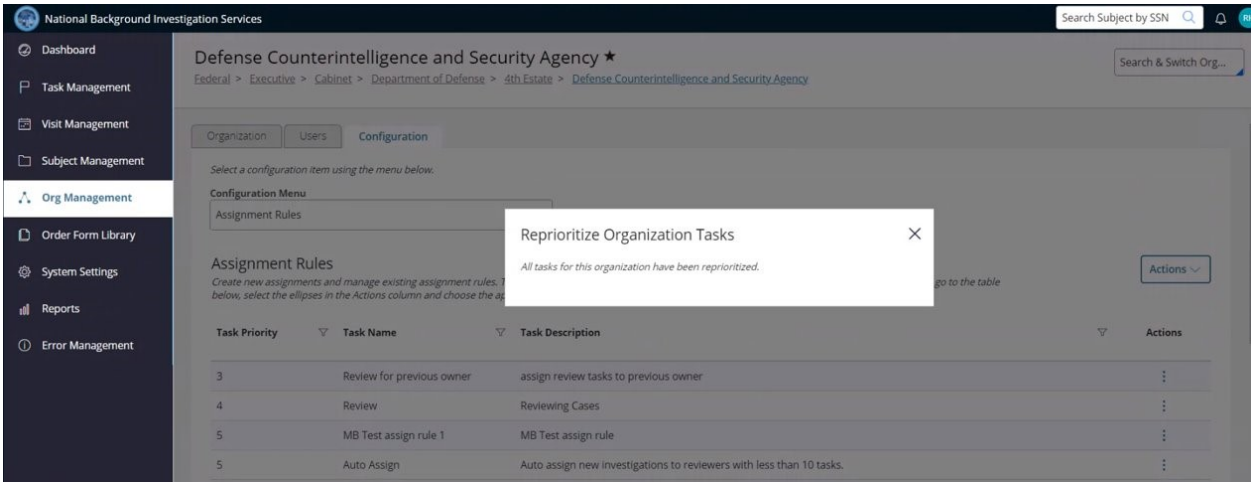
1. From log in, select **Organization Management** from the Navigation Menu on the left. Navigate to your Organization (if needed) then select the **Configuration** tab.
2. Select **Assignment Rules** from the Configuration drop down menu.



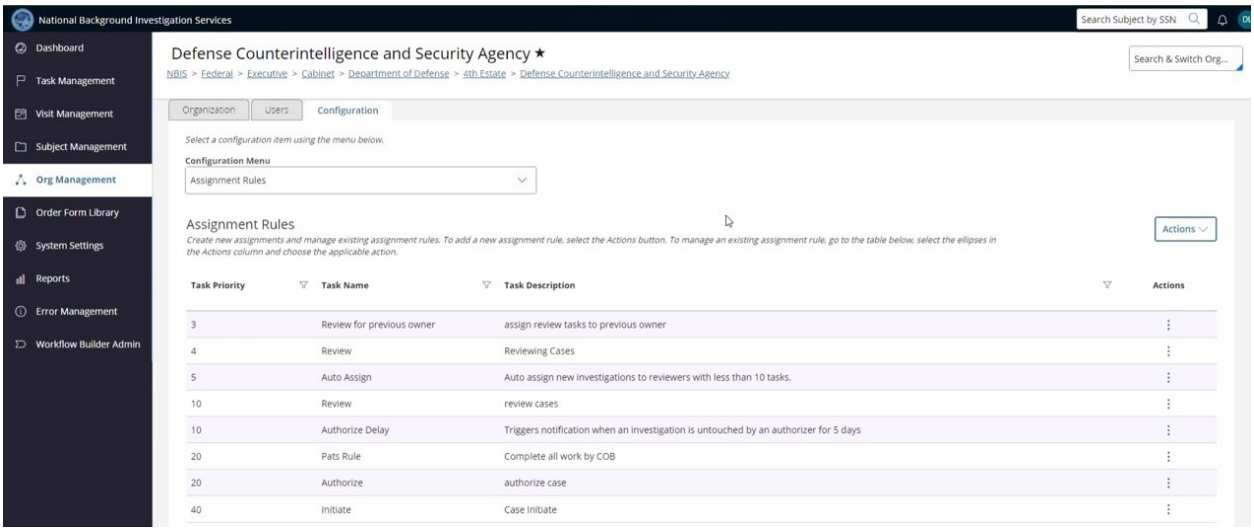
3. Select the **Actions** drop down menu and select **Reprioritize**.



4. Users will then be prompted with a message that confirms that all tasks for this organization have been reprioritized. Select the **X** to close this window.



5. Return to the list of existing Assignment Rules and review the Task Priority to verify the Assignment Rules were successfully reprioritized.



HOW TO CREATE, VIEW, AND EDIT AN ORDER FORM TEMPLATE

Order Form Templates can be configured to fill out some or all of the Order Form information and applied to a Subject's case. Users with the Order Form Template Manager role can manage an existing organization's Order Form Templates from the Order Form Library.

CREATE AN ORDER FORM TEMPLATE

Users with the Template Manager role can manage an organization's Order Form Templates from the Order Form Library. Order Form Templates streamline the review process for filling in some or all of the Order Form Information for the Position Details, Optional Coverage, and Financial Details. When the Order Form Template is selected and applied, it populates information to prevent having to manually enter data for each case request. Below is the 9-step process to Add an Order Form Template.

1. From initial log in, select **Order Form Library** from the left navigation menu
2. Select **the Organization** from the drop-down menu. Alternatively, a user can type into the Organization search box and a list of Orgs will appear. Select the Org name.
3. Select the **"+Add Template" hyperlink** to create/add a new Order Form Template.
4. Enter the **Template Name**.
5. Select **"Only My Organization"** if you do not want the template automatically inherited and used by sub-organizations within your hierarchy.
6. From the Select a **Base Template** drop-down menu choose from an existing parent org's base template, if available. Select either Link or Copy Template option to expedite the template creation process.
   - Linking a template will copy all the base templates values, and these values can only be changed on the new template if changes are made to the respective fields on the base template.
   - Copying a template will copy all the base templates values onto the new template, and those same values can be changed directly from the new template, without affecting the original values on the base template.
7. Manually enter the specific information to include in the template in each tab for the Position Details, Optional Coverage, and Financial Details.
8. Select **save**.
9. The Template will appear under "**Results**" in the Order Form Template list within your organization.

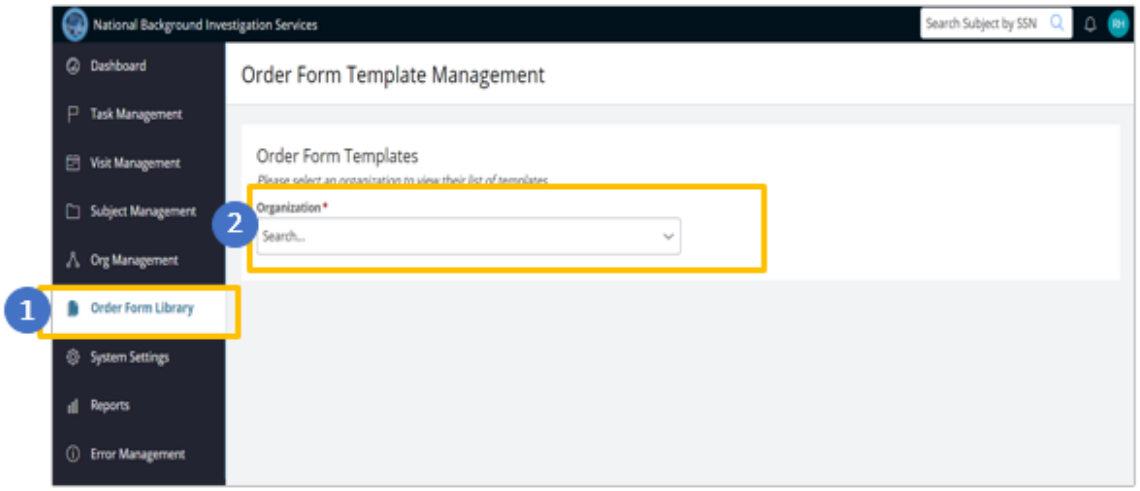
VIEW, EDIT, AND DELETE AN ORDER FORM TEMPLATE

Users with the Template Manager role can manage an existing organization's Order Form Templates from the Order Form Library. Below is the 4-step process to View, Edit, and Delete an Order Form Template.

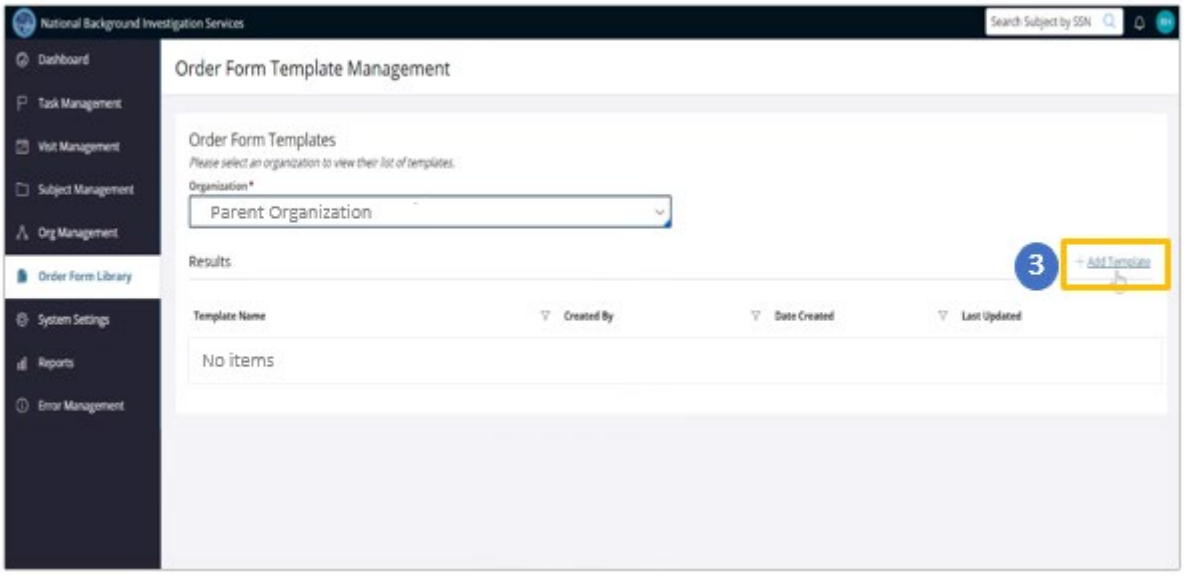
1. From initial log in, select **Order Form Library** from the navigation menu on the left.
2. **Select the Organization** from the drop-down menu. Alternatively, a user can type into the Organization search box and a list of Orgs will appear. Select the Org name.

3. A list of Order Form Templates will populate in the Order Form Library results. Select the **Template Name hyperlink** to view, edit or delete a specific template. To update or edit select Edit, make any changes, and select **Save**. To remove select Delete and Confirm to delete a specific template. Note: If no templates appear in the "Results" section, select the "+Add Template" hyperlink to create an Order Form Template.

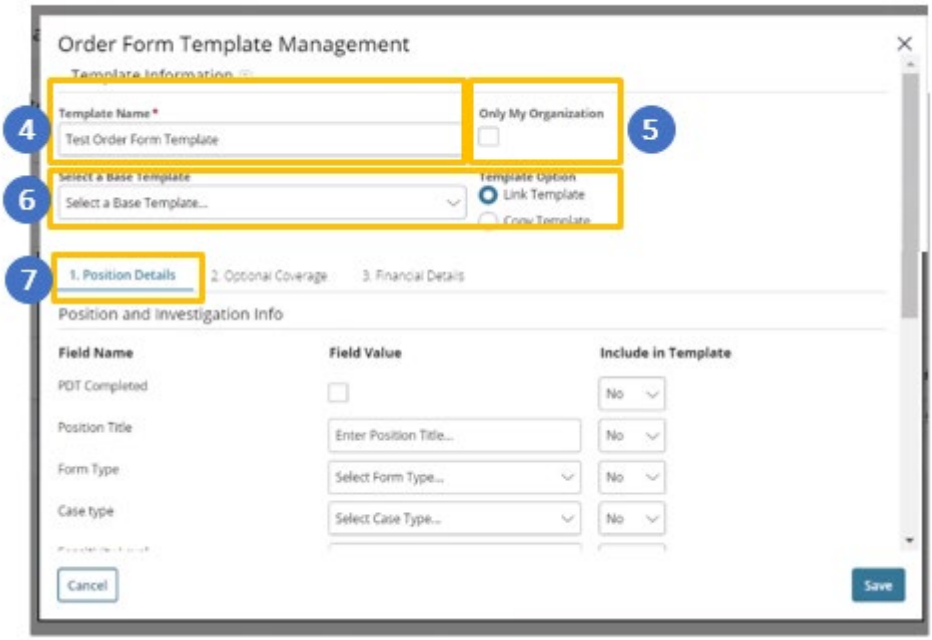
Create an Order Form Template (Steps 1-2)



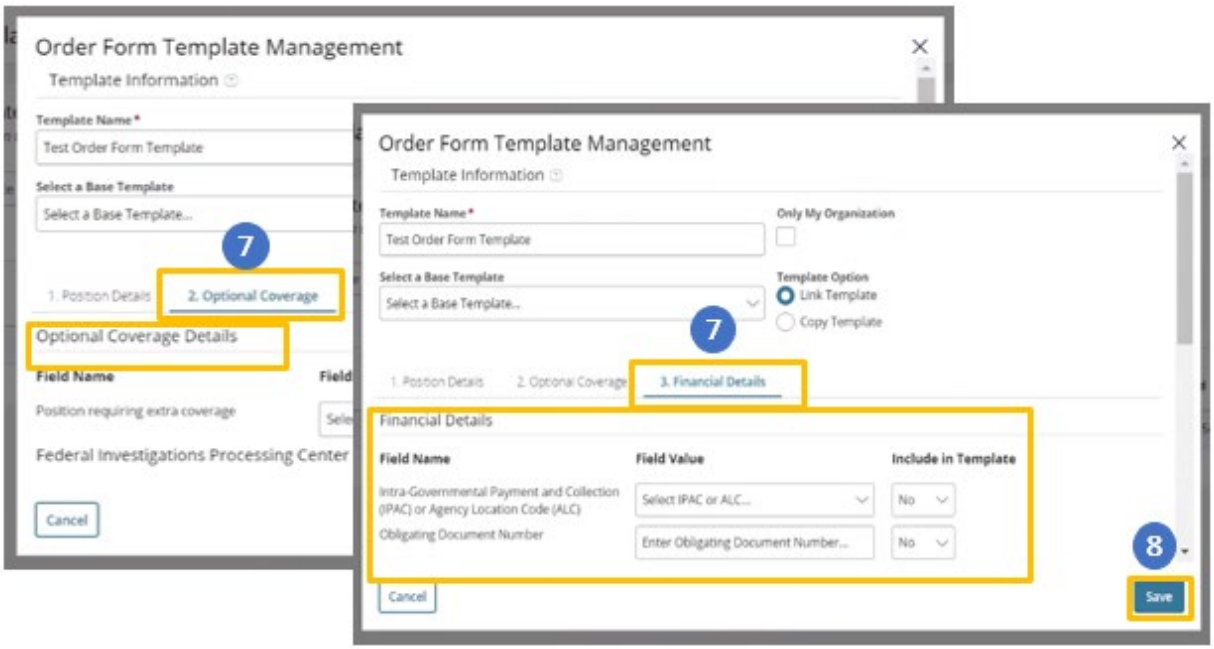
Create an Order Form Template (Step 3)



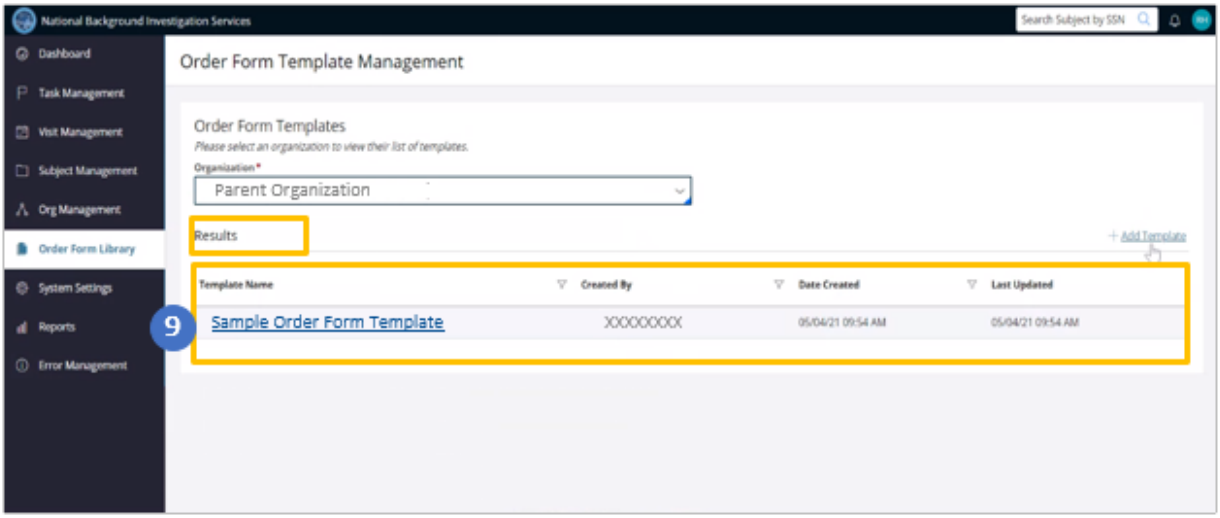
Create an Order Form Template (Steps 4-7)



Create an Order Form Template (Steps 7-8)



Create an Order Form Template (Step 9)

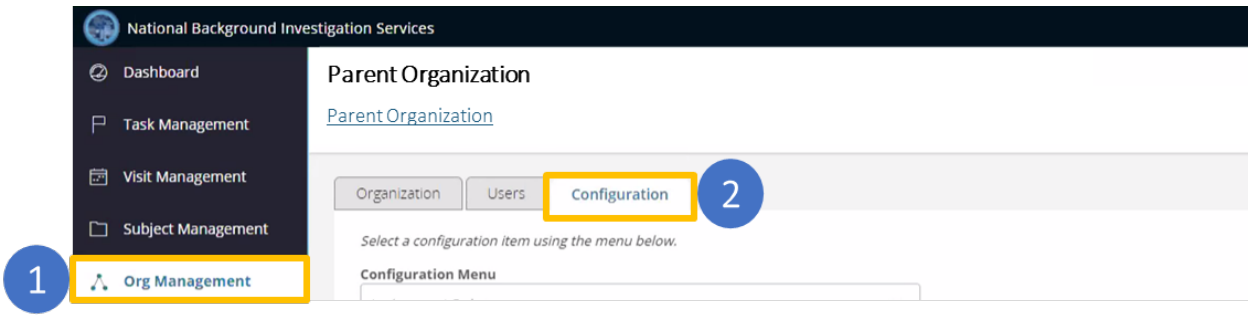


HOW TO VIEW AN ORGANIZATION NOTIFICATION

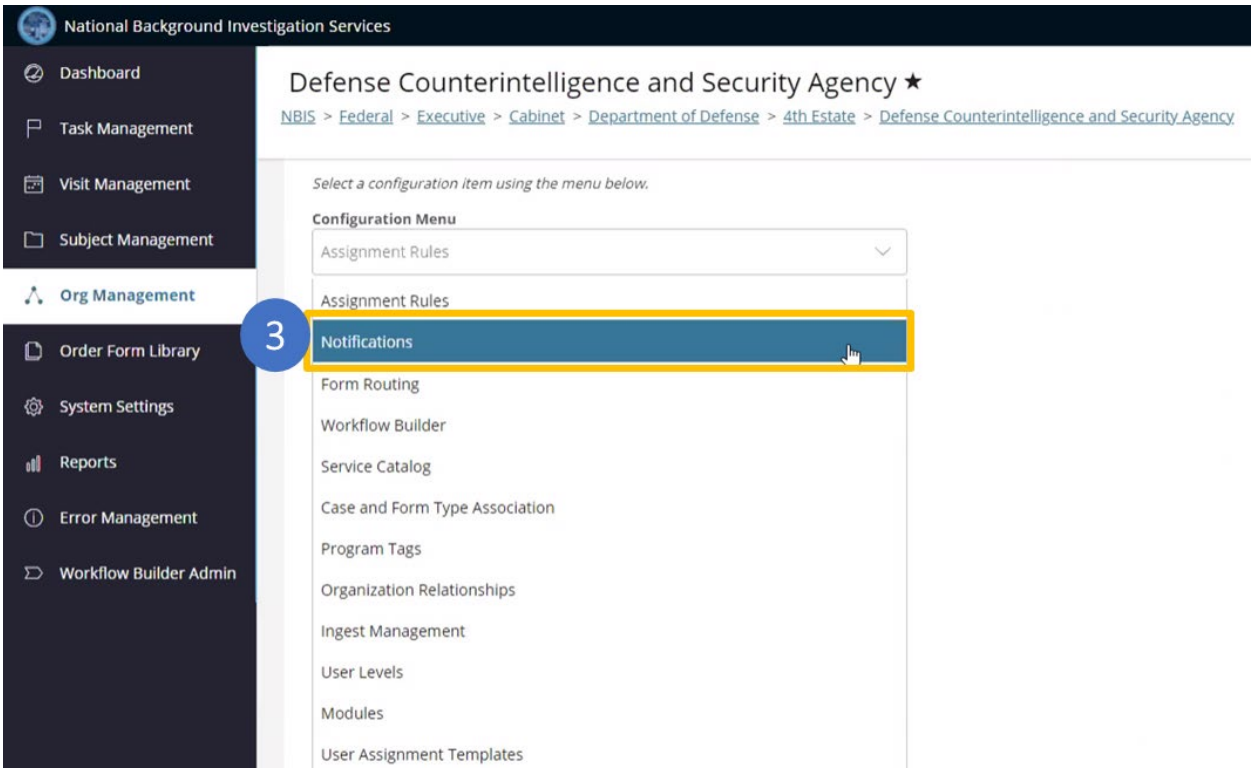
Listed below is the five-step process for how to View Notifications.

1. From initial log in, select **Org Management** from the Navigation Menu on the left.
2. Navigate to your Org (if needed) then select the **Configuration** tab.
3. Select **Notifications** from the Configuration Menu drop-down
4. After selecting Notifications from the drop-down, users will now be able to see the full list of existing notifications for the organization that they are logged into.
5. To view the details of a specific notification, search for and locate that notification using the Notification Name column. Select the **Notification Name** hyperlink to open the details of the selected notification.

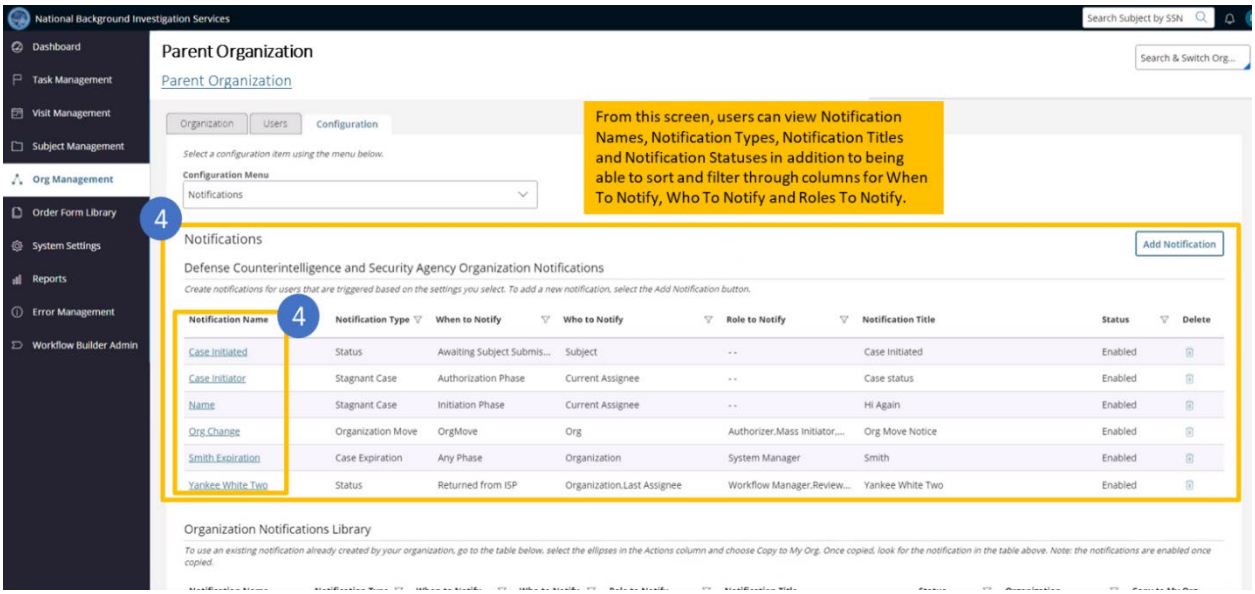
Seps 1-2



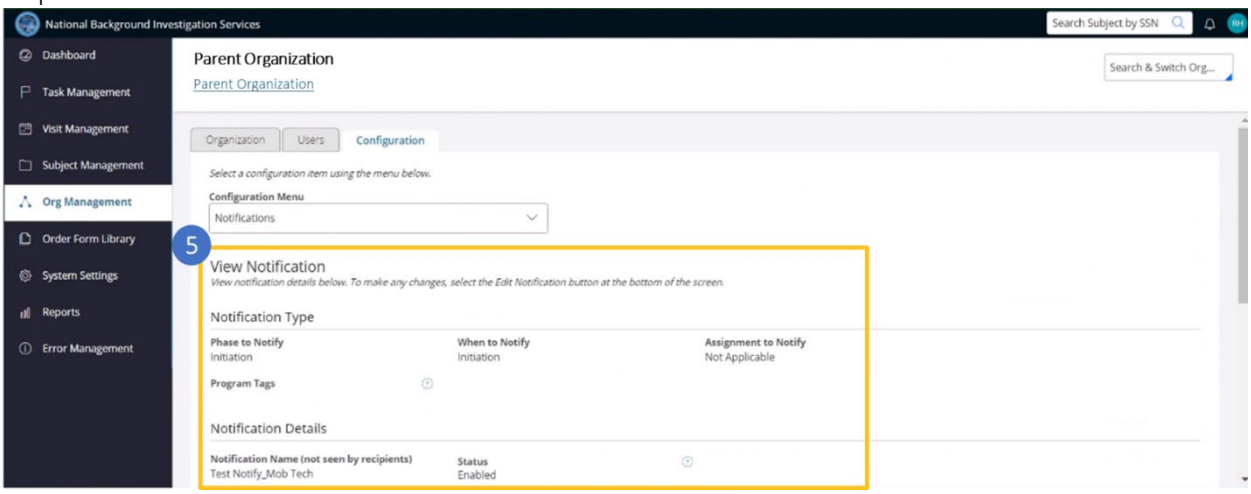
Sep 3


National Background Investigation Services
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
Select a configuration item using the menu below.
Configuration Menu
Assignment Rules
Assignment Rules
3
Notifications
Form Routing
Workflow Builder
Service Catalog
Case and Form Type Association
Program Tags
Organization Relationships
Ingest Management
User Levels
Modules
User Assignment Templates

Sep 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
Parent Organization
Parent Organization
Search & Switch Org...
Organization
Users
Configuration
Select a configuration item using the menu below.
Configuration Menu
Notifications
From this screen, users can view Notification Names, Notification Types, Notification Titles and Notification Statuses in addition to being able to sort and filter through columns for When To Notify, Who To Notify and Roles To Notify.
4
Notifications
Add Notification
Defense Counterintelligence and Security Agency Organization Notifications
Create notifications for users that are triggered based on the settings you select. To add a new notification, select the Add Notification button.
4
Notification Name
Notification Type
When to Notify
Who to Notify
Role to Notify
Notification Title
Status
Delete
Case Initiated
Status
Awaiting Subject Submis...
Subject
--
Case Initiated
Enabled
Case Initiator
Stagnant Case
Authorization Phase
Current Assignee
--
Case status
Enabled
Name
Stagnant Case
Initiation Phase
Current Assignee
--
Hi Again
Enabled
Org Change
Organization Move
OrgMove
Org
Authorizer.Mass Initiator....
Org Move Notice
Enabled
Smith Expiration
Case Expiration
Any Phase
Organization
System Manager
Smith
Enabled
Yankee White Two
Status
Returned from ISP
Organization.Last Assignee
Workflow Manager.Review...
Yankee White Two
Enabled
Organization Notifications Library
To use an existing notification already created by your organization, go to the table below, select the ellipses in the Actions column and choose Copy to My Org. Once copied, look for the notification in the table above. Note: the notifications are enabled once copied.

Step 5

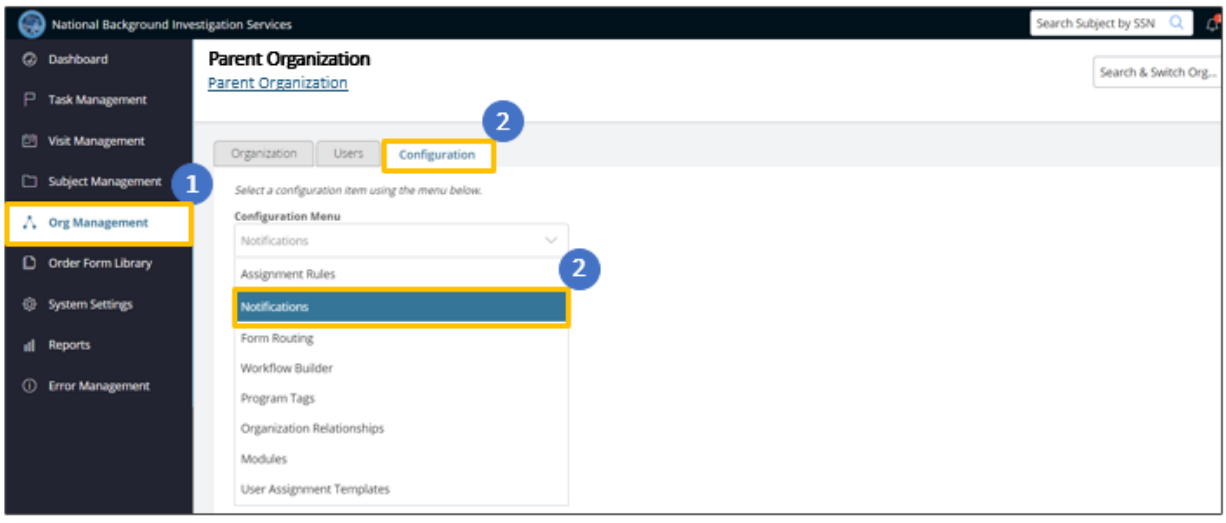

National Background Investigation Services
Search Subject by SSN
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Parent Organization
Parent Organization
Search & Switch Org...
Organization
Users
Configuration
Select a configuration item using the menu below.
Configuration Menu
Notifications
5
View Notification
View notification details below. To make any changes, select the Edit Notification button at the bottom of the screen.
Notification Type
Phase to Notify
Initiation
When to Notify
Initiation
Assignment to Notify
Not Applicable
Program Tags
Notification Details
Notification Name (not seen by recipients)
Test Notify_Mob Tech
Status
Enabled

HOW TO ADD STATUS/ASSIGNMENT NOTIFICATIONS

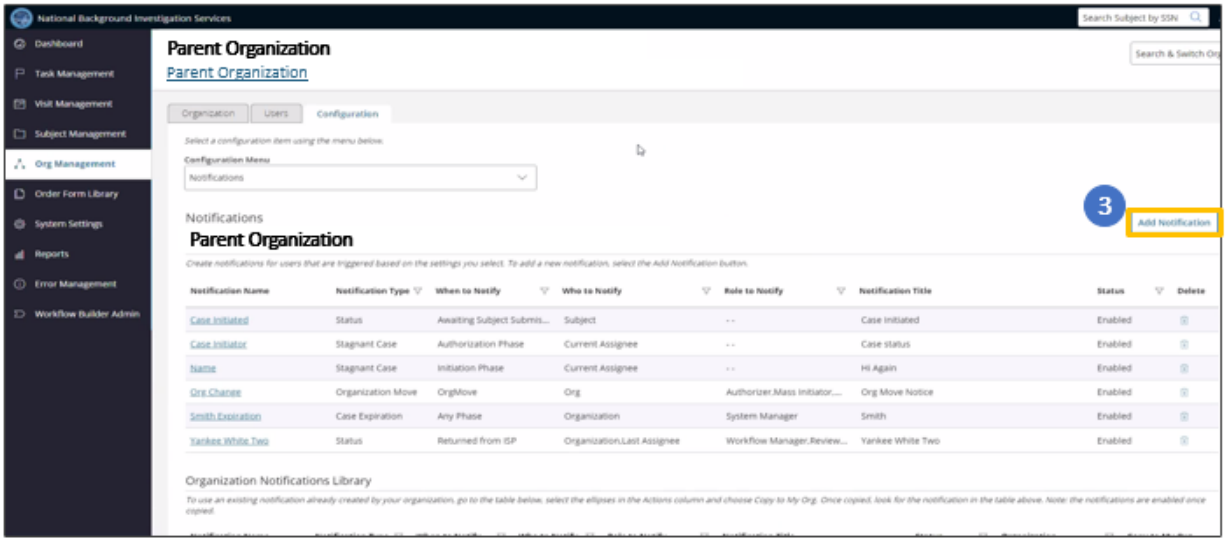
Users with the **Notification Manager role** can add and manage automatic notifications and alerts. Status/Assignment notifications can be created to alert users when the case request moves to a different status within a workflow and when a case is assigned to a user or workbasket depending on the phase. Below is the 8-Step process to Add a Status/Assignment Notification.

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 **Configuration** tab. From the Configuration Menu, select Notifications.
3. To create a new notification, click the Add Notification button on the far-right side of the screen.
4. For the Notification Type, select **Status/Assignment** from the options listed.
5. Select **Phase** to Notify to reveal options from the drop-down menu. Depending on what is selected for Phase to Notify, fields for When to Notify and Assignment to Notify may be required.
6. **When to Notify** chooses the specific status for notifications. Select an option for When to Notify from the drop-down menu. A field for 'Assignment to Notify' may appear depending on what is selected for When to Notify. Select an option for Assignment to Notify if it appears as a required field. Selecting a Program Tag is optional.
7. Users can proceed to **Notification Details**. Enter the Notification Name, make sure the Status box is checked (enabled). Select options for 'Who to Notify' and 'Roles to Notify' using the drop-down menus for each field.
8. Complete Message to Recipients, Title of Notification to Recipients, and Message Text Editor fields. Select **Save and Add**.

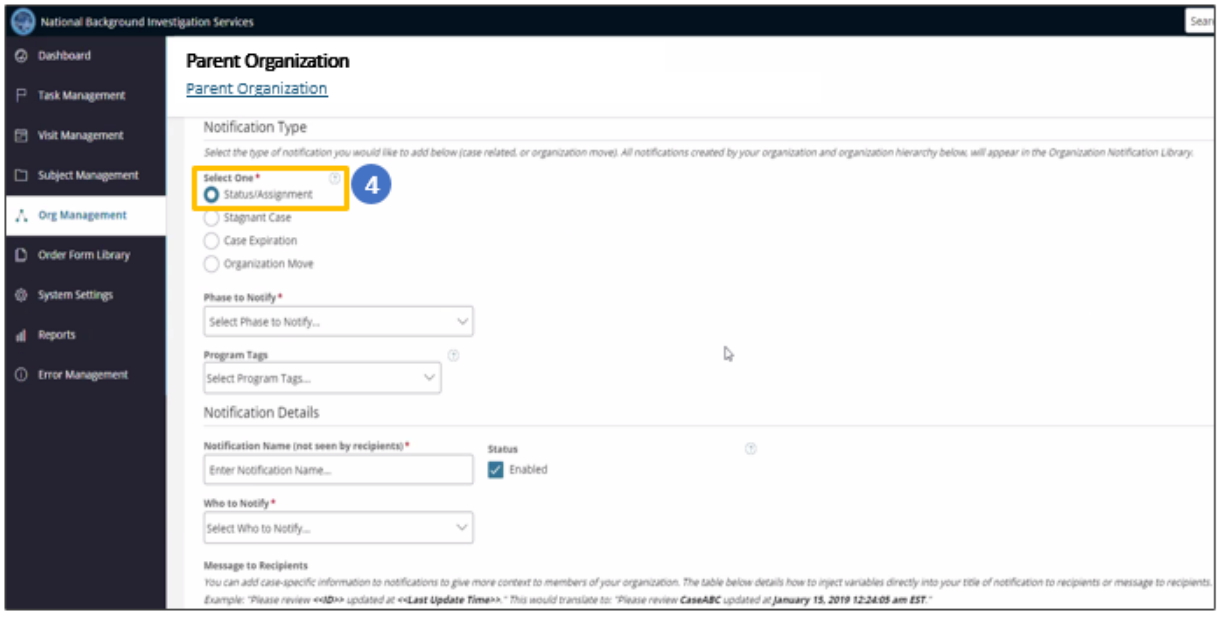
Steps 1-2



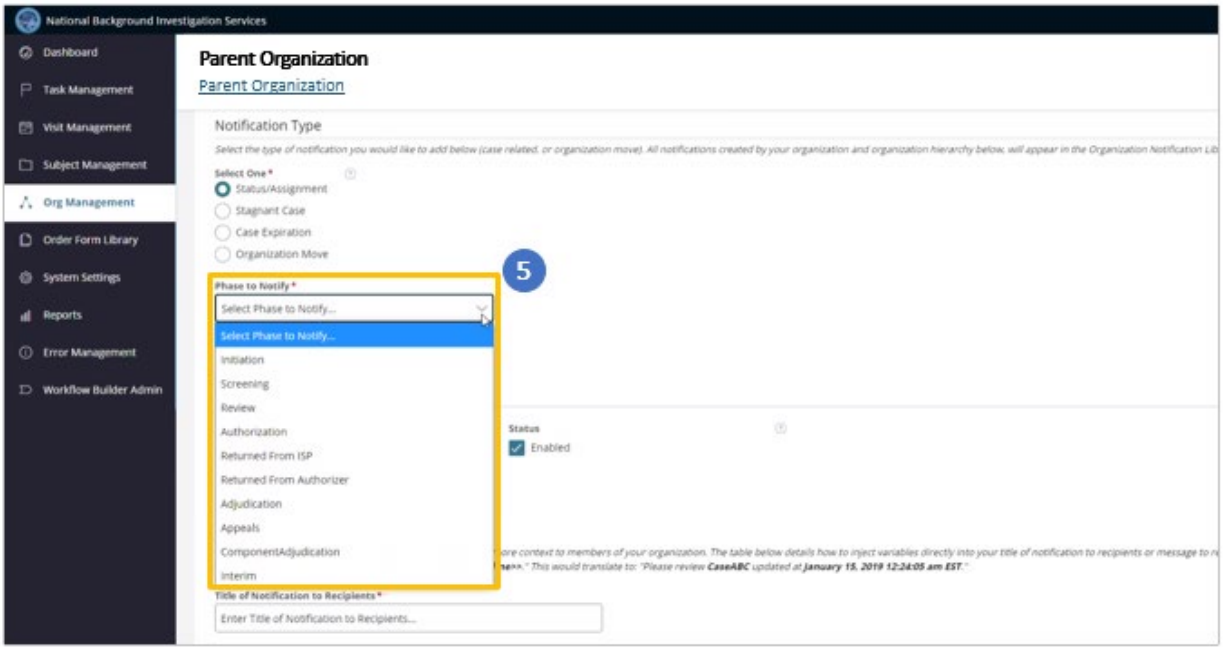
Step 3


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 Organization
Parent Organization
Organization
Users
Configuration
Configuration Menu
Notifications
3
Add Notification
Notifications
Parent Organization
Notification Name
Notification Type
When to Notify
Who to Notify
Role to Notify
Notification Title
Status
Delete
Organization Notifications Library

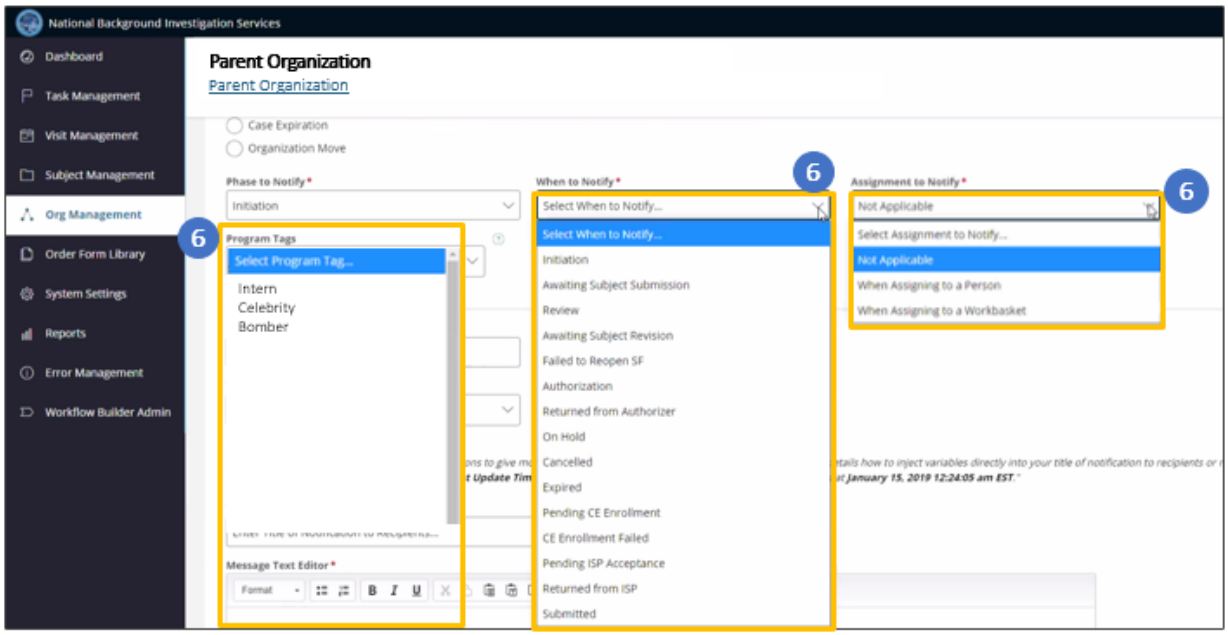
Step 4


National Background Investigation Services
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Parent Organization
Parent Organization
Notification Type
Select One *
Status/Assignment
Stagnant Case
Case Expiration
Organization Move
4
Phase to Notify *
Select Phase to Notify...
Program Tags
Select Program Tags...
Notification Details
Notification Name (not seen by recipients) *
Enter Notification Name...
Status
Enabled
Who to Notify *
Select Who to Notify...
Message to Recipients

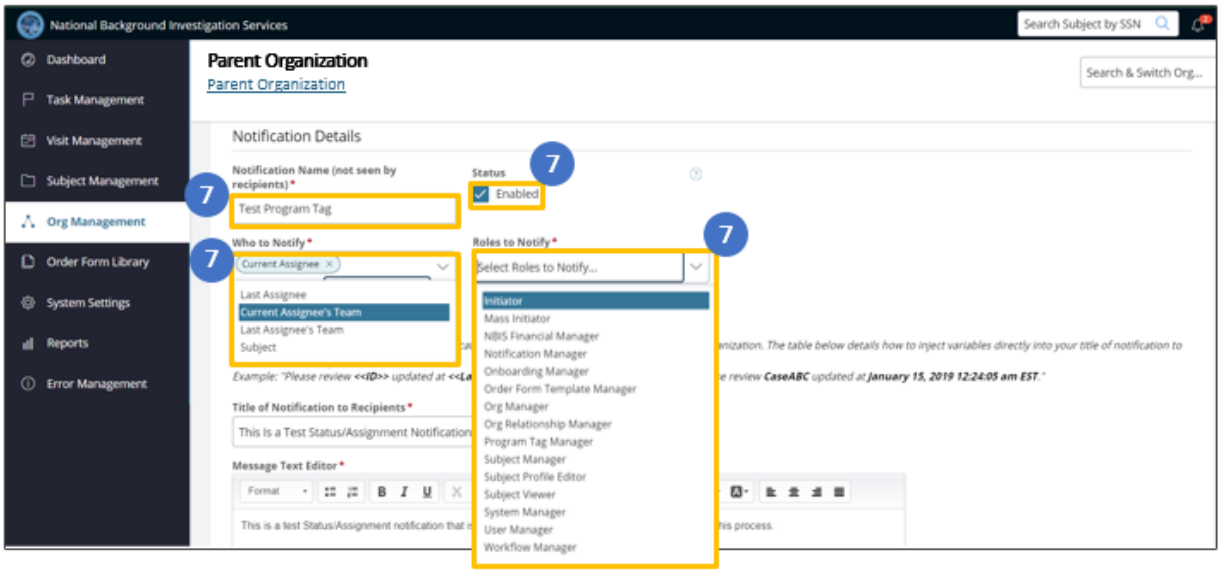
Step 5


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 Organization
Parent Organization
Notification Type
Select One *
Status/Assignment
Stagnant Case
Case Expiration
Organization Move
5
Phase to Notify *
Select Phase to Notify...
Select Phase to Notify...
Initiation
Screening
Review
Authorization
Returned From ISP
Returned From Authorizer
Adjudication
Appeals
ComponentAdjudication
Interim
Status
Enabled
Title of Notification to Recipients *
Enter Title of Notification to Recipients...

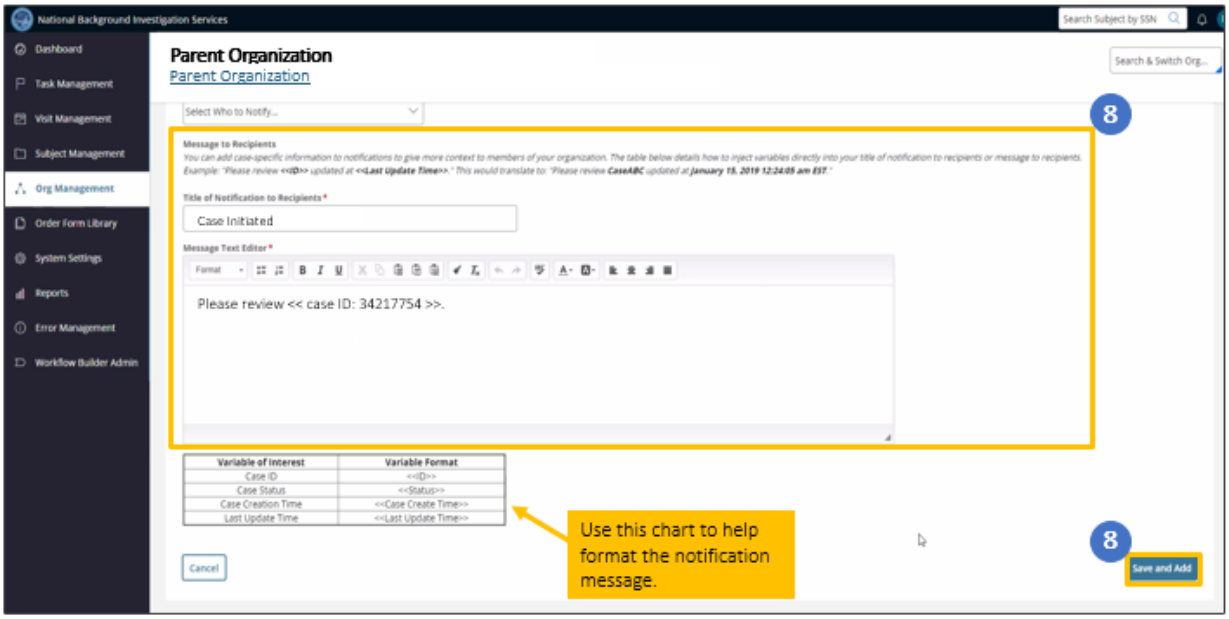
Step 6


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 Organization
Parent Organization
Case Expiration
Organization Move
Phase to Notify *
Initiation
6
When to Notify *
Select When to Notify...
6
Assignment to Notify *
Not Applicable
6
Program Tags
Select Program Tag...
Intern
Celebrity
Bomber
Select When to Notify...
Initiation
Awaiting Subject Submission
Review
Awaiting Subject Revision
Failed to Reopen SF
Authorization
Returned from Authorizer
On Hold
Cancelled
Expired
Pending CE Enrollment
CE Enrollment Failed
Pending ISP Acceptance
Returned from ISP
Submitted
Select Assignment to Notify...
Not Applicable
When Assigning to a Person
When Assigning to a Workbasket
Message Text Editor *

Step 7


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
Parent Organization
Parent Organization
Search & Switch Org...
Notification Details
Notification Name (not seen by recipients)*
Test Program Tag
Status
Enabled
Who to Notify*
Current Assignee
Last Assignee
Current Assignee's Team
Last Assignee's Team
Subject
Roles to Notify*
Select Roles to Notify...
Initiator
Mass Initiator
NBIS Financial Manager
Notification Manager
Onboarding Manager
Order Form Template Manager
Org Manager
Org Relationship Manager
Program Tag Manager
Subject Manager
Subject Profile Editor
Subject Viewer
System Manager
User Manager
Workflow Manager
Title of Notification to Recipients*
Message Text Editor*
7

Step 8

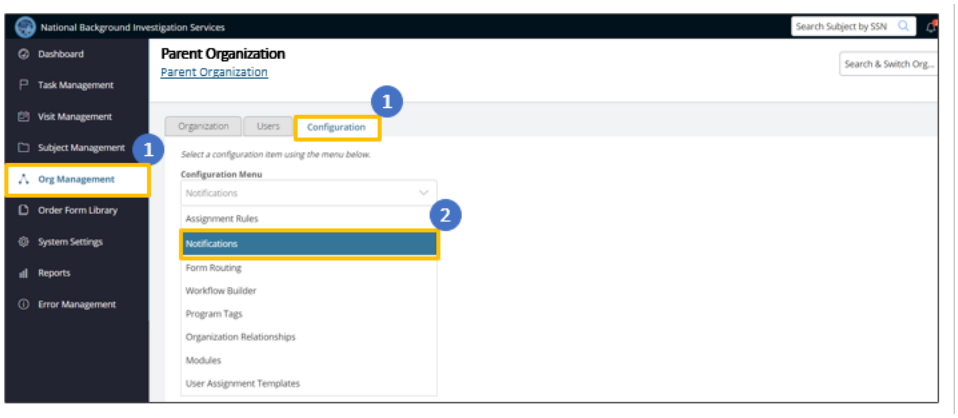

National Background Investigation Services
Search Subject by SSN
Parent Organization
Parent Organization
Search & Switch Org...
Select Who to Notify...
Message to Recipients
Title of Notification to Recipients*
Case Initiated
Message Text Editor*
Please review << case ID: 34217754 >>.
Variable of Interest
Variable Format
Case ID
<<ID>>
Case Status
<<Status>>
Case Creation Time
<<Case Create Time>>
Last Update Time
<<Last Update Time>>
Use this chart to help format the notification message.
Cancel
Save and Add
8

HOW TO ADD STAGNANT CASE NOTIFICATIONS

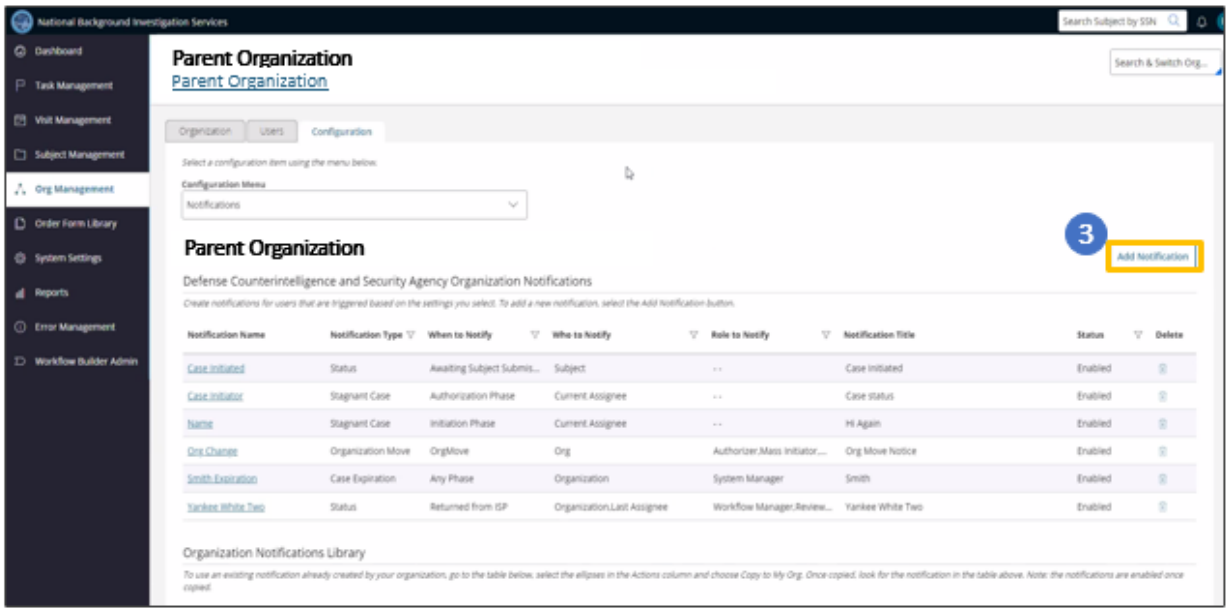
Users with the **Notification Manager role** can add and manage automatic notifications and alerts. Stagnant Case Notifications can be configured to alert users when no action has been taken on a case or when a case request has been delayed in a certain phase for a specific amount of time. Within each Stagnant Case notification, users have the option to schedule 3 instances of notifications (1st, 2nd, and 3rd notifications).

1. From initial log in, access the **Org Management** tab from the navigation menu on the left. Switch to the designated Org (if needed) and select the Configuration tab.
2. Click the arrow within the Configuration Menu to reveal the drop-down options and select **Notifications**.
3. To create a new notification, click the **Add Notification** button on the far-right side of the screen.
4. For the Notification Type, select **Stagnant Case** from the options provided.
5. Select an option for the "Phase to Notify" and "When to Notify" fields. It is optional to select a Program Tag.
6. Proceed to **Notification Details**. Enter a Notification Name by typing into the Notification Name field. Enabled is automatically checked for the Status. If unchecked, the notification will not be sent.
7. For the **first notification reminder**, click the arrow in the "Who to Notify" field and select an option from the choices provided. If "Organization" is selected for the 1st, 2nd or 3rd notification reminder, users will be required to select options for the "Roles to Notify" field. Enter a numerical value for the "Days Before Notification" field to specify the amount of time the case can be stagnant before the notification is sent.
8. For the **second notification reminder**, click the arrow in the "Who to Notify" field and select an option from the choices provided. Enter a numerical value for the "Days After First Notification" field. If configuring the third notification reminder, it is pre-set to send the notification every 15 days for a maximum of 4 times, or until the case is moved out of the specific phase.
9. Proceed to the **Message to Recipients** section. This will enable case-specific information for notifications to provide more details to the members of the organization. Add a title for the "Title of Notification to Recipients" field.
10. Include a message in the "**Message Text Editor**." The table shows how to use variables within the Title of Notification or Message Text Editor fields. Select **Save and Add**.

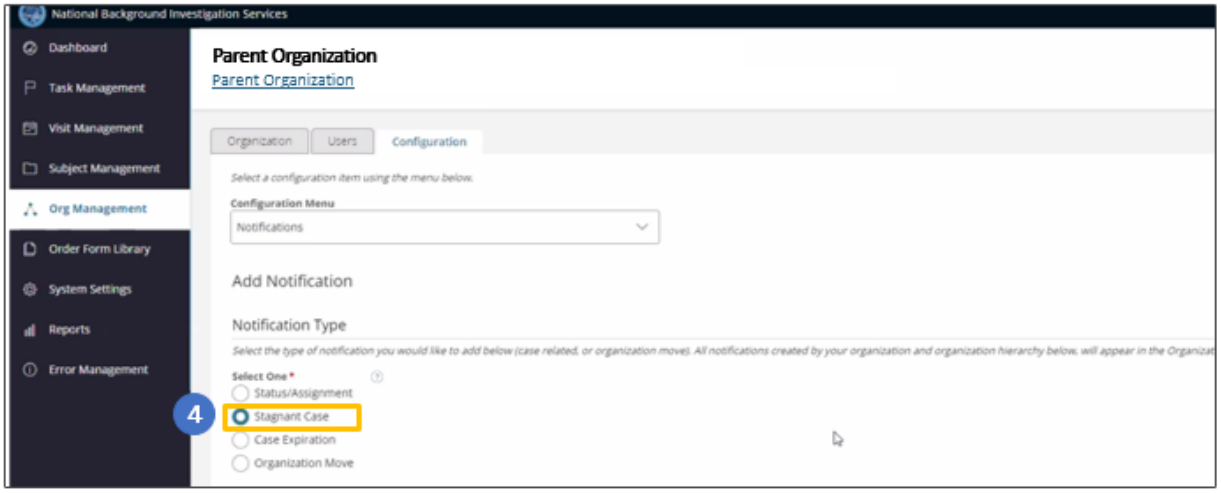
Steps 1-2



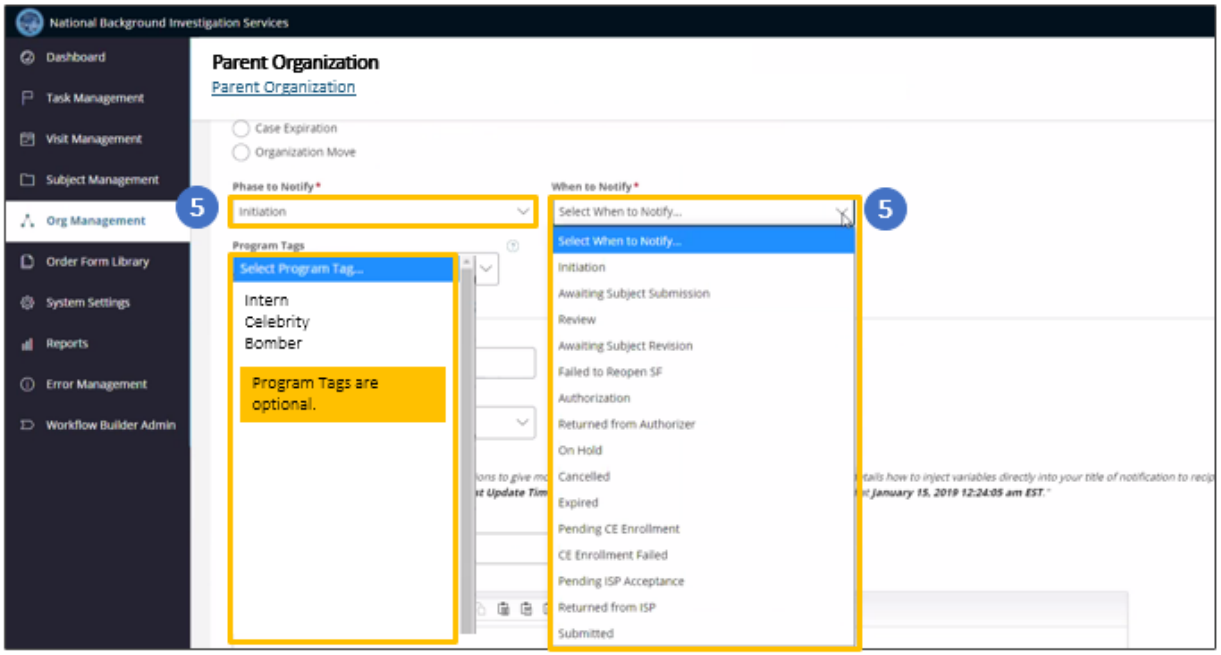
Step 3



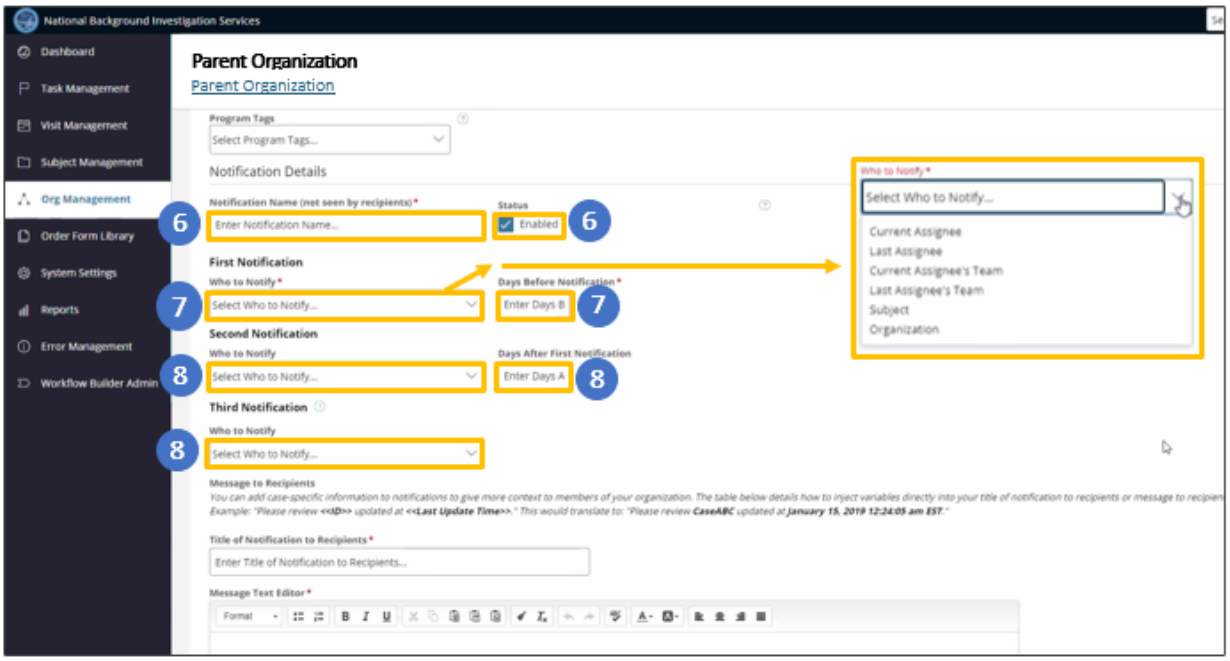
Step 4


National Background Investigation Services
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Parent Organization
Parent Organization
Organization
Users
Configuration
Select a configuration item using the menu below.
Configuration Menu
Notifications
Add Notification
Notification Type
Select the type of notification you would like to add below (case related, or organization move). All notifications created by your organization and organization hierarchy below, will appear in the Organizat
Select One *
Status/Assignment
Stagnant Case
Case Expiration
Organization Move
4

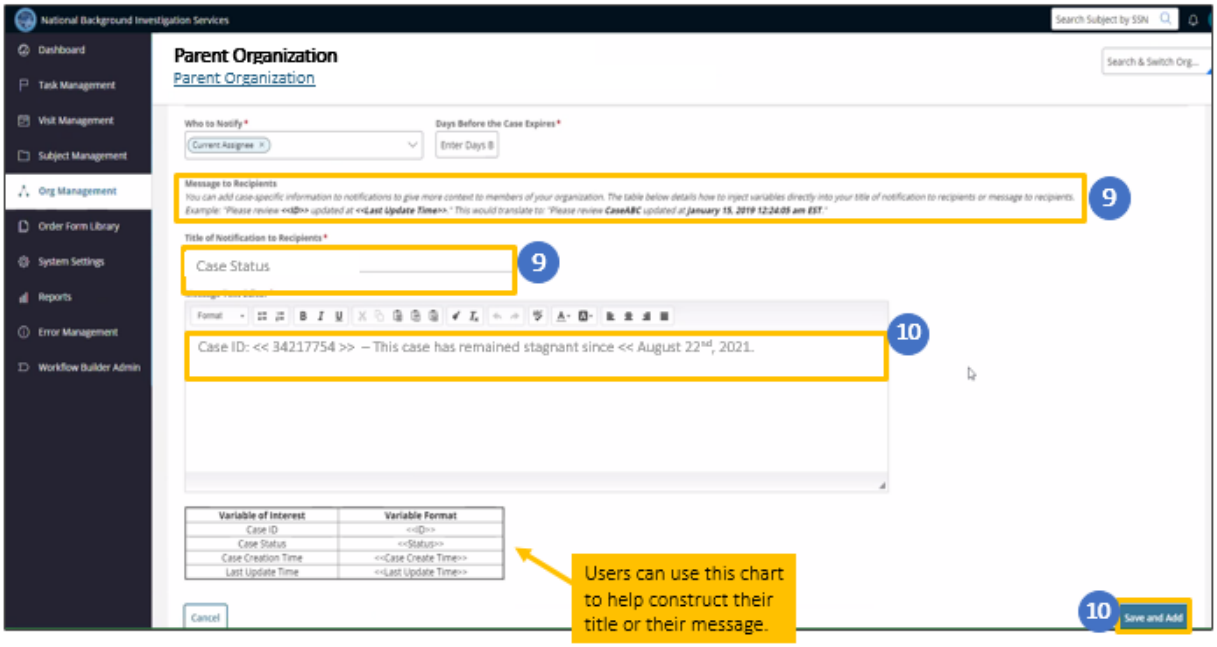
Step 5


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 Organization
Parent Organization
Case Expiration
Organization Move
Phase to Notify *
Initiation
5
When to Notify *
Select When to Notify...
5
Program Tags
Select Program Tag...
Intern
Celebrity
Bomber
Program Tags are optional.
Select When to Notify...
Initiation
Awaiting Subject Submission
Review
Awaiting Subject Revision
Failed to Reopen SF
Authorization
Returned from Authorizer
On Hold
Cancelled
Expired
Pending CE Enrollment
CE Enrollment Failed
Pending ISP Acceptance
Returned from ISP
Submitted

Steps 6-8



Steps 9-10

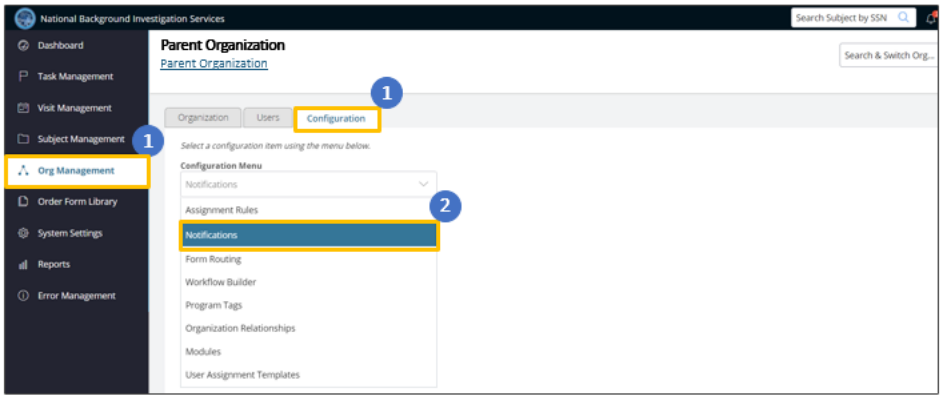


HOW TO ADD CASE EXPIRATION NOTIFICATIONS

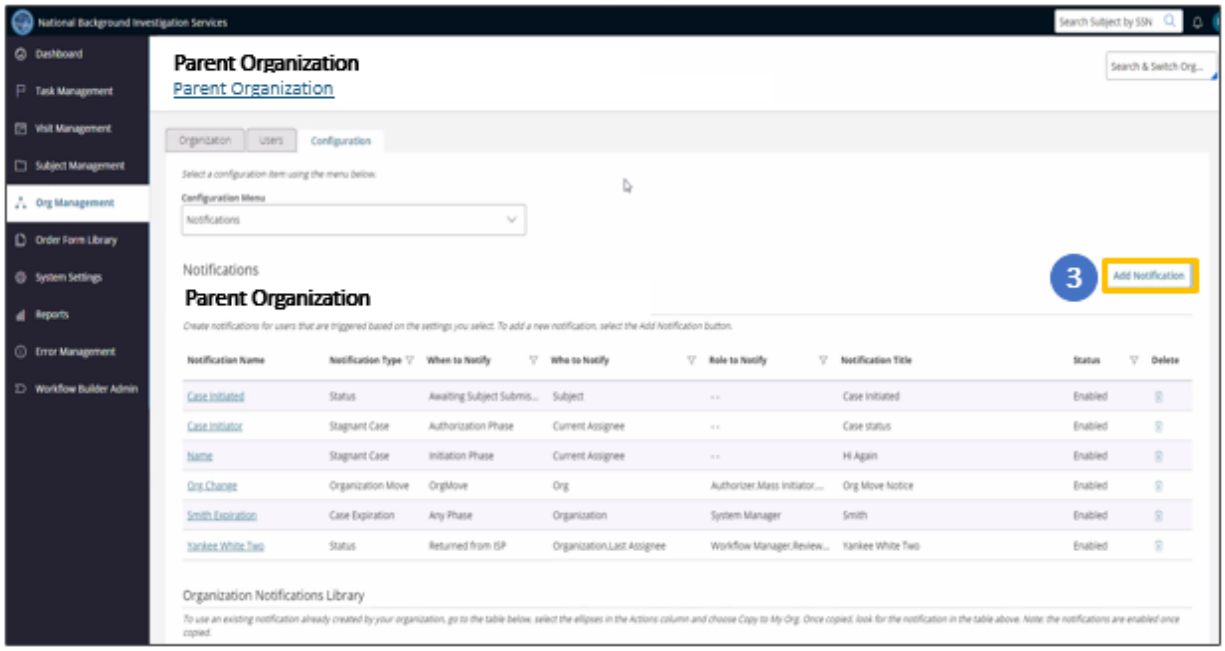
Users with the **Notification Manager role** can add and manage automatic notifications and alerts. Case Expiration Notifications set the timing for how long cases remain active after the Standard Form (SF) is received in the system. Users can send a case expiration reminder by entering the number of days a reminder will be sent before the case expiration.

1. From log in select **Org Management**. Switch to the designated Org (if needed) then select the Configuration tab.
2. Click the arrow within the Configuration Menu to reveal the drop-down options and select **Notifications**.
3. To create a new notification, click the **Add Notification** button on the far-right side of the screen.
4. For the Notification Type, select **Case Expiration** from the options provided.
5. Enter a **Notification Name**. Make sure Enabled is checked for the Status. If unchecked, the notifications will not be sent.
6. For "Who to Notify" and "Roles to Notify," select option(s) from the drop-down menu.
7. Enter the number of days a case can be active in the "Days for the Case Expiration and Notification" field.
8. Add a "Title of Notification to Recipients" and a "Message to Recipients."
9. Select **Save and Add**.

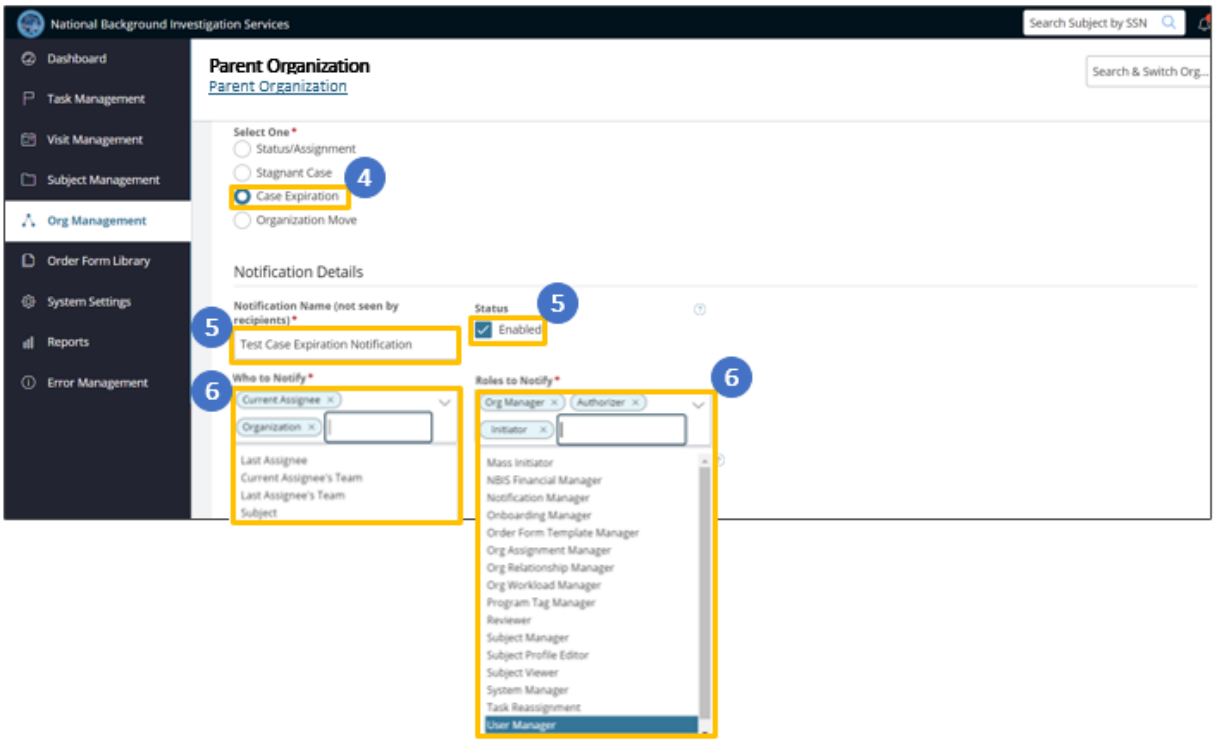
Steps 1-2



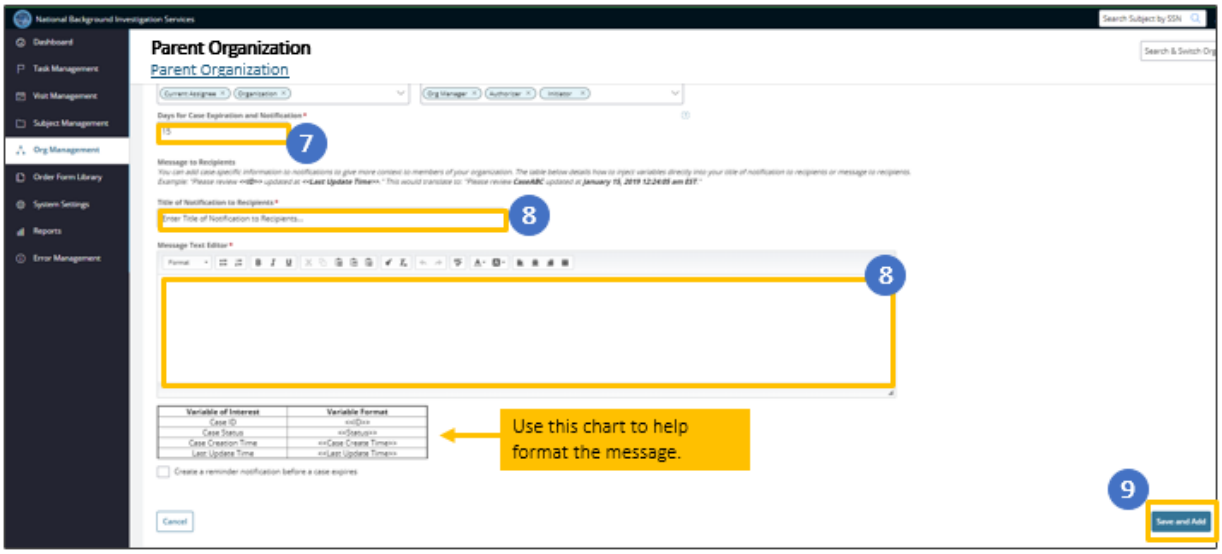
Step 3



Steps 4-6



Steps 7-9

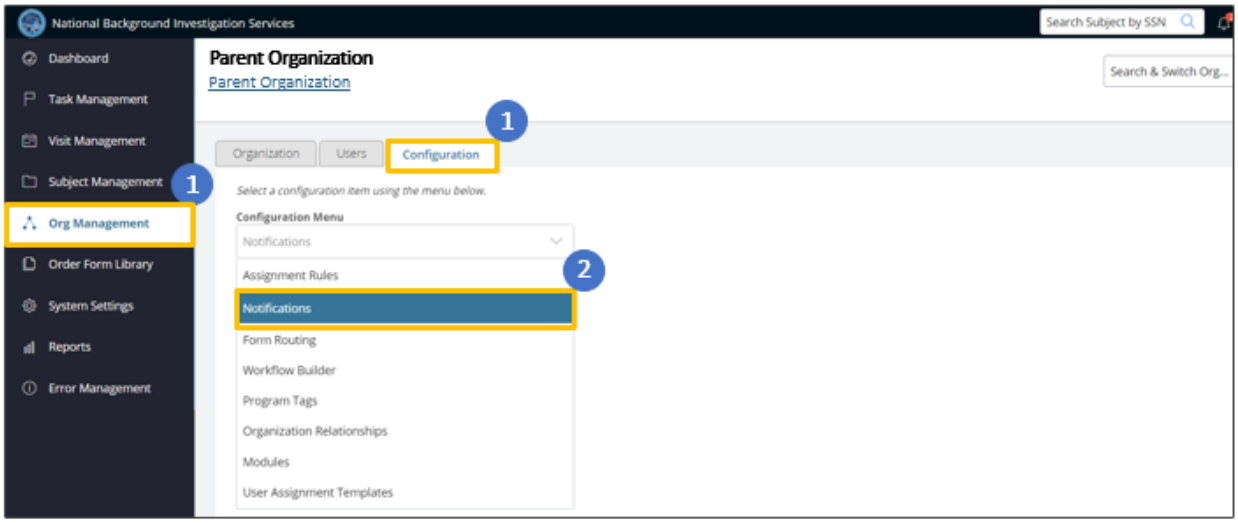

Parent Organization
Parent Organization
7
8
8
Use this chart to help format the message.
9
Cancel
Save and Add

HOW TO ADD AN ORGANIZATION MOVE/MIGRATION NOTIFICATION

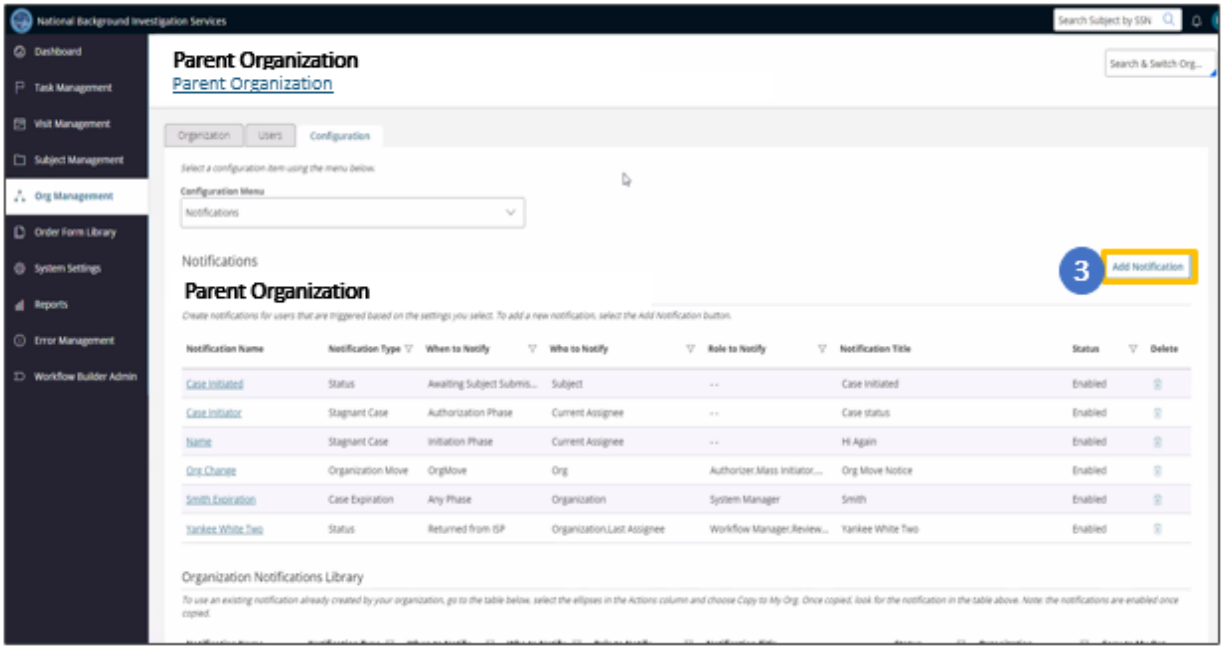
Users with the **Notification Manager role** can add and manage automatic notifications and alerts. Organization Move/Migration Notifications are utilized to alert users when a team or an organization is moved internally or externally. If the notifications feature is enabled, a notification will be sent as an alert to users when a team or an organization is moved internally or externally. For External Organization Migrations, notifications will automatically be sent out to affected Organizations. Users with the Organization Manager role of the losing Organization (parent of migration Organization) and users in the migrating and gaining Organizations will be notified. Below is the 8-Step process to Add a Move/Migration Notification.

1. From login, select **Org Management**. Switch to the designated Org (if needed) then select the Configuration tab.
2. Click the arrow within the Configuration Menu to reveal the drop-down options and select **Notifications**.
3. To create a new notification, click the **Add Notification** button on the far-right side of the screen.
4. Select **Organization Move** as the notification type and enter the Notification Name.
5. Make sure Enabled is checked for the Status, if unchecked, the notification will not be sent.
6. Choose either “A Team is Moved,” or “An Organization is Moved” from the “When to Notify” drop-down menu.
7. If “A Team is Moved” is selected for the When to Notify field, then select either (1) Team or (2) Organization from the “Who to Notify” drop-down menu.
8. If “An Organization is Moved” is selected from the When to Notify field, then Organization will automatically be selected under “Who to Notify.”
9. After users have selected an option for Who to Notify, the “Roles to Notify” drop-down menu will populate. Users with the Notification Manager role can select specific roles within the organization to be notified or every role within the organization to be notified.
10. Add a “Message to Recipients.” This will allow case-specific information for notifications in order to provide more details to the members of a user’s organization.
11. Add “Title of Notification to Recipients” and include a message in the Message Text Editor.
12. Select **Save and Add**.

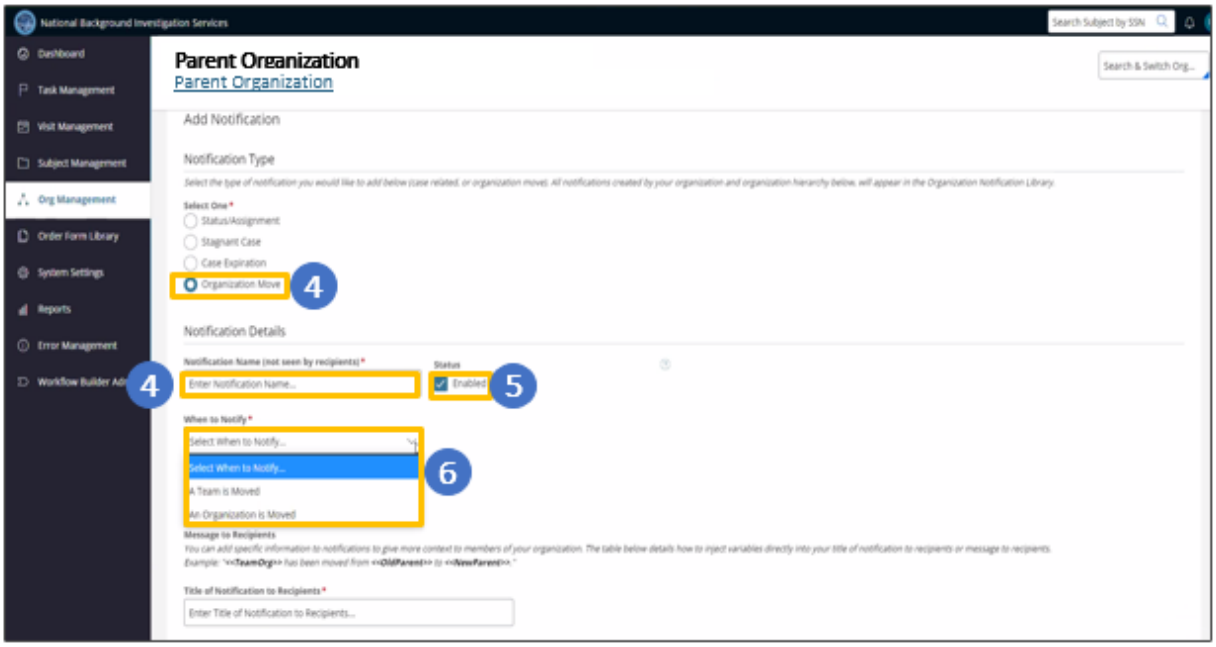
Steps 1-2



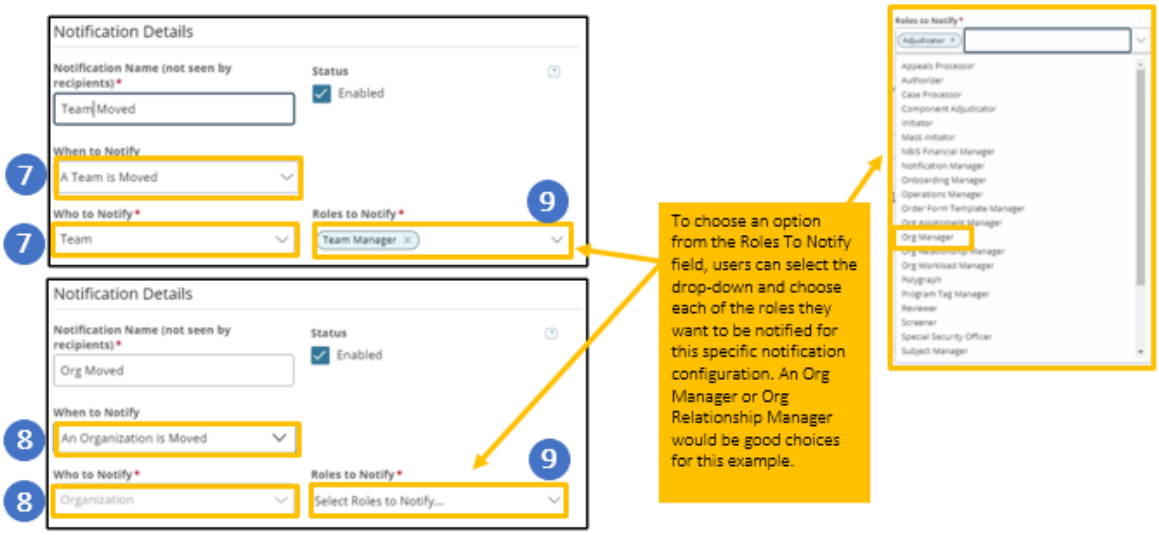
Step 3



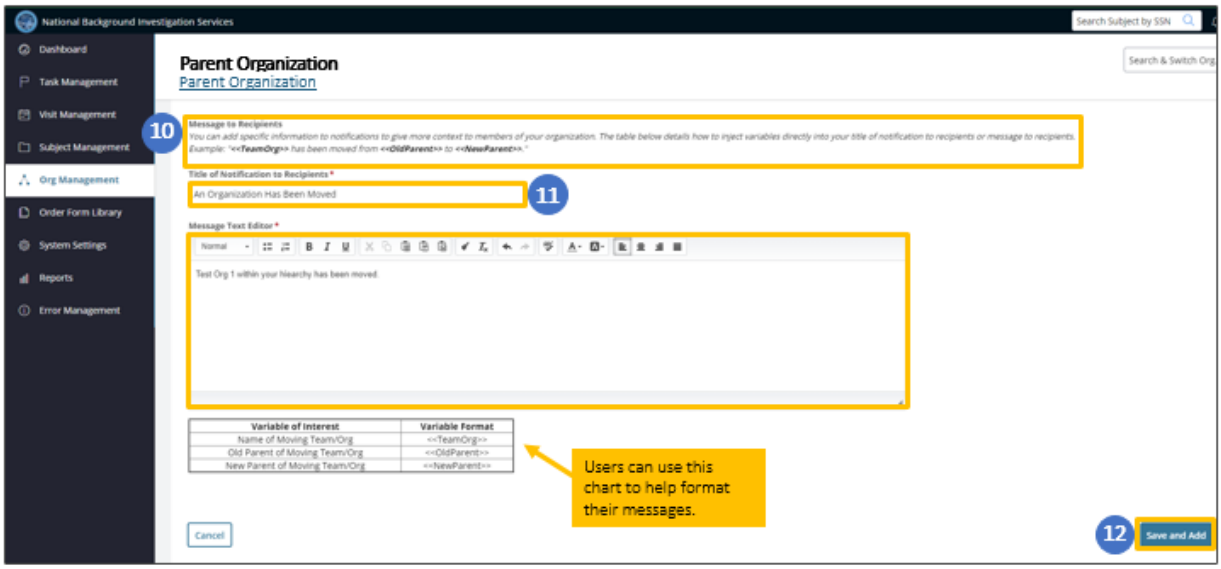
Steps 4-6



Steps 7-9



Steps 10-12


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
Parent Organization
Parent Organization
Search & Switch Org
10
Message to Recipients
You can add specific information to notifications to give more context to members of your organization. The table below details how to inject variables directly into your title of notification to recipients or message to recipients.
Example: "<<TeamOrg>> has been moved from <<OldParent>> to <<NewParent>>."
Title of Notification to Recipients*
An Organization Has Been Moved
11
Message Text Editor*
Normal
Test Org 1 within your hierarchy has been moved
Variable of Interest
Variable Format
Name of Moving Team/Org
<<TeamOrg>>
Old Parent of Moving Team/Org
<<OldParent>>
New Parent of Moving Team/Org
<<NewParent>>
Users can use this chart to help format their messages.
Cancel
12
Save and Add

HOW TO MANAGE ORG NOTIFICATIONS

HOW TO COPY A NOTIFICATION

1. From initial log in, select **Organization Management** from the Navigation Menu on the left.
2. Navigate to your organization (if needed) then select the **Configuration** tab.
3. Select **Notifications** from the Configuration Menu drop-down.
4. After selecting Notifications from the drop-down, users will now be able to see the full list of existing notifications for the organization that they are logged into.
5. Scroll down to the Organization Notifications Library section. Locate the notification you want to copy to your organization and select the "**Copy to My Organization"** button to add that notification to the Organization you are signed into.
6. Scroll back up to view the list of existing notifications for the Organization that you are signed into. You should now see the notification that you copied within the list of existing notifications for your organization.

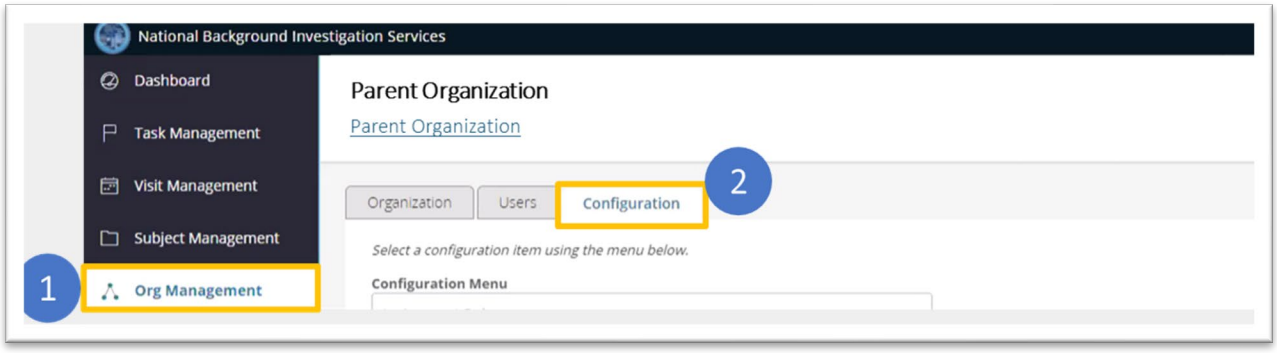
How to Delete a Notification

1. From initial log in, select **Organization Management**. from the Navigation Menu on the left.
2. Navigate to your Organization (if needed) then select the **Configuration** tab.
3. Select **Notifications** from the Configuration Menu drop down to view all existing Notifications.
4. Select the **trash can** icon in the Delete column to delete any existing notification.

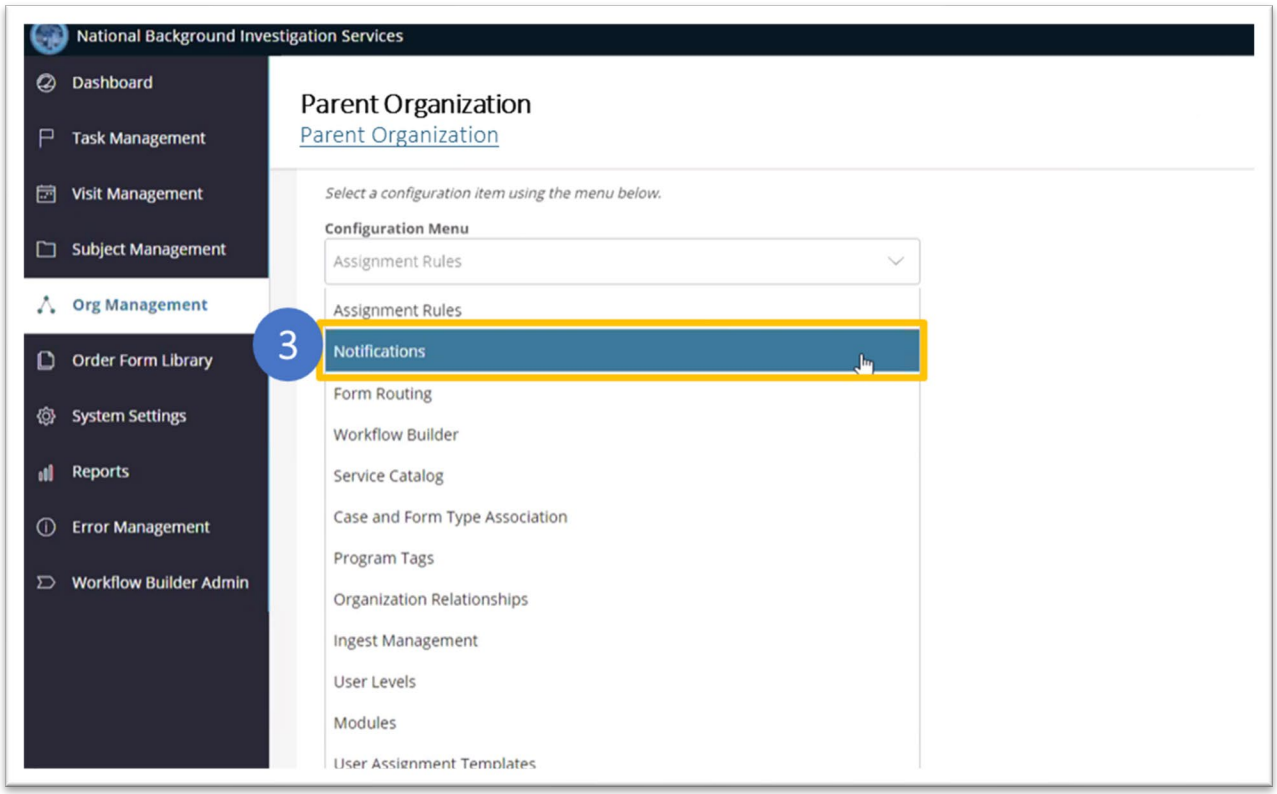
How to Edit a Notification

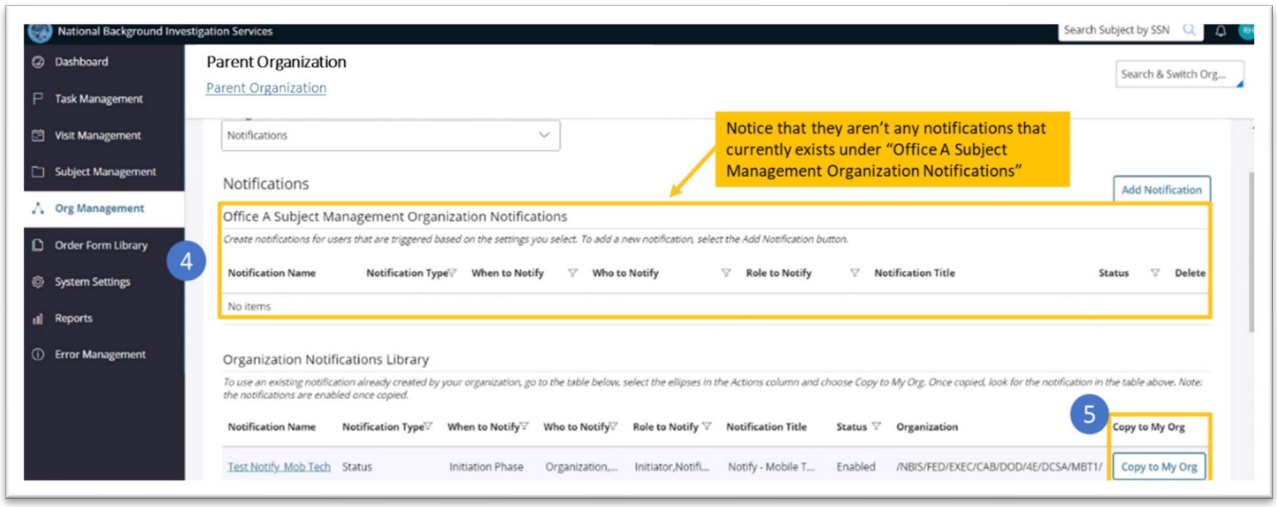
1. From initial log in, select **Organization Management** from the Navigation Menu on the left.
2. Navigate to your organization (if needed) then select the **Configuration** tab.
3. Select **Notifications** from the Configuration Menu drop-down.
4. After selecting Notifications from the drop-down, users will now be able to see the full list of existing notifications for the organization that they are logged into.
5. To view the details of a specific notification, search for and locate that notification using the **Notification Name** column and select the Notification Name to open the details of the selected notification.
6. From this screen, scroll down to bottom of the page and select the **Edit** button. Make necessary edits to any configurable fields. Select **Save and Add**.

Copy Notifications

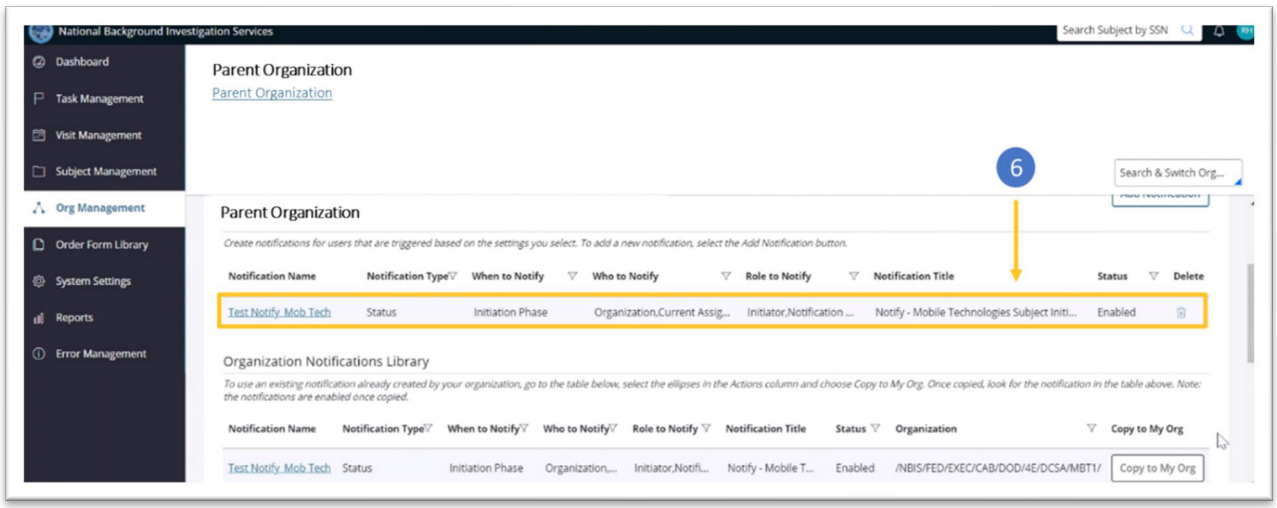


Copy Notifications

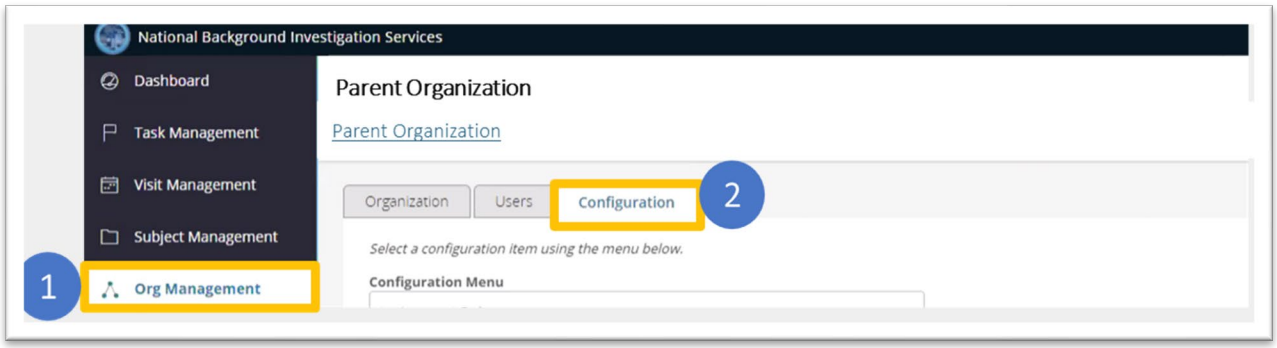




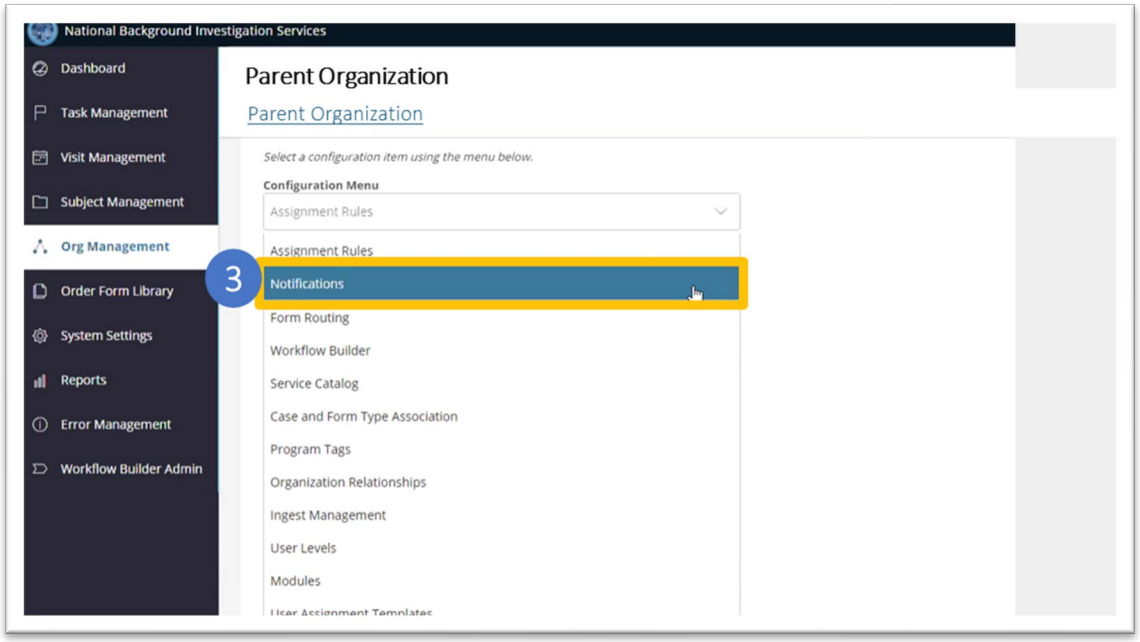
Copy Notifications



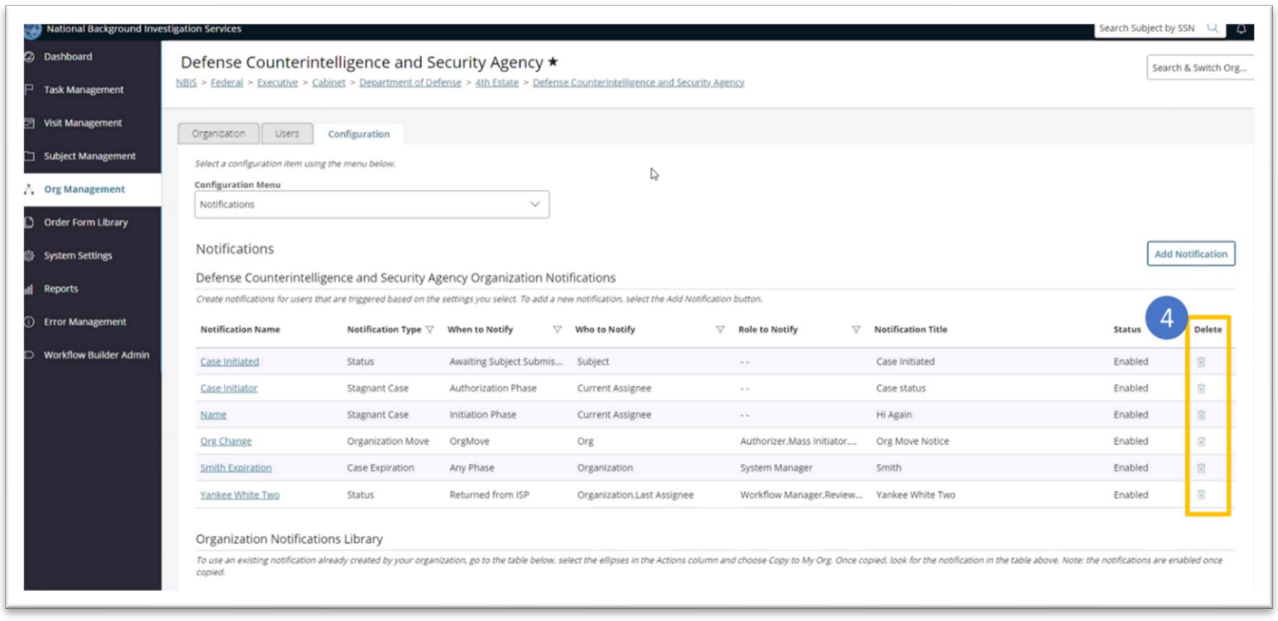
Delete Notifications



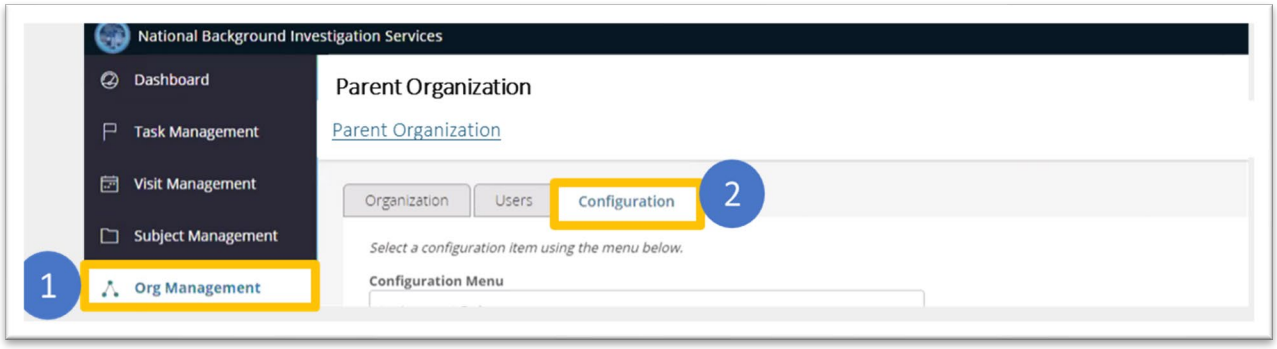
Delete Notifications



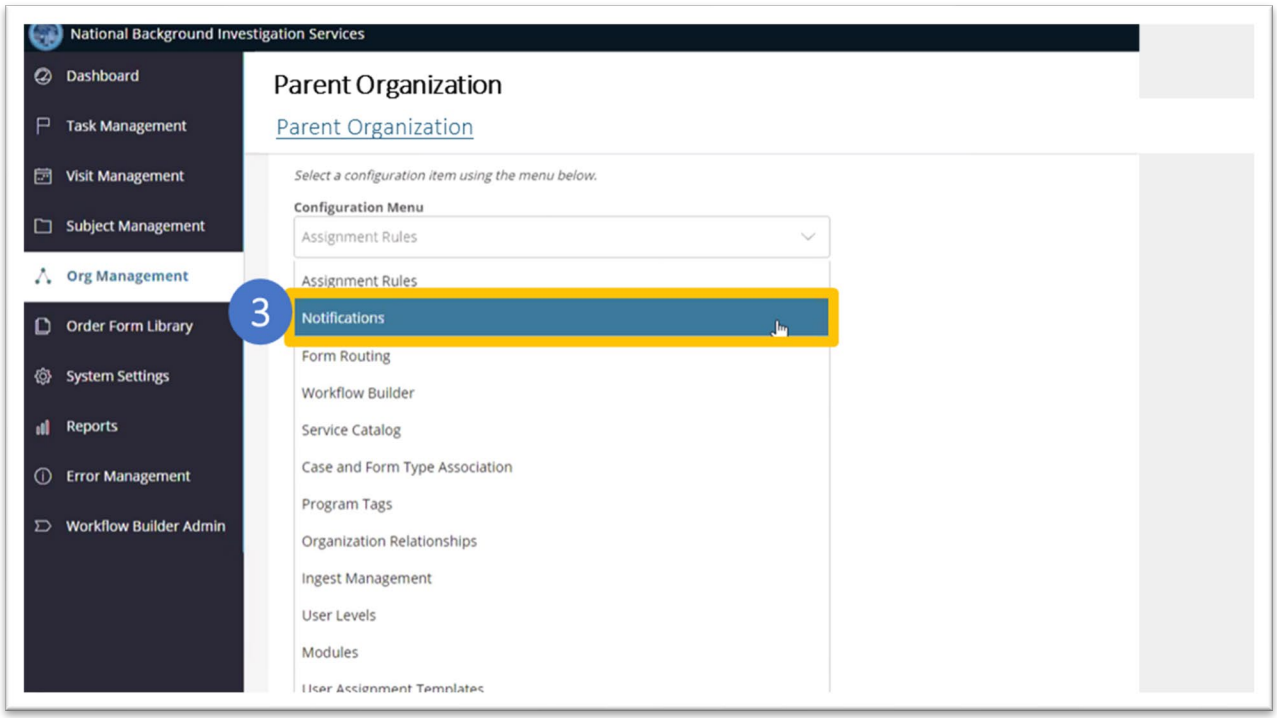
Delete Notifications



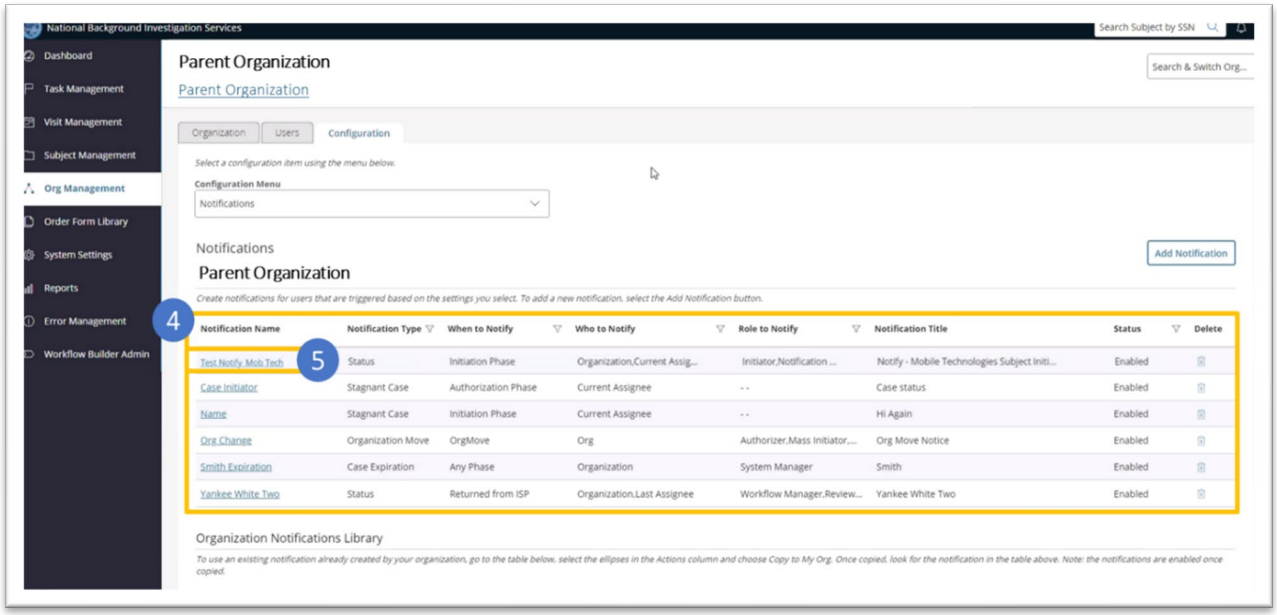
Edit Notifications



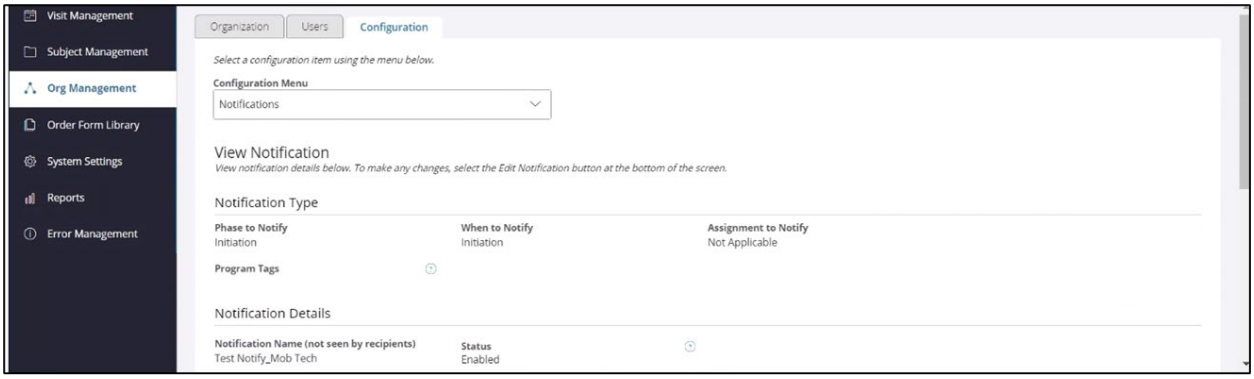
Edit Notifications

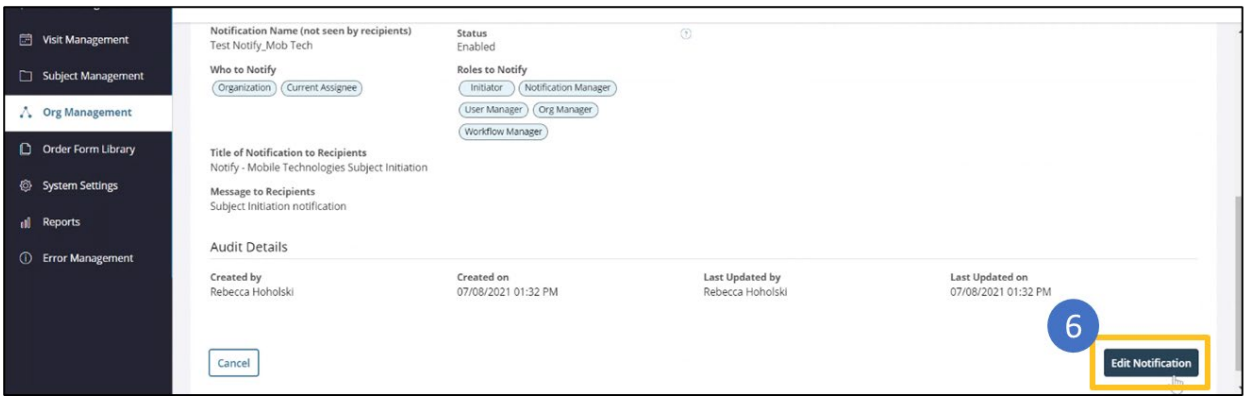


Edit Notifications

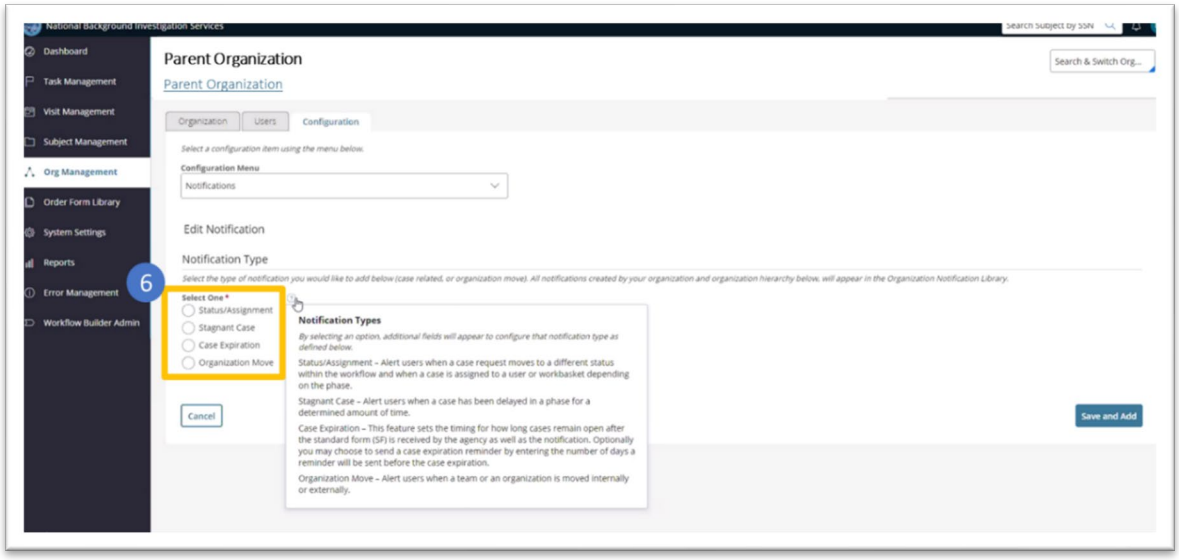


Edit Notifications

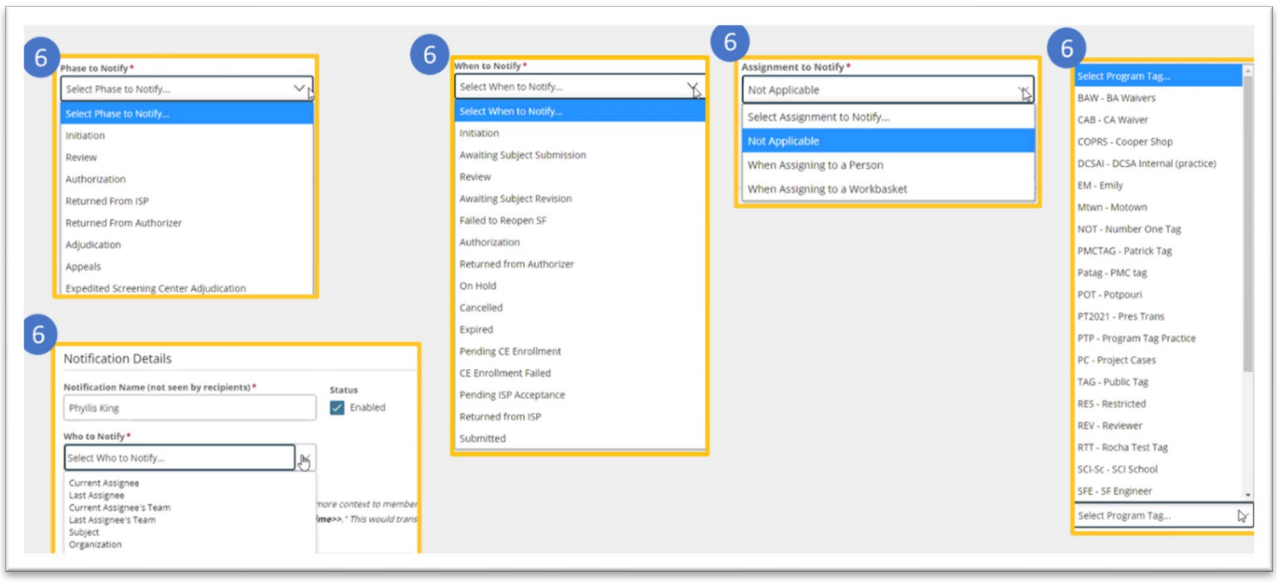




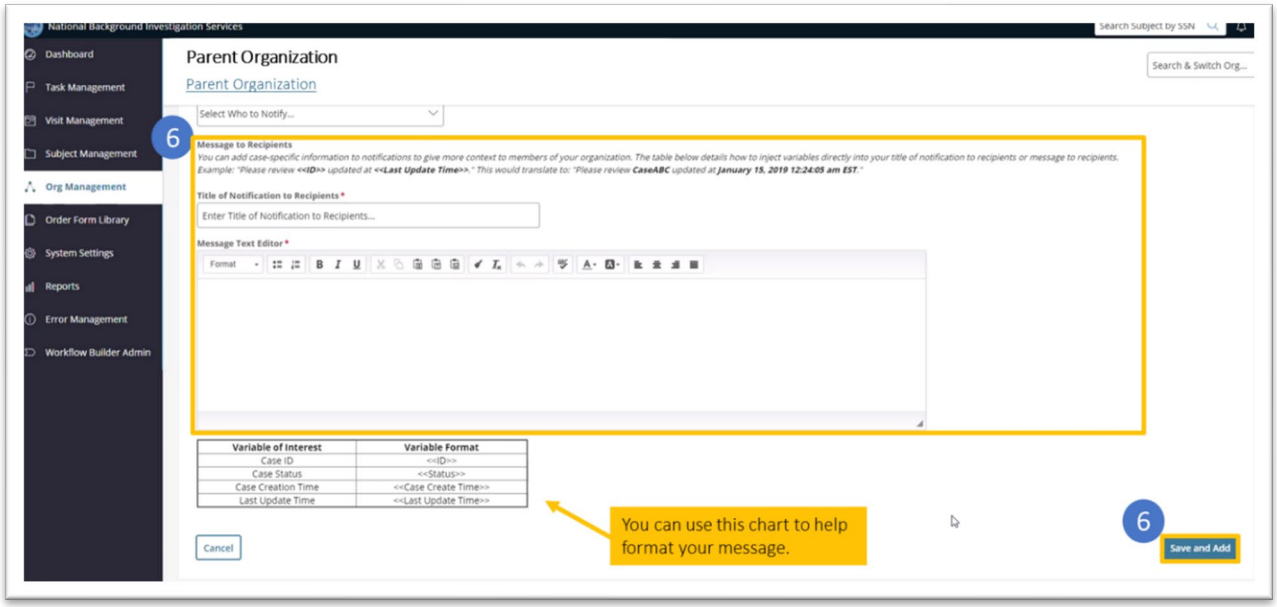
Edit Notifications



Edit Notifications



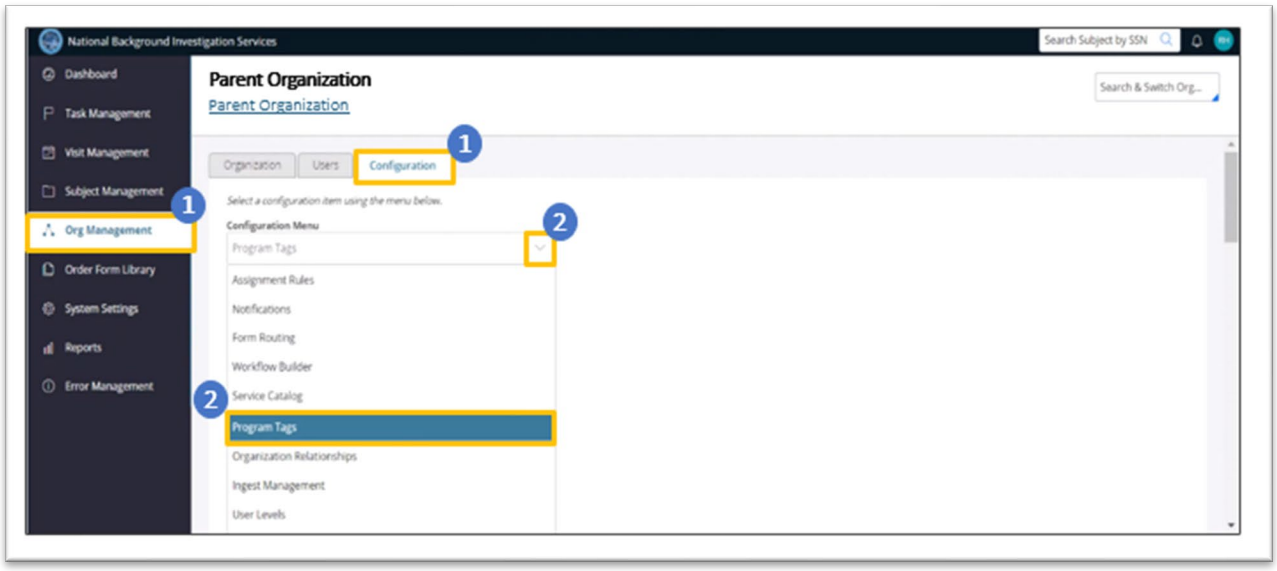
Edit Notifications

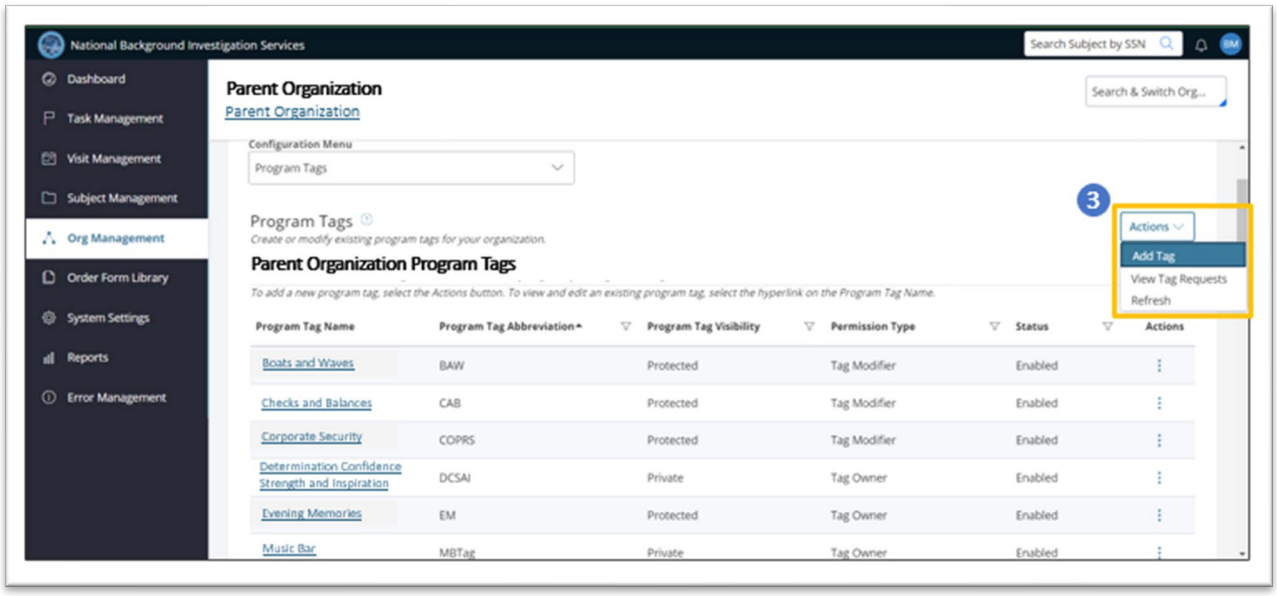


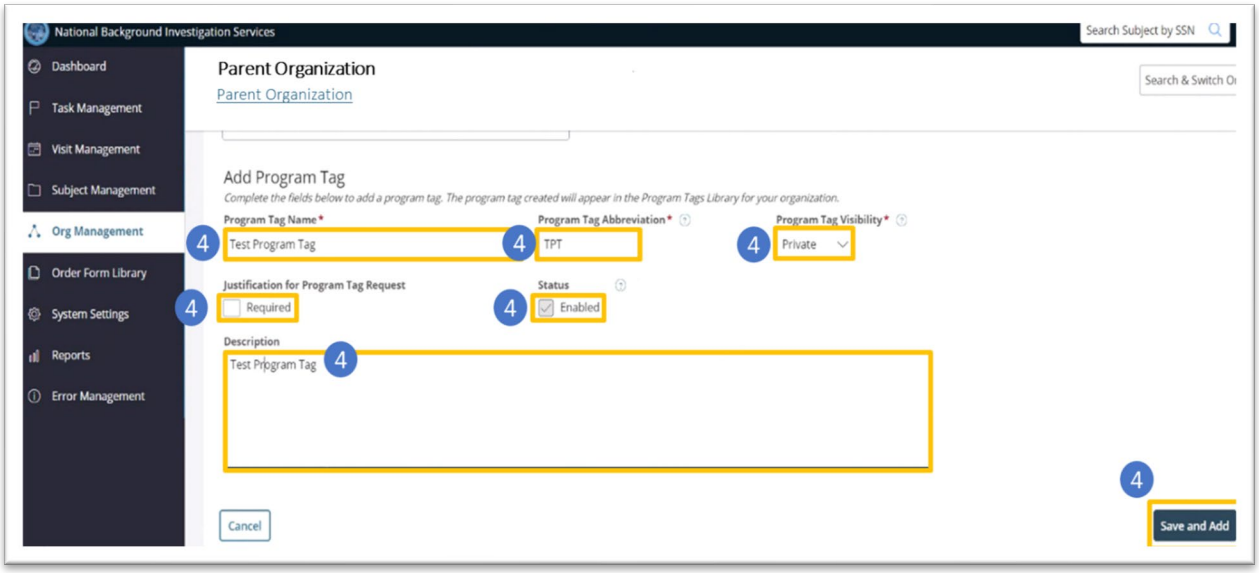
HOW TO ADD A PROGRAM TAG

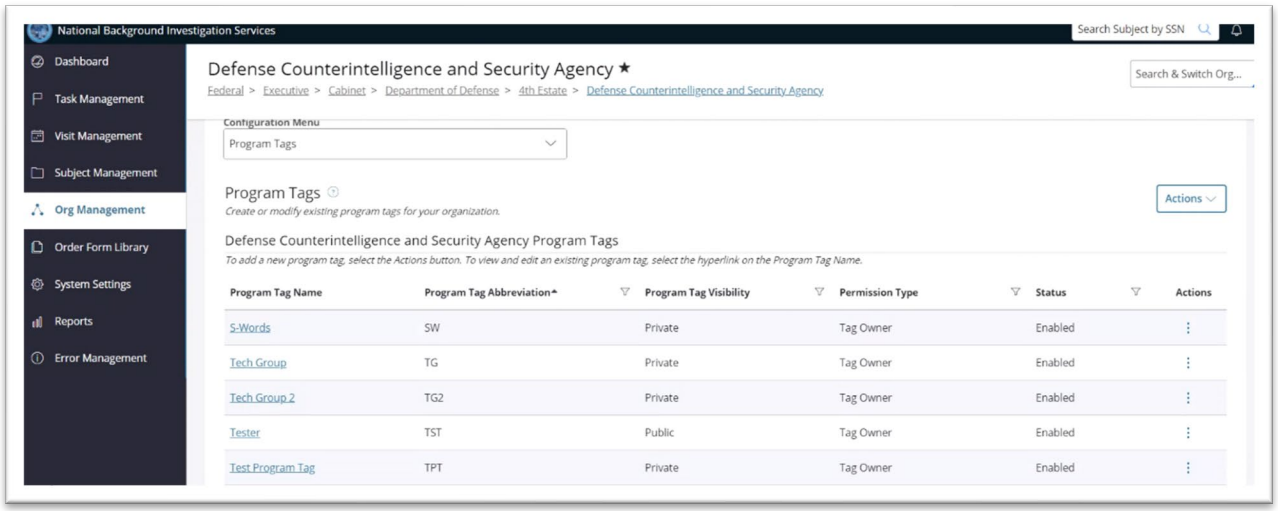
Users with the **Program Tag Manager role** can access, add, join, and manage program tags for their Org. Below are steps 1 and 2 of the 4-step process for how to Add a Program Tag.

1. From log in, select **Org Management** from the Navigation Menu on the left. Switch to the designated Org (if needed) and select the Configuration tab.
2. Click the arrow under the Configuration Menu to reveal drop-down options. Select **Program Tags** from the Configuration Menu drop-down. Users will be prompted with the list of Program Tags and the Program Tag Library for their Org.
3. Click the arrow within the Actions button to reveal the Actions drop-down menu. Select **Add Tag** to create a new Program Tag.
4. Complete all required fields and any desired optional fields for the Program Tag. Click **Save and Add** when finished. The newly added Program Tag should now appear in the list of existing Program Tags.




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
Parent Organization
Parent Organization
Search & Switch Org...
Configuration Menu
Program Tags
Program Tags
Create or modify existing program tags for your organization.
Parent Organization Program Tags
To add a new program tag, select the Actions button. To view and edit an existing program tag, select the hyperlink on the Program Tag Name.
3
Actions
Add Tag
View Tag Requests
Refresh
Program Tag Name
Program Tag Abbreviation
Program Tag Visibility
Permission Type
Status
Actions
Boats and Waves
BAW
Protected
Tag Modifier
Enabled
Checks and Balances
CAB
Protected
Tag Modifier
Enabled
Corporate Security
COPRS
Protected
Tag Modifier
Enabled
Determination Confidence Strength and Inspiration
DCSAI
Private
Tag Owner
Enabled
Evening Memories
EM
Protected
Tag Owner
Enabled
Music Bar
MBTag
Private
Tag Owner
Enabled


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
Parent Organization
Parent Organization
Add Program Tag
Complete the fields below to add a program tag. The program tag created will appear in the Program Tags Library for your organization.
Program Tag Name*
Test Program Tag
Program Tag Abbreviation*
TPT
Program Tag Visibility*
Private
Justification for Program Tag Request
Required
Status
Enabled
Description
Test Program Tag
4
Cancel
Save and Add


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
Defense Counterintelligence and Security Agency ★
Federal > Executive > Cabinet > Department of Defense > 4th Estate > Defense Counterintelligence and Security Agency
Search & Switch Org...
Configuration Menu
Program Tags
Program Tags
Create or modify existing program tags for your organization.
Actions
Defense Counterintelligence and Security Agency Program Tags
To add a new program tag, select the Actions button. To view and edit an existing program tag, select the hyperlink on the Program Tag Name.
Program Tag Name
Program Tag Abbreviation
Program Tag Visibility
Permission Type
Status
Actions
S-Words SW Private Tag Owner Enabled
Tech Group TG Private Tag Owner Enabled
Tech Group 2 TG2 Private Tag Owner Enabled
Tester TST Public Tag Owner Enabled
Test Program Tag TPT Private Tag Owner Enabled

HOW TO MANAGE A PROGRAM TAG

HOW TO VIEW A PROGRAM TAG

1. From initial log in, select **Organization Management** on the left from the Navigation Menu.
2. Users can Navigate to their organization (if needed). Select the **Configuration** tab.
3. Select the drop-down arrow under the Configuration Menu. Select **Program Tags** to view and manage Program Tags for user's Organization.
4. Users will be prompted with the list of existing Program Tags for user's organization.

HOW TO EDIT A PROGRAM TAG

Only users with the Program Tag Manager role can edit, manage, and modify the tags that are available for their organization.

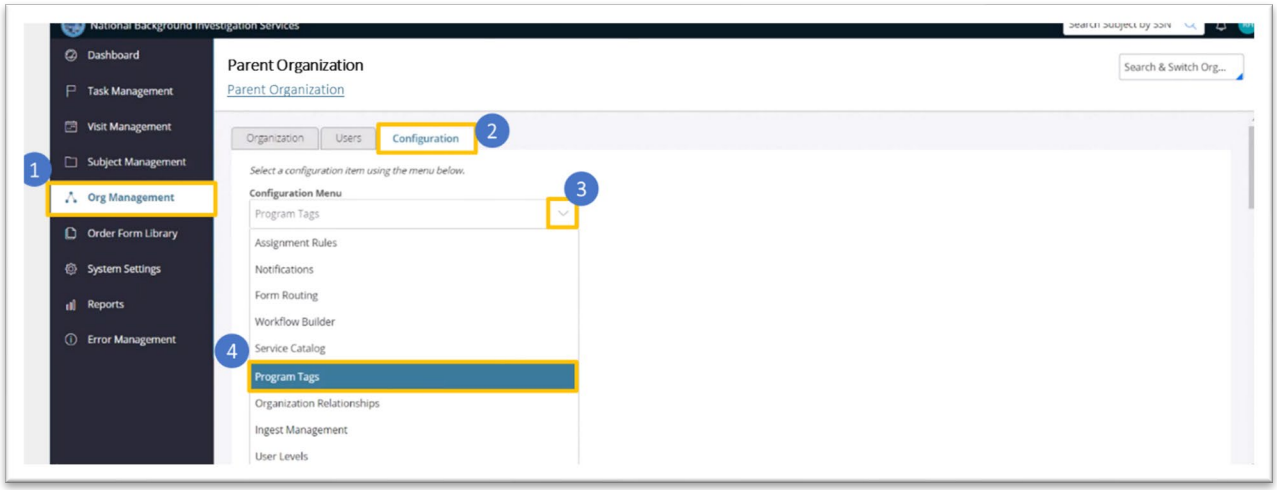
1. From log in, select **Organization Management** from the Navigation Menu on the left. Navigate to users Organization (if needed) then select the Configuration tab.
2. Select **Program Tags** from the Configuration Menu drop-down.
3. In the "Program Tag Name" column, click the hyperlinked text on the row of the Program Tag that users would like to edit or manage.
4. On the right side of the page, click the **Edit Details** hyperlink to Edit any of the required or optional fields for the Program Tag information. **Select Save**. Repeat Step 3, this time click the Edit Configurations hyperlink to Edit any of those fields. Click Save.
5. After clicking save, users will be returned to the list of existing Program Tags. In the Program Tag Name column, locate and click on the hyperlinked text for the Program Tag that users just edited. Verify that the details of users edited Program Tag saved and are accurate.

HOW TO DISABLE A PROGRAM TAG

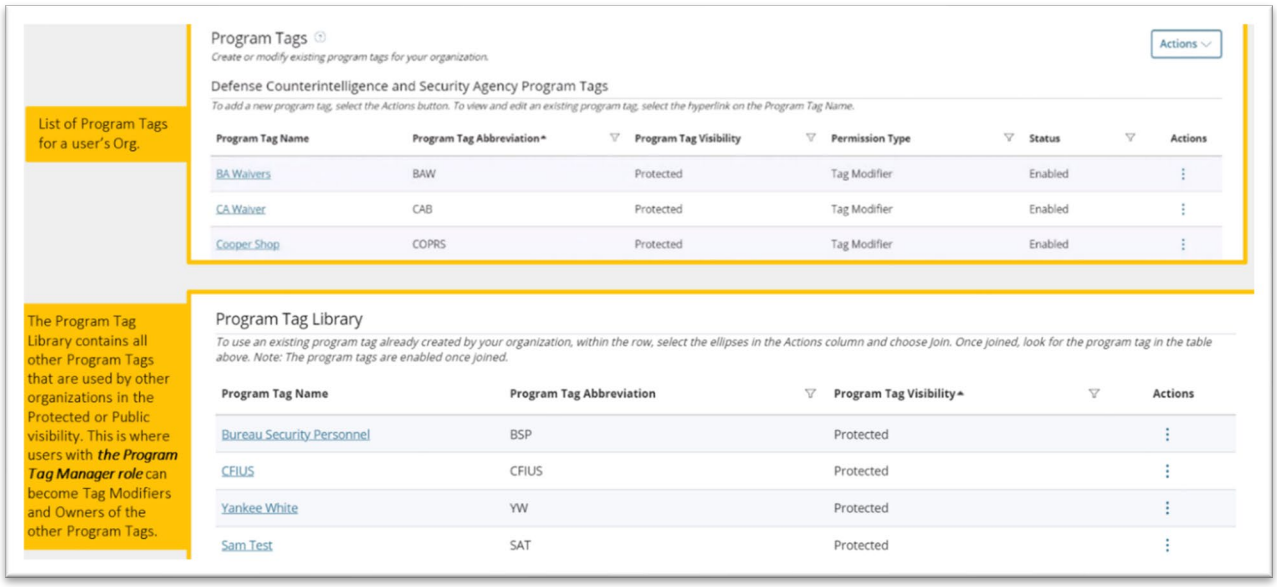
Only users with the Program Tag Manager role can disable Program Tags and Program Tags can only be disabled if users are the only user with access to the Program Tag.

1. From log in, select **Organization Management** from the Navigation Menu on the left. Navigate to users Organization (if needed) then select the Configuration tab.
2. Select **Program Tags** from the Configuration Menu drop-down.
3. In the "Program Tag Name" column, click the hyperlinked text on the row of the Program Tag to disable.
4. On the right side of the page, click the **Edit Details** hyperlink to edit any of the required or optional fields.
5. Uncheck the box under **Status to disable** this specific Program Tag. Click **Save**.

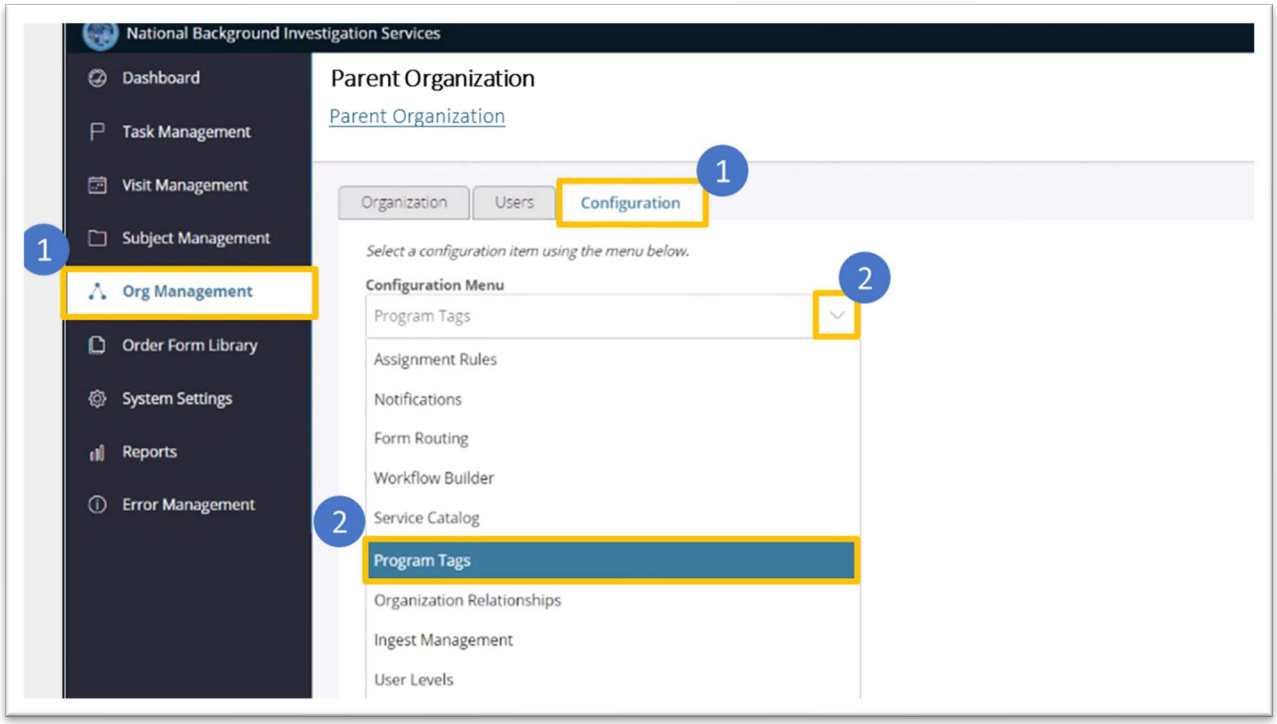
View Program Tag



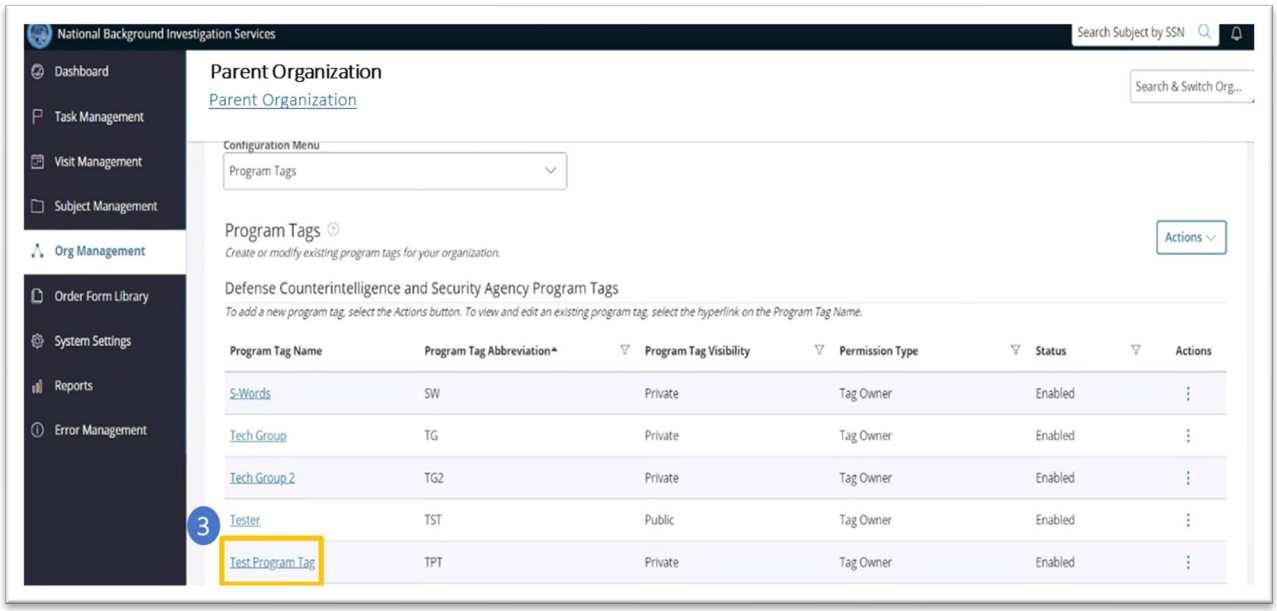
View Program Tag



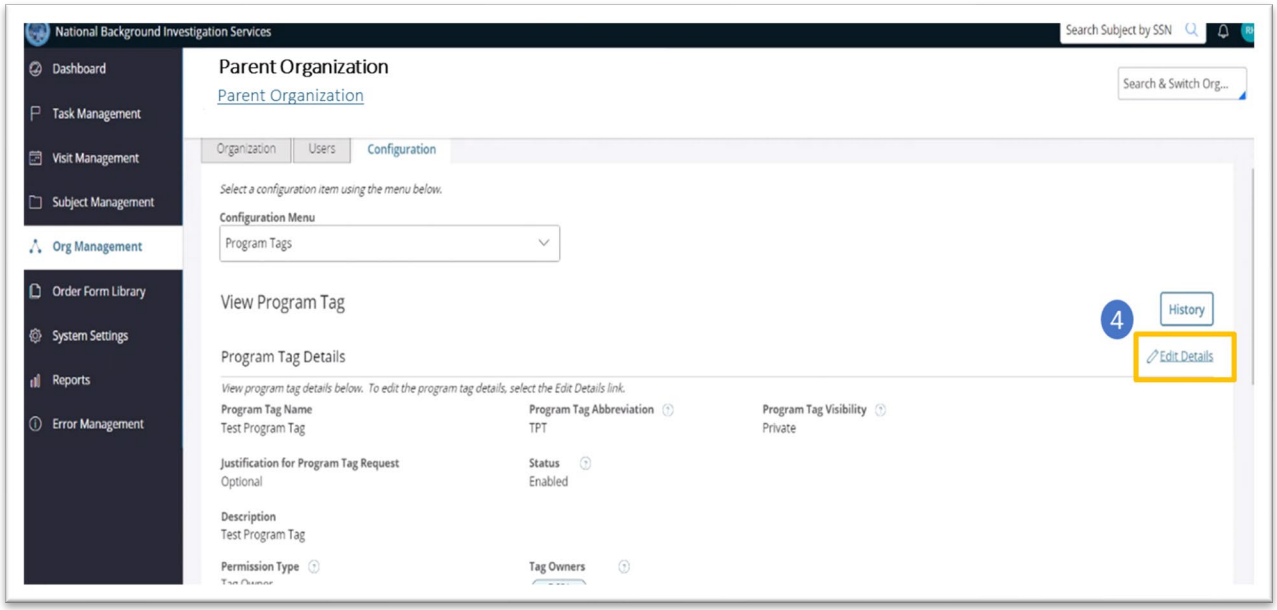
Edit Program Tag



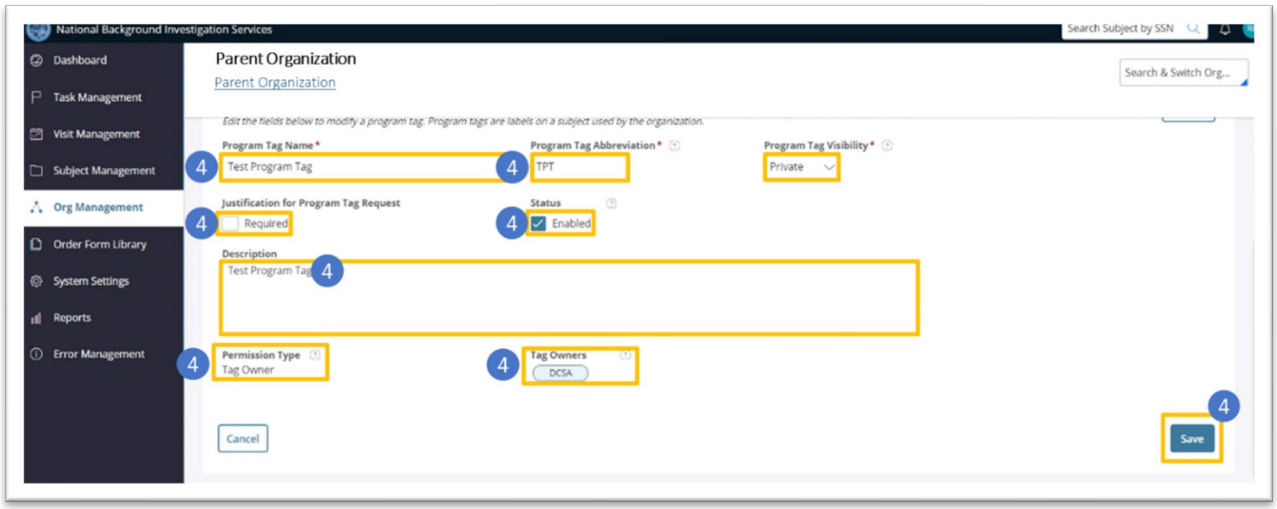
Edit Program Tag



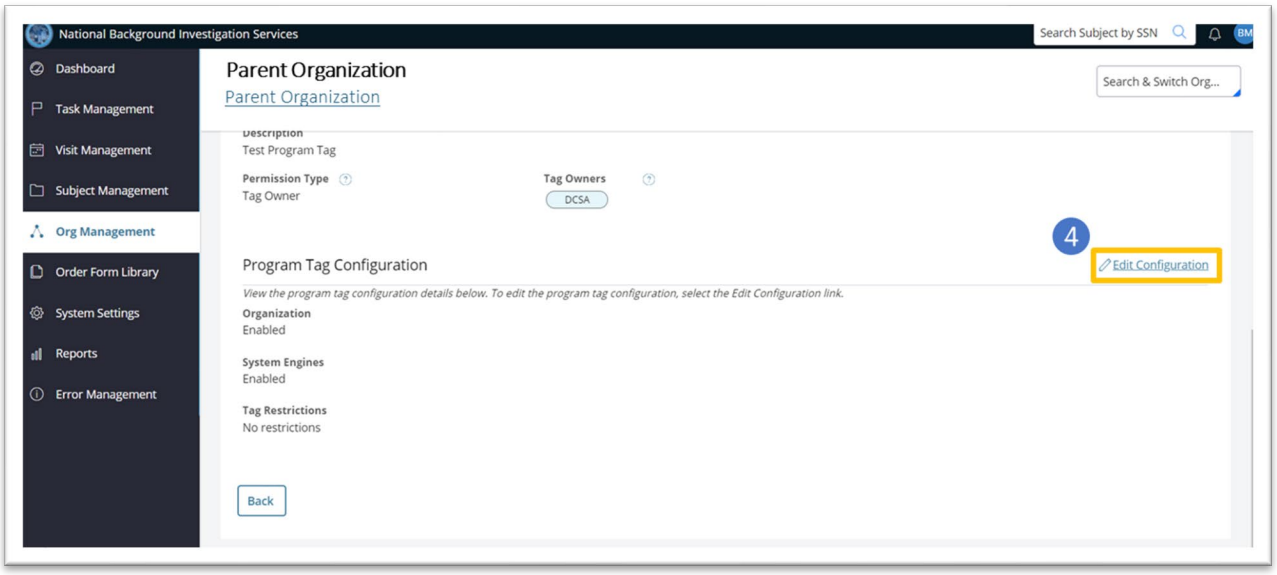
Edit Program Tag



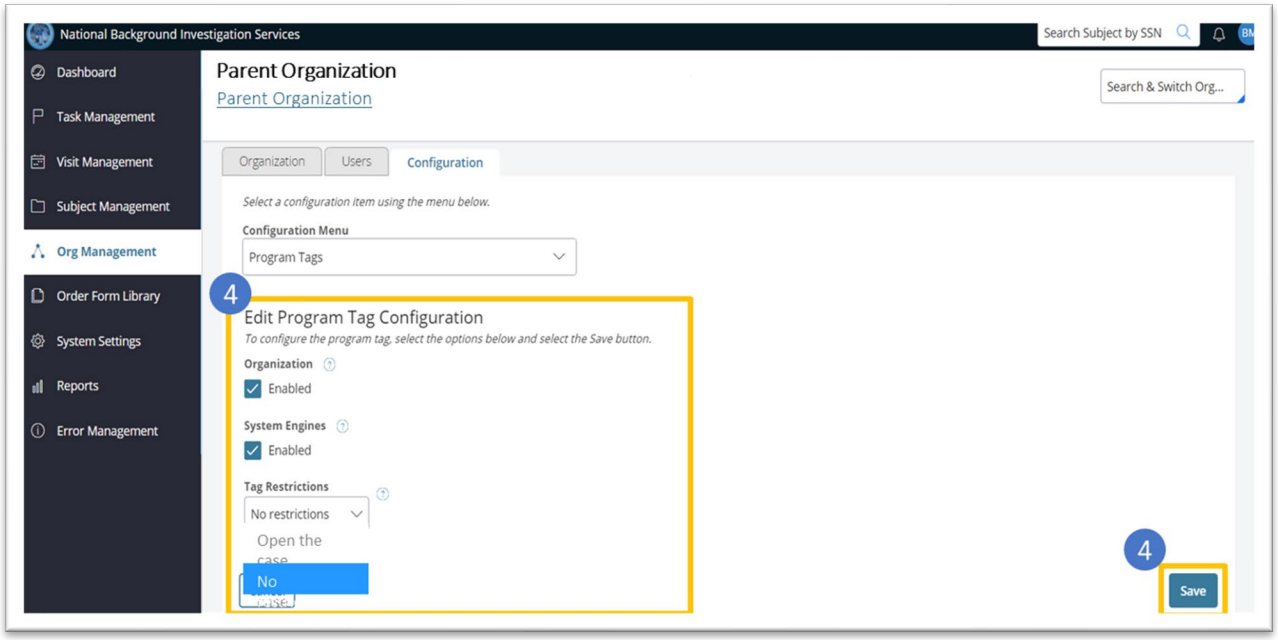
Edit Program Tag



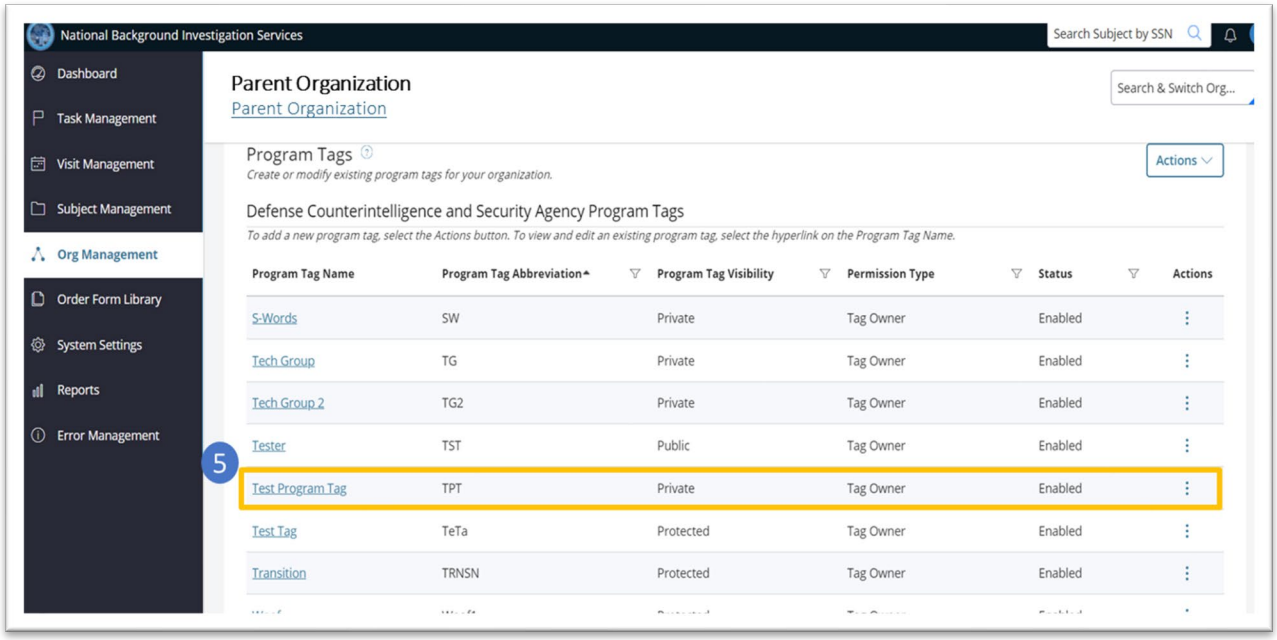
Edit Program Tag



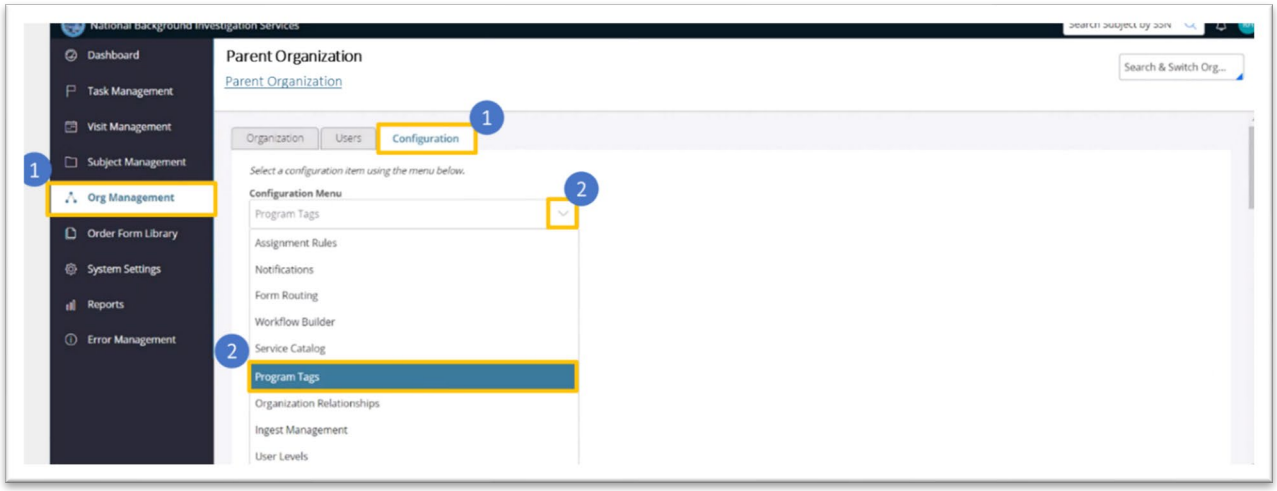
Edit Program Tag



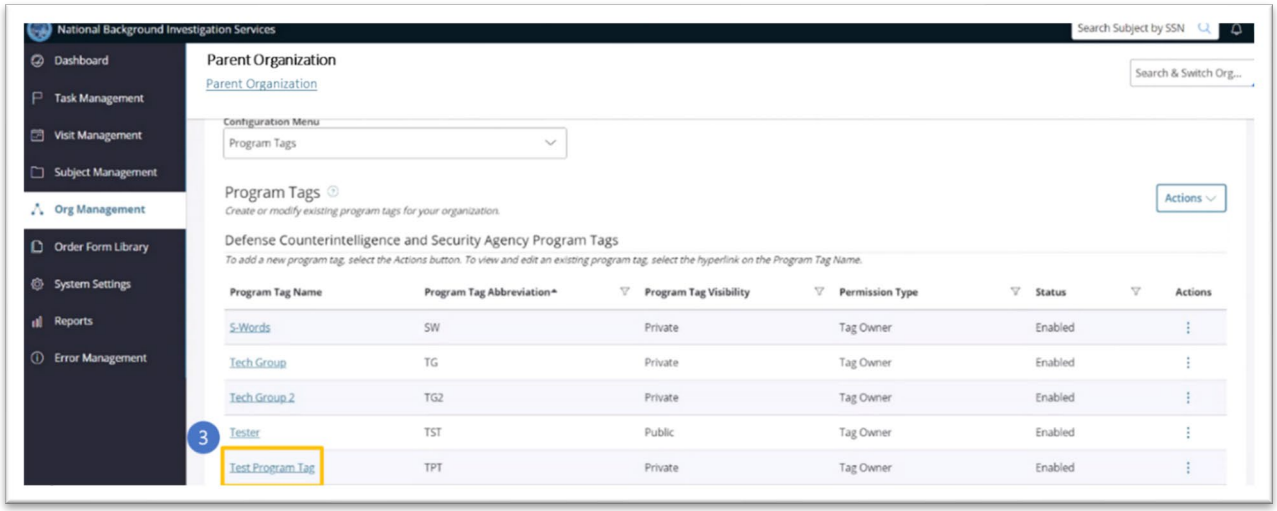
Edit Program Tag



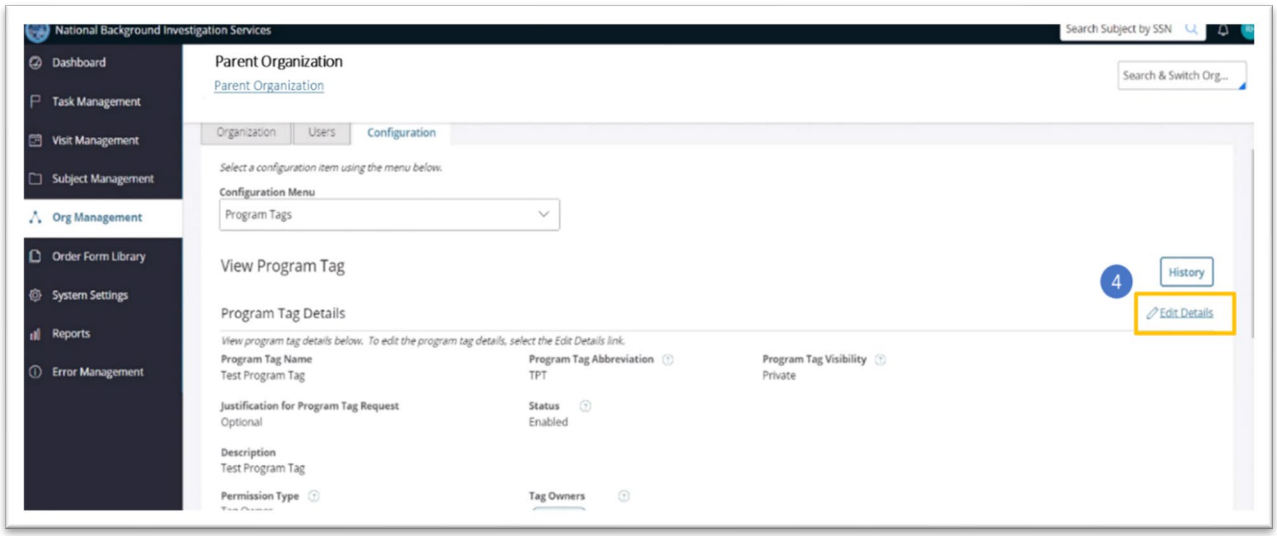
Disable Program Tag



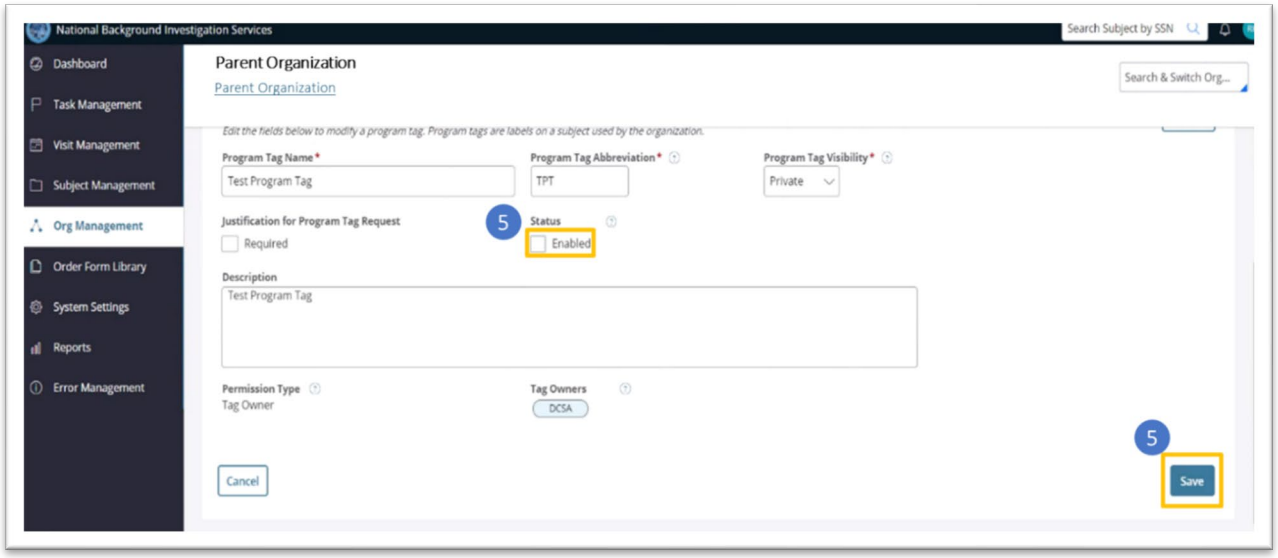
Disable Program Tag



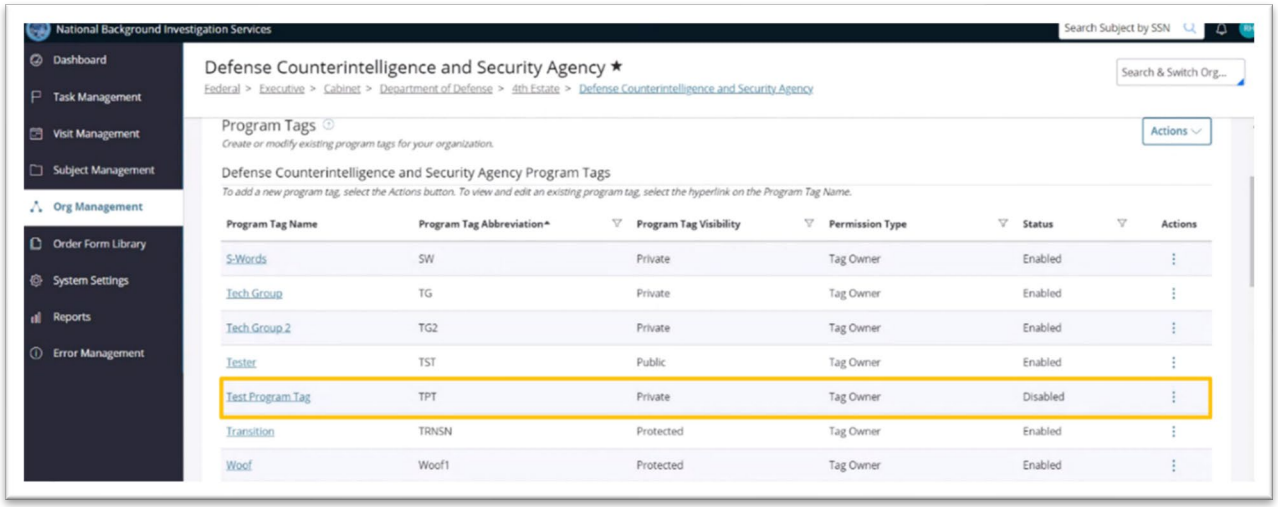
Disable Program Tag



Disable Program Tag



Disable Program Tag



HOW TO APPROVE/REJECT PROGRAM TAGS

Users with the **Program Tag Manager** role can Approve/Reject Program Tag Requests for their Org. Below is the 5-step process for how to Approve/Reject Program Tags.

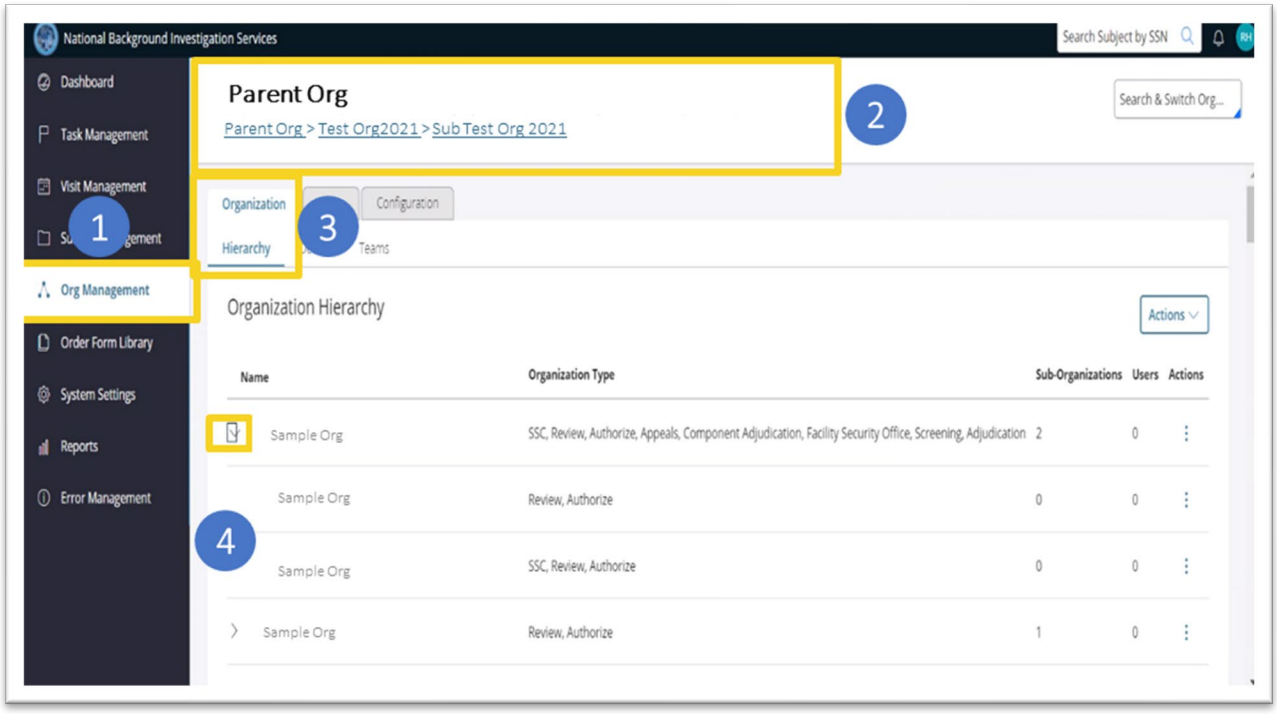
1. From log in, select **Org Management** from the Navigation Menu on the left. Switch to the designated Org (if needed) and select the Configuration tab.
2. Click the arrow under the Configuration Menu to reveal drop-down options. Select **Program Tags** from the Configuration Menu drop-down. Users will be prompted with the list of Program Tags and the Program Tag Library for their Org.
3. Click the Actions button to reveal the options from the Actions drop-down menu and select **View Tag Requests**. The page will display all the Incoming and Outgoing Requests for a user's organization.
4. Incoming Requests are requests from other organizations to gain access to tags the current organization is a Modifier of. Outgoing Requests lists the requests for the current organization to gain access to other Program Tags. Check the box that says "**include Completed Requests**" to reveal additional Program Tag Requests.
5. To approve or reject an incoming tag request, select the Program Tag Name on the request or select the ellipses under the Actions column. The Program Tag Request Details screen shows all the relevant information on the request. The Program Tag Details are found at the bottom to remind the user which tag this organization is requesting. Select **Reject/Approve** in the bottom right corner.

HOW TO VIEW AN ORGANIZATION HIERARCHY AND DETAILS

Users with the Org Manager role can view their designated hierarchy, details, and teams' tabs. The breadcrumbs are a link that will move to that Organization's page if users navigate to different organization levels and can be referenced to show users which Org they are currently viewing. Below is the 5-step process for how to view hierarchies and organization details.

1. Navigate to **Org Management** on the left-hand side of the navigation panel and switch to the designated Org (if needed).
2. The **Organization title and breadcrumbs** will tell users which Organization's attributes they are viewing.
3. Navigate to the **Hierarchy tab** to view the Sub-Orgs in the current Organization's hierarchy.
4. **Select the arrow**, if available, to view an expansion of the Sub-Org's hierarchy. If no arrow is visible, there are no Sub-Orgs underneath the Org.
5. **Navigate to the Details tab** to view the current Organization's details. This includes an overview of the organization; the designated organization types, functions, and roles; and additional information (i.e., CV Settings, Legacy Systems, Location, Mailing Address, and Point of Contact).

Steps 1-4



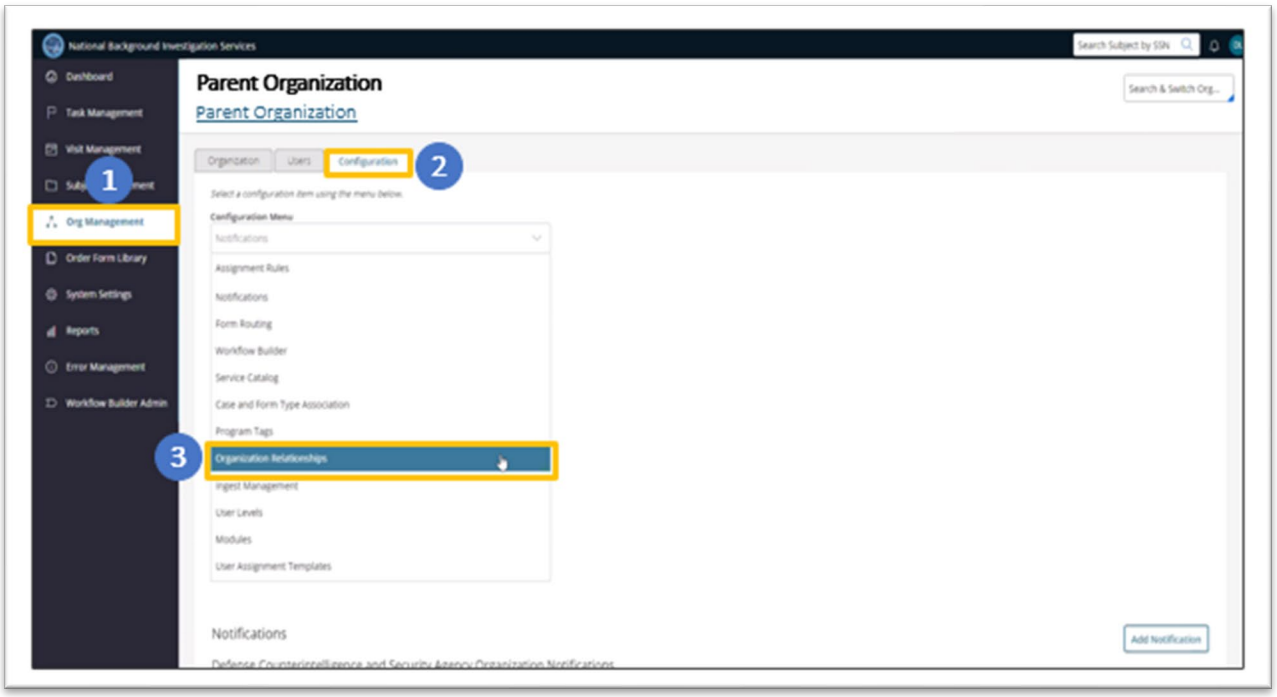
HOW TO VIEW AND EDIT INTERNAL ORG RELATIONSHIPS

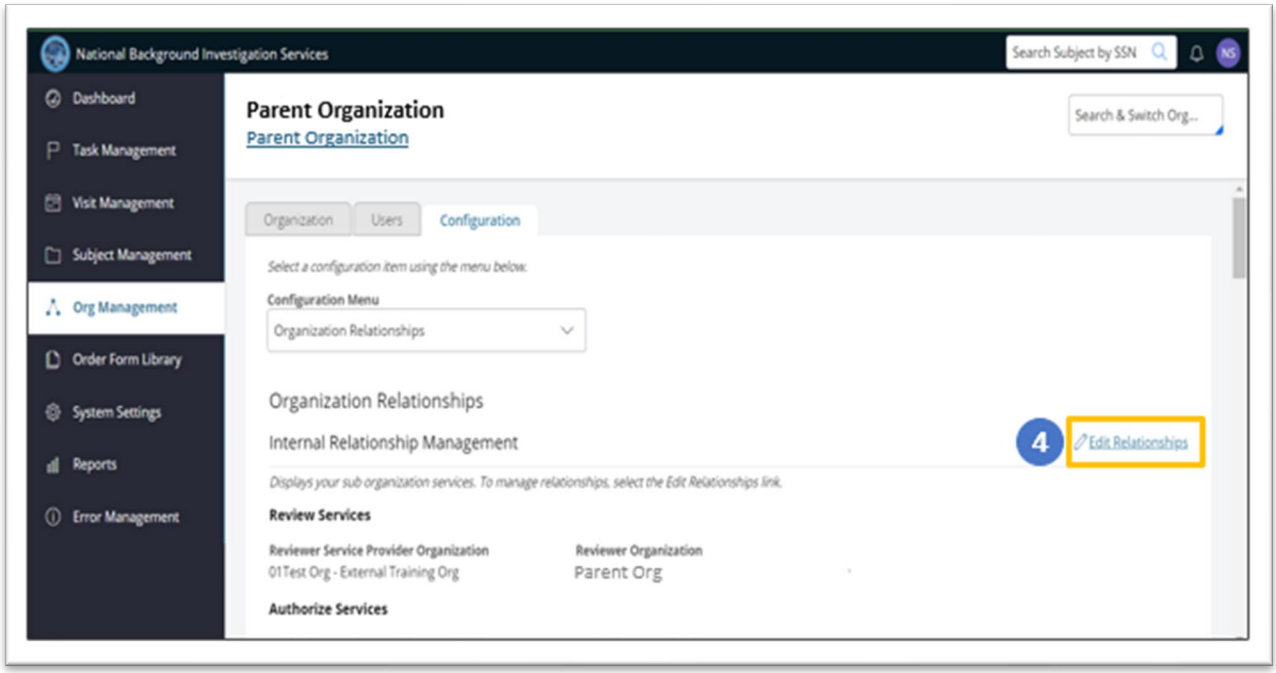
The Organization Relationships page allows a user's organization to establish connections with other organizations internally and externally to provide services for other organizations to utilize. Only users with the **Organization Relationship Manager role** can configure these relationships and they must be added by users with the **Org Manager role**. Establishing Org Relationships will grant specific privileges within NBIS to users with the Org Relationship Manager role such as utilizing other Orgs outside of their Org's hierarchy in Form Routing.

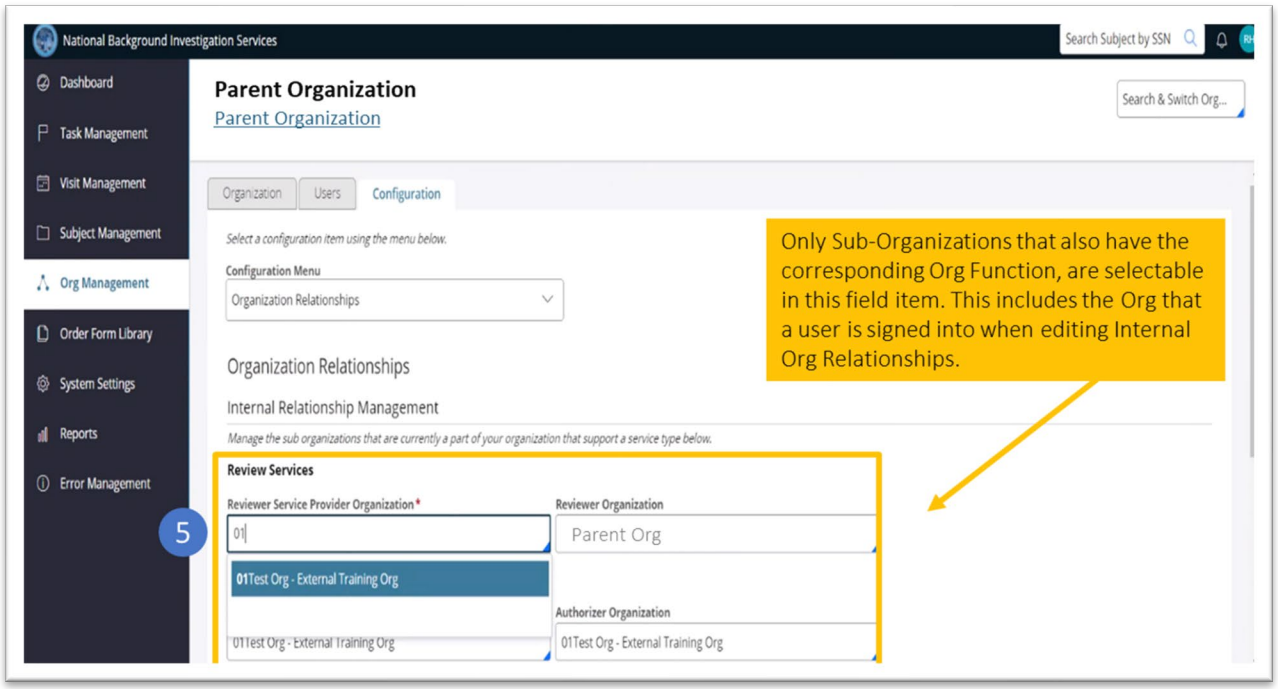
In order to make edits or appear on the Org Relationships page, an org must have either an Authorizer, Reviewer, Appeals, Screening or Adjudicator Provider org function. The Internal Relationship Management section in NBIS also allows Service Provider Orgs to edit who they provide services to within their org's hierarchy and how their org's services will be implemented.

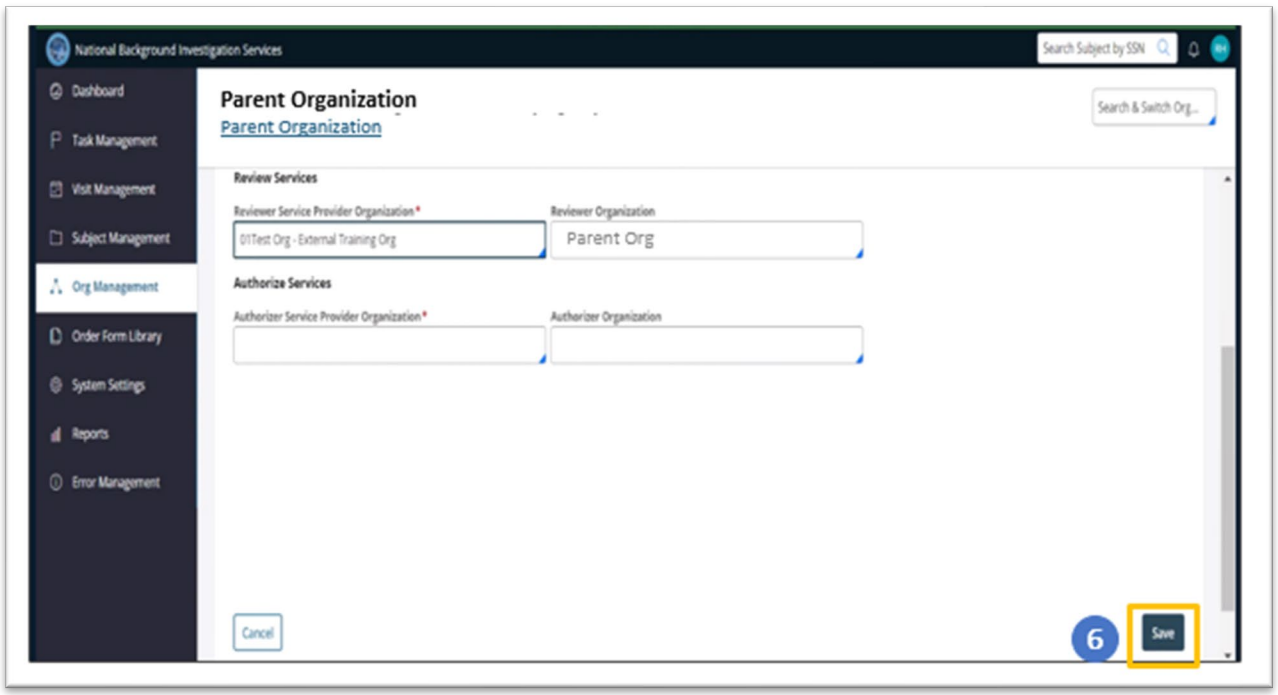
Below outlines the 6-Step process to view and edit Internal Org Relationships.

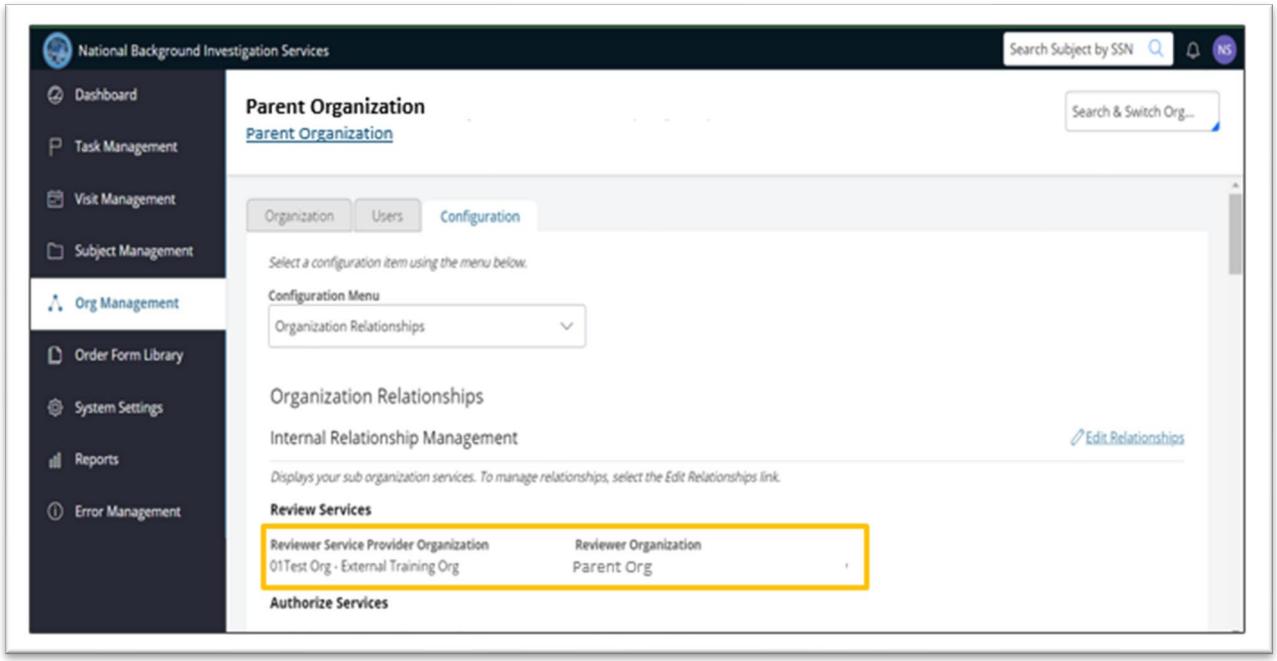
1. From log in, select **Org Management** from the Navigation menu.
2. Switch to the designated Org (if needed) and select the **Configuration** tab.
3. Click the arrow within the Configuration Menu to reveal the drop-down options and select **Organization Relationships**.
4. Within the Internal Relationship Management section, click the **Edit Relationships** hyperlink with the pencil icon.
5. Users can edit and manage specific configurations according to their organizational needs. Users can edit designations for Review, Authorize, Adjudication and Screening services.
6. Click **Save** in the bottom right corner after making edits.


National Background Investigation Services
Search Subject by SSN
Dashboard
Task Management
Visit Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Workflow Builder Admin
Parent Organization
Parent Organization
Search & Switch Org...
Organization
Users
Configuration
1
2
3
Select a configuration item using the menu below.
Configuration Menu
Notifications
Assignment Rules
Notifications
Form Routing
Workflow Builder
Service Catalog
Case and Form Type Association
Program Tags
Organization Relationships
Ingest Management
User Levels
Modules
User Assignment Templates
Notifications
Add Notification


National Background Investigation Services
Search Subject by SSN
NS
Dashboard
Task Management
Visit Management
Subject Management
Org Management
Order Form Library
System Settings
Reports
Error Management
Parent Organization
Parent Organization
Search & Switch Org...
Organization
Users
Configuration
Select a configuration item using the menu below.
Configuration Menu
Organization Relationships
Organization Relationships
Internal Relationship Management
4
Edit Relationships
Displays your sub organization services. To manage relationships, select the Edit Relationships link.
Review Services
Reviewer Service Provider Organization
01Test Org - External Training Org
Reviewer Organization
Parent Org
Authorize Services


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
Parent Organization
Parent Organization
Search & Switch Org...
Organization
Users
Configuration
Select a configuration item using the menu below.
Configuration Menu
Organization Relationships
Organization Relationships
Internal Relationship Management
Manage the sub organizations that are currently a part of your organization that support a service type below.
Review Services
Reviewer Service Provider Organization *
Reviewer Organization
01
Parent Org
01Test Org - External Training Org
Authorizer Organization
01Test Org - External Training Org
01Test Org - External Training Org
5
Only Sub-Organizations that also have the corresponding Org Function, are selectable in this field item. This includes the Org that a user is signed into when editing Internal Org Relationships.


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
Parent Organization
Parent Organization
Search & Switch Org...
Review Services
Reviewer Service Provider Organization *
Reviewer Organization
01Test Org - External Training Org
Parent Org
Authorize Services
Authorizer Service Provider Organization *
Authorizer Organization
Cancel
6
Save


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
Parent Organization
Parent Organization
Search & Switch Org...
Organization
Users
Configuration
Select a configuration item using the menu below.
Configuration Menu
Organization Relationships
Organization Relationships
Internal Relationship Management
Edit Relationships
Displays your sub organization services. To manage relationships, select the Edit Relationships link.
Review Services
Reviewer Service Provider Organization
Reviewer Organization
01Test Org - External Training Org
Parent Org
Authorize Services

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/answersshed13htm.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.