DRAFT

INVESTIGATION MANAGEMENT
ONLINE SERVICE PROVIDERS GUIDE

NBIS Program Release: 4.3 _ 02/02/2023 Draft

USER GUIDE

SERIAL NUMBER #

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

NBIS Service Desk Information Phone: (724) 794-5612 x4600 | Email: dcsa.boyers.nbis.mbx.nbis-agency-support@mail.mil

CHANGE LOG

NBIS Program Release: 4.3 _ 02/02/2023 Draft

This document is the property of: National Background Investigation Services

Date	Feature	Change Description	Section	Configuration Update?
08/24/2022	N/A	Updated Guide to Release 4.3 See 4.2 Knoxville Guide for previous changes	All Sections	
11/22/2022	NBISPLAT-56292	Added note for the affiliation Category dropdown	3.1.2 Add Persona	Yes
11/22/2022	NBISPLAT-56292	Added note for the affiliation Category dropdown	7.1 Assignment Rule Management	Yes
12/5/2022	NBISPLAT-57676	Added section for managing report access	11.5 Manage Report Access	Yes
12/7/2022	NBISPLAT-58239	Added subsection for mandatory contextual fields from a data source	9.9.1 Mandatory Fields to Add from a Data Source	Yes
12/07/2022	NBISPLAT-48821	Updated screenshot for bulk reassign and “Select All Tasks” checkbox was added.	2.2 Reassign a case from Task Management	
12/08/2022	NBISPLAT-57570	Updated screenshots and added note for system generated program tag abbreviation	7.3 Program Tag Management	
12/21/2022	NBISPLAT-58239	Added new subsection for validating a lead	9.14 Validate a Lead	
12/21/2022	NBISPLAT-57679	Updated Org Details fields for Grouping and CV Settings	6.3.2 Creating an Organization	Yes
12/21/2022	NBISPLAT-57570	Updated Program Tag Library screens	7.3.4 Program Tag Library	
12/21/2022	NBISPLAT-57102	Added Org Redistribution Module Description	10.5 Manage Workflow Modules	
12/22/2022	NBISPLAT-53924	Added ID Prefix Description for Lead ID	7.6 Case Categories	Yes

Date	Feature	Change Description	Section	Configuration Update?
12/22/2022	NBISPLAT-51702	Added new section for the org redistribution module configuration	10.5.10 Org Redistribution Module Configuration	Yes
01/05/2023	NBISPLAT-55234	Updated screenshot and fields for Protected Source designation	7.6 Case Categories	Yes
01/19/2023	NBISPLAT-57577	Added note for Suspend Case Status checkbox	10.3.1 Add a Workflow Status	Yes
01/19/2023	NBISPLAT-54015	Added table entry for BI Close module	10.5 Manage Workflow Modules	Yes
01/19/2023	NBISPLAT-54016	Added new section for Question Configuration	7.12 Question Configuration	Yes
01/19/2023	N/A	Updated role matrix	13.3 Role Matrix	
01/27/2023	NBISPLAT-55434	Added description for Case Product Case Type field	7.5.1 Configuring a Case Type (Service)	Yes
01/30/2023	NBISPLAT-55434	Added description for Case Product Item Group field	7.6 Case Categories	Yes
02/01/2023	NBISPLAT-57676	Updated the wording to reflect changes for configuring report access	11.1 Mange Report Access	Yes
02/01/2023	NBISPLAT-58797	Added table entry for CV Enrollment Failure report	11.2 Types of Reports	
02/02/2023	NBISPLAT-57676	Removed available to User Role Column	11.2 Types of Reports	

TABLE OF CONTENTS

1 Overview and Requirements

This user guide provides tasks and steps for the National Background Investigation System. It is intended for NBIS System Administrators, Organization Administrators, and User Administrators. The guide also includes steps for Financial Administration.

1.1 Requirements Overview

1.1.1 SYSTEM REQUIREMENTS

You must have a government furnished computer, have been granted appropriate access, and have a PIV or CAC for access to the system.

1.1.2 SOFTWARE REQUIREMENTS

This section lists the software required to use NBIS Enterprise Portal web application. The software packages listed below are the recommended versions for use with *NBIS Enterprise Portal*. The use of other applications, or versions older than the ones listed, may result in unexpected or undesired behavior.

Table 1-1: System Requirements

Operating Systems	Browsers Supported
Microsoft Windows 8 Microsoft Windows 10	Recommended use of latest Version for all browsers • Google Chrome • Firefox • Microsoft Edge (Chromium) • Internet Explorer

PDF Document Viewer

Some portions of the *NBIS* system use Adobe Acrobat PDF document format. To view these files, you will need Adobe Reader, Acrobat Standard, or Acrobat Professional version 7.0 or later. Contact IT Help Desk support if needed.

1.2 Logging In

The following steps will guide you through logging into the NBIS Enterprise Portal. Please contact your supervisor or IT Help Desk for additional support.

1.2.1 CERTIFICATE ENROLLMENT

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

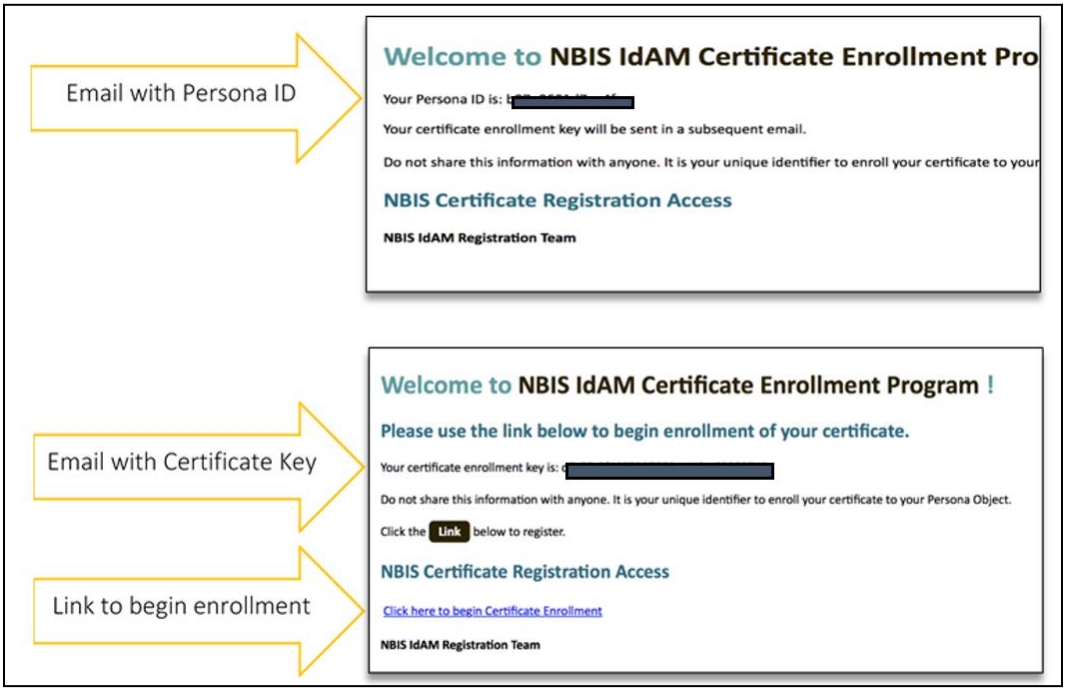


Figure 1-1: NBIS IdAM Emails

2. After reading the Terms of Service select, **I Accept** to agree to the service terms.

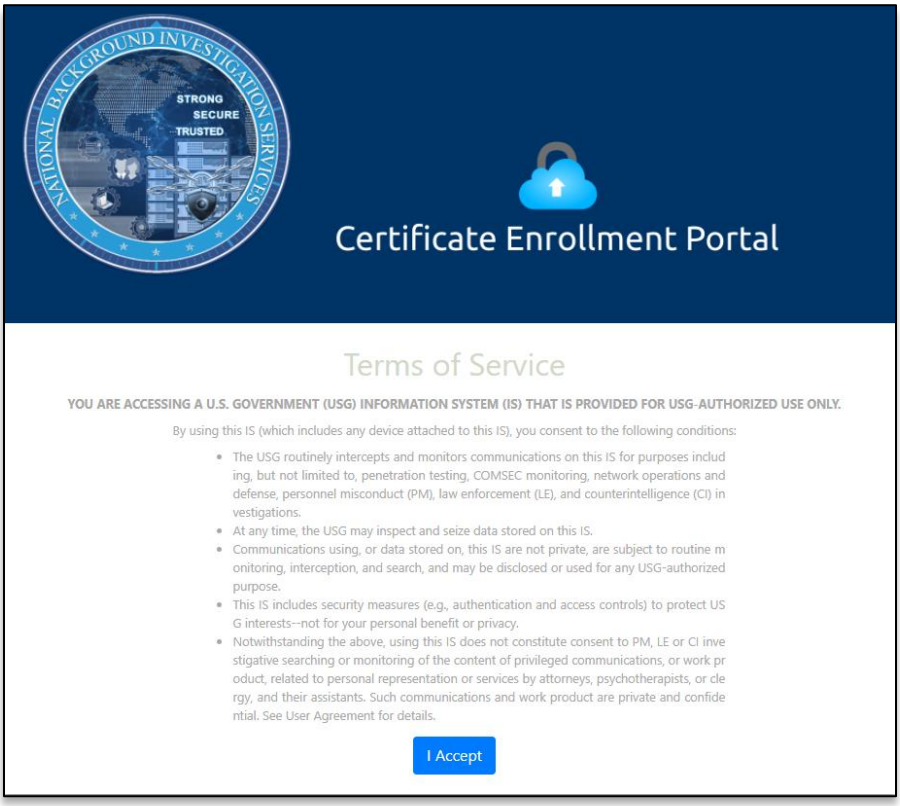


Figure 1-2: Terms of Service

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.

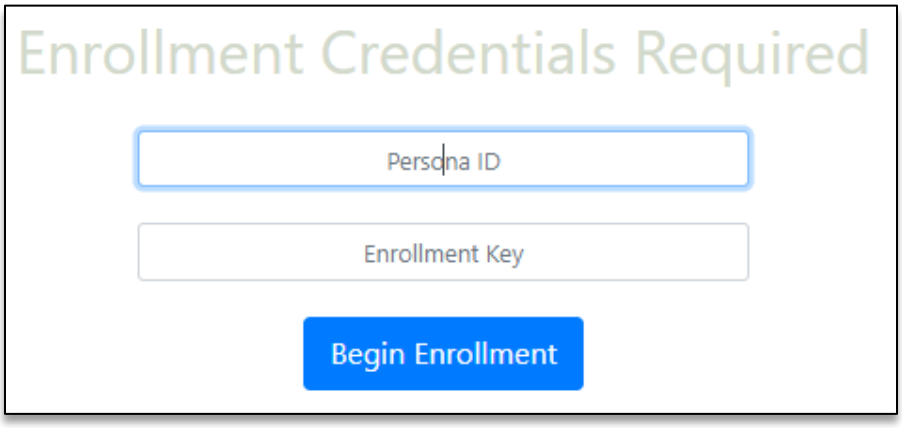


Figure 1-3: Begin Enrollment Screen

4. Use the **Select Certificate** button to open the certificate selection popup.
5. Choose the applicable certificate and select **OK**.

   Note*:* Ensure the certificate being selected is for ID or Authentication Purposes. Other certificates will not work.

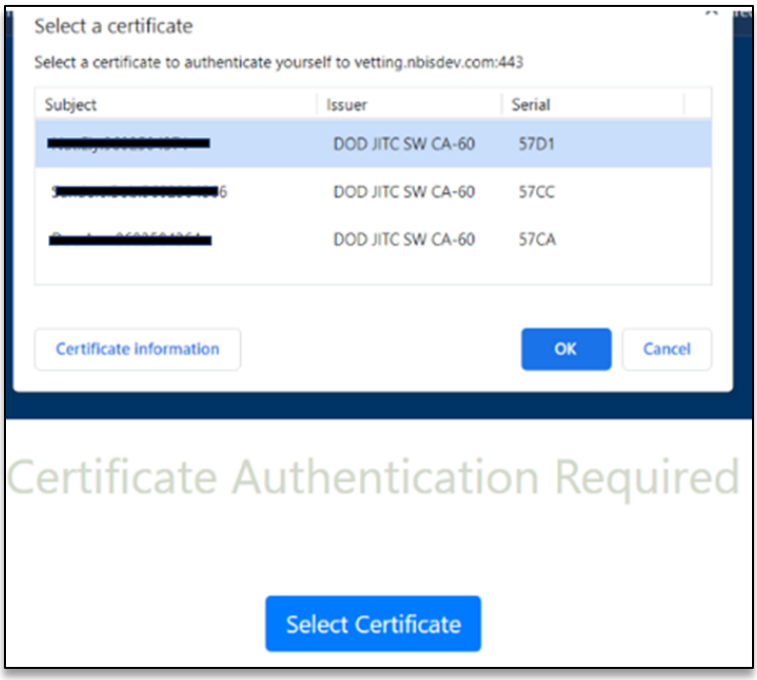


Figure 1-4: Certificate Selection

6. A Certificate enrollment processing review is conducted to check for authenticity and validation of the submission.

7. Review the returned certificate information and select **Confirm Certificate** to continue.

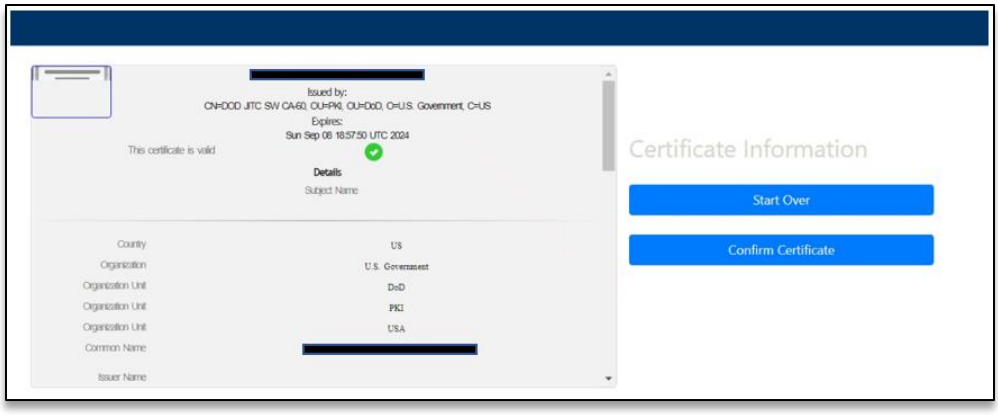


Figure 1-5: Certificate Review

8. 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.

Figure 1-6: SSN & DOB Authentication

9. Select **Logout** to complete the Certificate enrollment process.

   Note*:* Make a note of the *Enrollment Submission Code* for future troubleshooting should there be issues logging in with the persona.

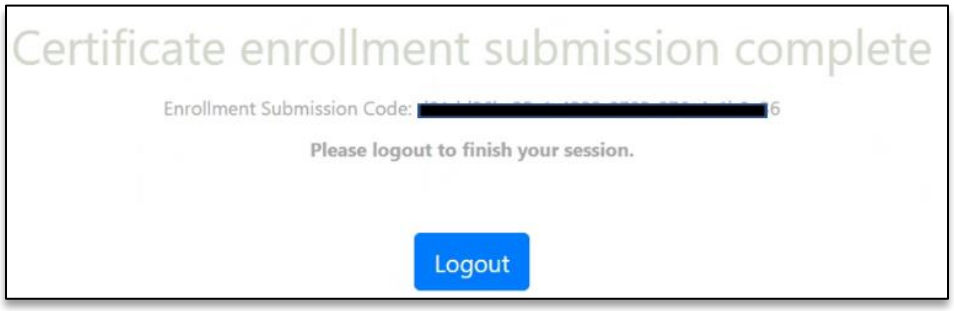


Figure 1-7: Certificate Enrollment Complete

Users in NBIS will need to have their CAC enrollment reset if they change CAC cards or information was entered incorrectly when registering a persona to their CAC. To request a reset, contact your **User Manager**.

1.2.2 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.

10. From the Welcome to NBIS Investigation Management System email, select the link **Click here to access NBIS Enterprise Portal**. Bookmark the link as needed.

Figure 1-8: NBIS Portal Email

11. Review the Terms of Service and select **I Accept.**

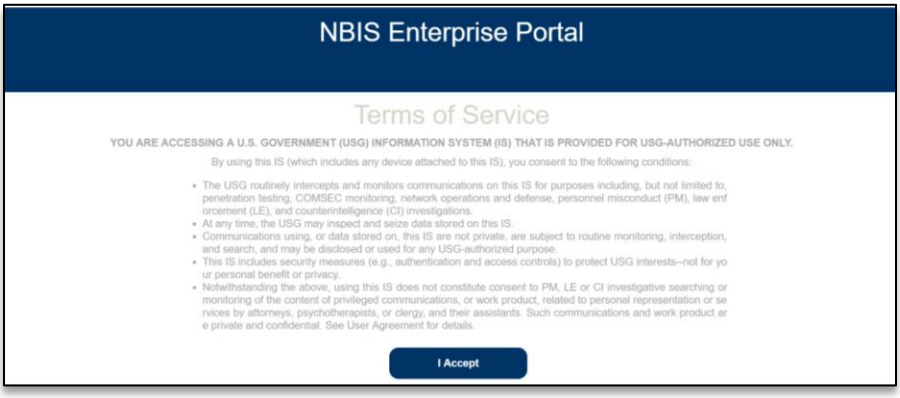


Figure 1-9: Terms of Service

12. Use the **Select Certificate** button to open the certificate selection popup.

13. Choose the applicable certificate and select **OK**.

    Note*:* Certificate selected must match the previous certificate used in the enrollment process.

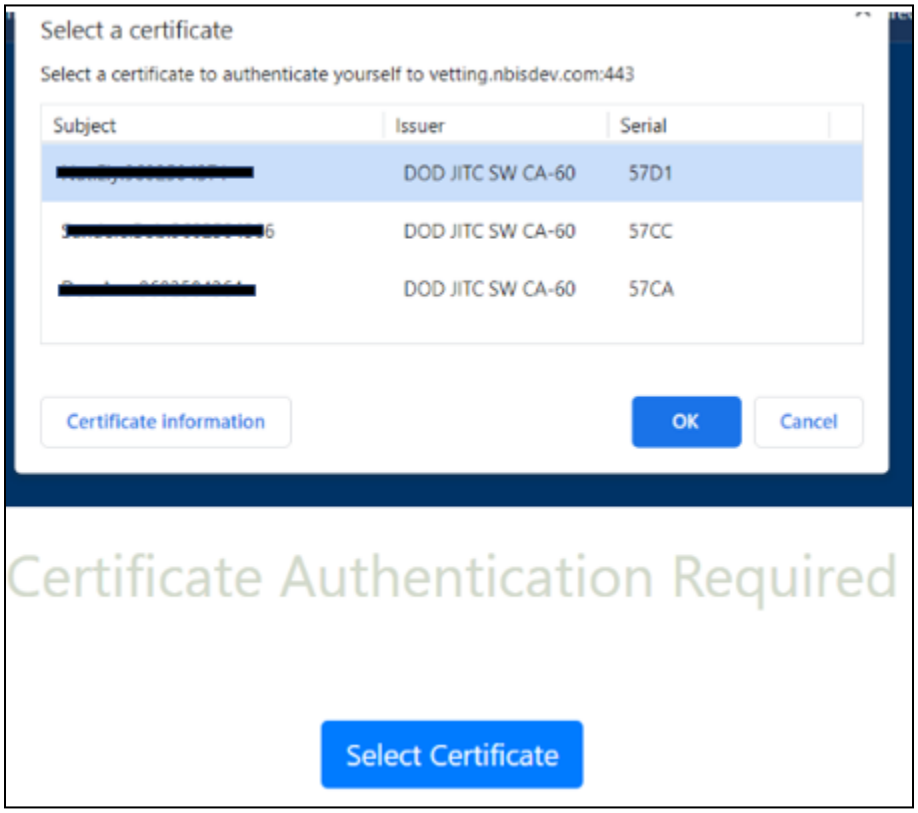


Figure 1-10: Certificate Selection Screen

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.

1.2.3 MULTI-PERSONA USERS

If you have more than one persona linked to your CAC card, you will be prompted to select which persona to login as. After selecting a Persona, you will be logged into the NBIS system and have access to the selected organizations and roles configured in that persona.

Note: For users with multiple personas, only the capabilities and access for the selected persona will be available to you during that session. Other personas access will not affect your current session.

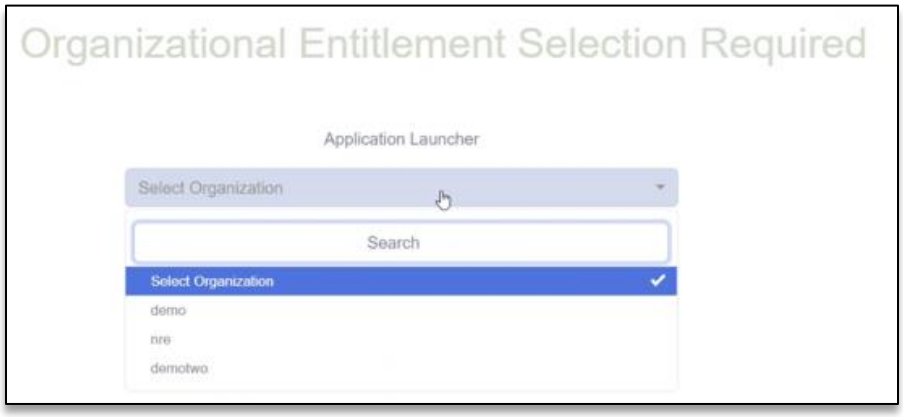


Figure 1-11: Multiple Persona Selection

1.2.4 CONCURRENT SESSIONS

NBIS is limited to 1 (at maximum) concurrent session. Concurrent Sessions are how many sessions a user can login to at the same time. A user cannot be simultaneously logged into NBIS from different browsers or different computers at the same time. If you attempt to login to NBIS while another session is active, NBIS will block the active concurrent session. You will need to close the browser and may have to wait up to 10 minutes before navigating to the URL to login again.

Figure 1-12: Current Session Error

Single Browser

Logging in on the same computer and/or same browser is handled as one session. While you can login and open another tab in the same browser to the NBIS URL, NBIS will auto refresh the first tab to the same NBIS window as the newly opened tab.

1.3 General Use and Information

1.3.1 USER ROLE TO USER GUIDE MAPPING

The table below maps user roles to the relevant user guide. This table can be used to direct you to the appropriate user guide based on your assigned user role(s).

Table 1-2: User Role to User Guide Mapping

Admin Guide	Service Provider Guide	Agency User Guide
System Manager* NBIS Financial Manager Onboarding Manager	Distribution Manager Notification Manager Onboarding Manager Operations Manager Order Form Template Manager Org Assignment Manager Org Manager Org Relationship Manager Org Workload Manager Program Tag Manager Reports Manager Scoping Manager Team Manager Team Structure Manager User Manager Workflow Manager	Adjudicator Authorizer Appeals Processor Case Processor Component Adjudicator CV Analyst Enrollment Manager Facility Security Officer Field Analyst Initiator Investigator Leads Analyst Polygraph Preparer Quality Reviewer Reviewer Screener Special Security Officer Subject Manager Subject Profile Editor Subject Viewer Task Reassignment Validator

***NBIS Level Workflow Builder & Module Configuration**

A **System Manager** can access Workflow Builder and configure/validate a workflow at the NBIS level for the Component and Interim Adjudication phases.

Refer to the **NBIS Service Provide Guide** - Workflow Builder & Module Configuration section for instructions on how to create and configure a workflow.

1.3.2 GETTING HELP INSIDE NBIS

Tooltips throughout the application can be displayed in various ways. There are three types of help available in the application: Hovers, Smart Info Icons, and Hyperlinks.

1. **Hover:** Certain fields may have on-hover descriptions that appear when the mouse hovers over the field.

Figure 1-13: Create Assignment Screen Showing Hover Tip

2. **Smart Info Tips:** Additional information or help appears in two ways:

When an encircled question mark icon ⓘ or an encircled lowercase "i" ⓘ that appears next to a label or field is selected.

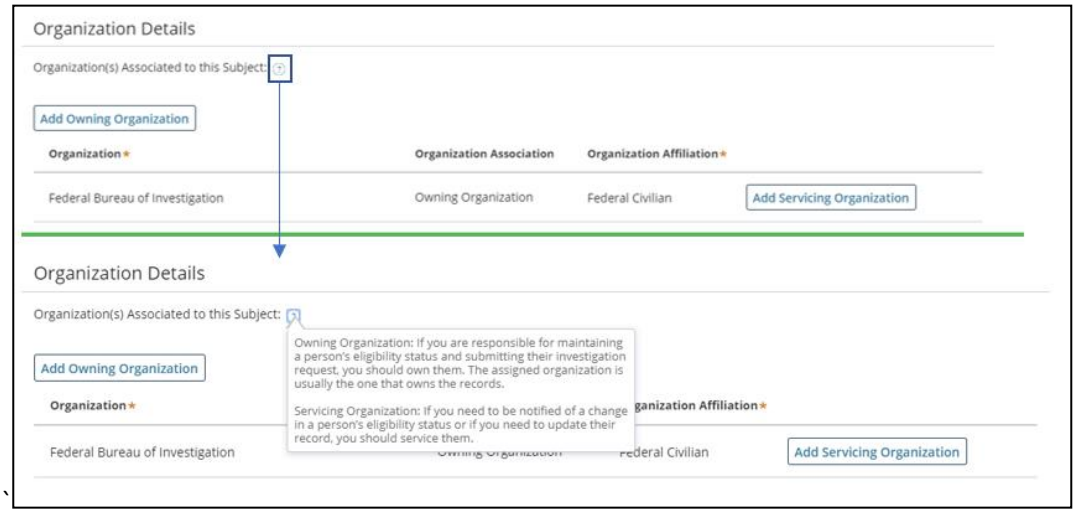


Figure 1-14: Visual of Smart Info Tip

3. **Hyperlinks:** Hyperlinks display a popup bubble or window with more information when selected.

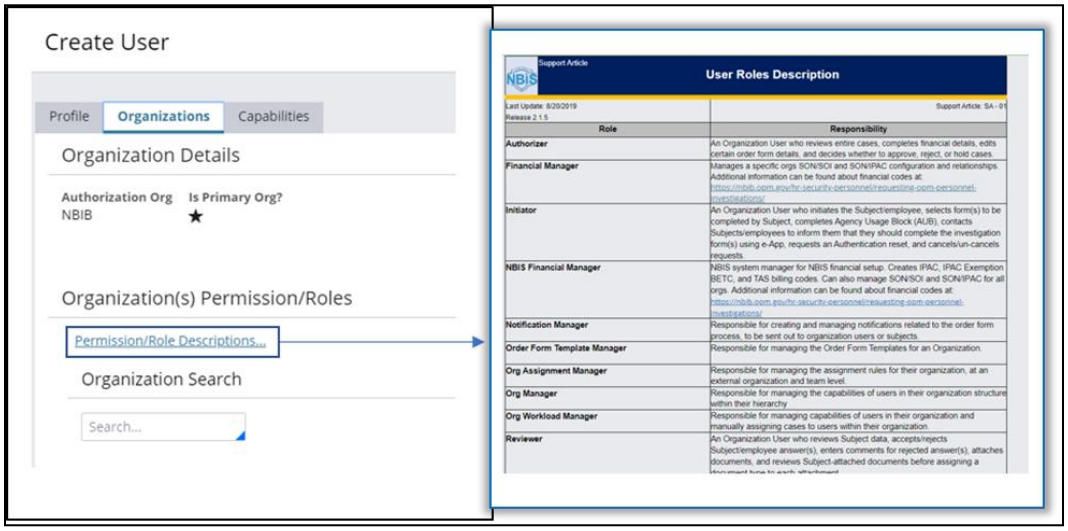


Figure 1-15: Hyperlink Opening to Roles Description Document

1.3.3 DASHBOARD

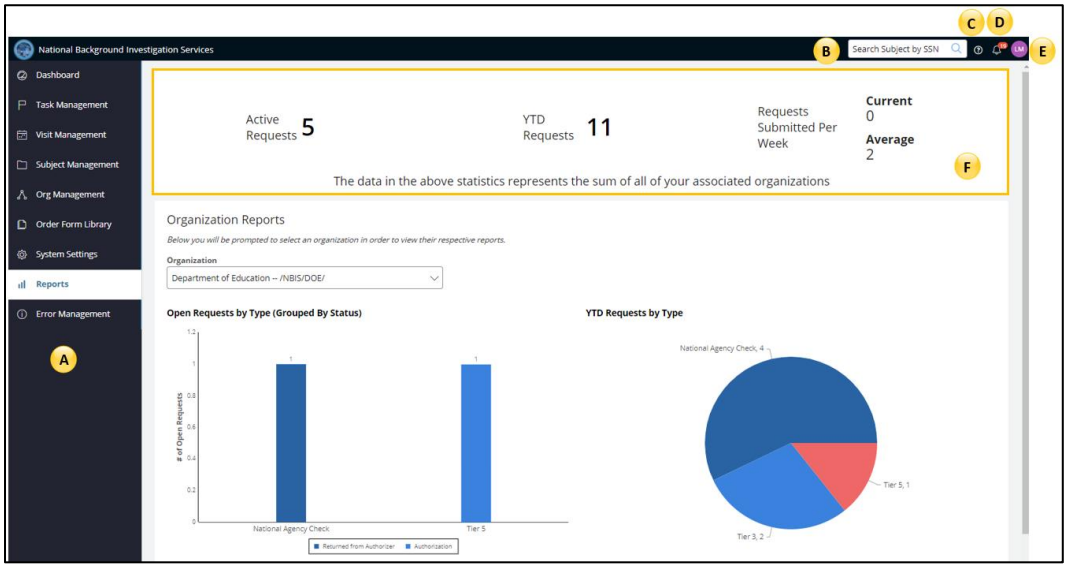


Figure 1-16: Application Dashboard with Identifiers

A. **Navigation Menu** – Dashboard, Task Management, Subject Management. When the page is at 100% zoom and up, a menu bar instead of the left navigation menu will be visible. Depending on your zoom level and monitor resolution, select from the top left select the hamburger icon ☰ to display the navigation menu if not already displayed.

B. **Global Subject Search** – Search for subject by SSN. If the subject exists, you will be brought to the subject's profile. If the subject does not exist, you will be brought to the Create New Subject page.

C. **NBIS Help** – Help menu that displays a selectable link for DCSA's online ticket portal, the service desk phone number, and the NBIS version number

D. **Notifications** – Shows a list of notifications to the user, and a link to the case request depending on the user's roles.

E. **My Profile** – Displays the user's icon (user's initials) and once selected, the user can view their Profile or Log off.

F. **Active Requests –** The sum of all open requests from your associated organizations
YTD Requests – Submitted and cancelled requests to date for current Fiscal Year

1.3.4 NAVIGATION MENU

In the application, the left navigation menu is always visible and accessible to users as they navigate through different screens. However, the content that is visible in the menu varies based on the user's screen size or the browser zoom percent setting. If the screen is zoomed in to a certain point, the labels for the tabs in the menu may be hidden and only the icons will display.

Depending on your zoom level and monitor resolution, the hamburger icon ☰ might be present instead of the navigation menu.

The access permissions/roles you are granted determine which items are visible in the left navigation menu. An Organization User may be granted one or multiple roles by the **User Manager**.

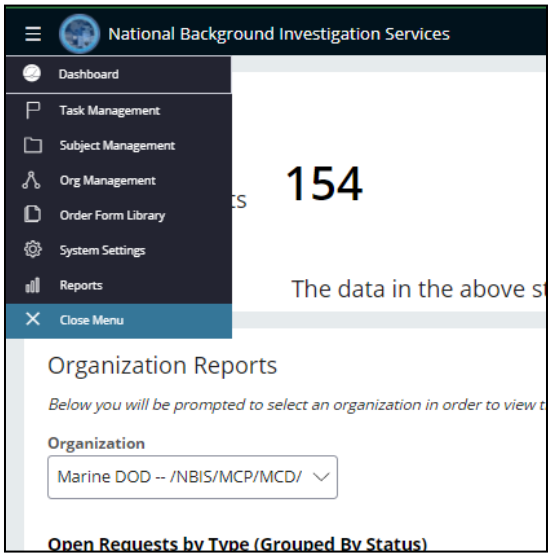


Figure 1-17: Navigation Menu on Landing Page

1.3.5 DROP-DOWNS AND COMBINATION FIELDS

For regular drop-downs, it will jump to the first available entry based on the character you just pressed. For example, pressing "A" would select "Alabama" and the up and down arrow keys can be used to navigate through the available results while focus is on the drop-down field. Once choices are displayed for a drop-down field, the user can select any choice and have it automatically entered in the field.

Quick Tip: If the field isn't showing a list of possible values, pressing the down arrow key on the keyboard will prompt the list to appear on screen. Nothing will appear if there are no values applicable to the field.

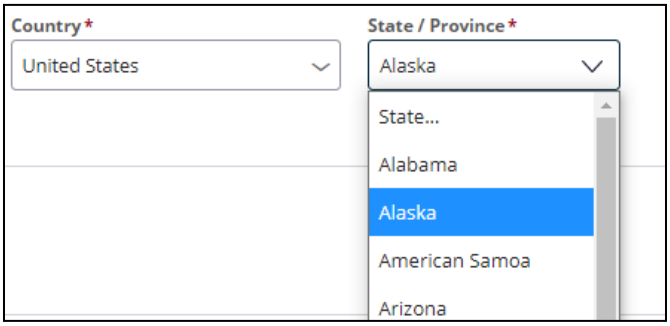


Figure 1-18: Regular Drop-down

Some combination drop-downs in the application allow for the user to type in characters also. The entered characters will start filter or autocomplete the available results for the selected field. If the characters entered do not have any matches to available results, a "no results found" message will be displayed. Entering text is not required, these fields can be used just like a normal dropdown. Combination Fields can be identified by a blinking cursor once selected.

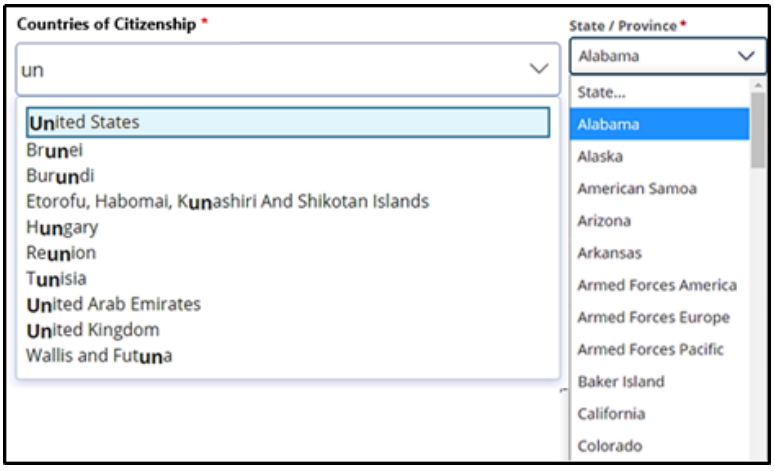


Figure 1-19: Citizenship Drop-down with Auto Complete

1.3.6 TABLES

The tables in the application share common designs for how to sort, filter, and view the rows of data.

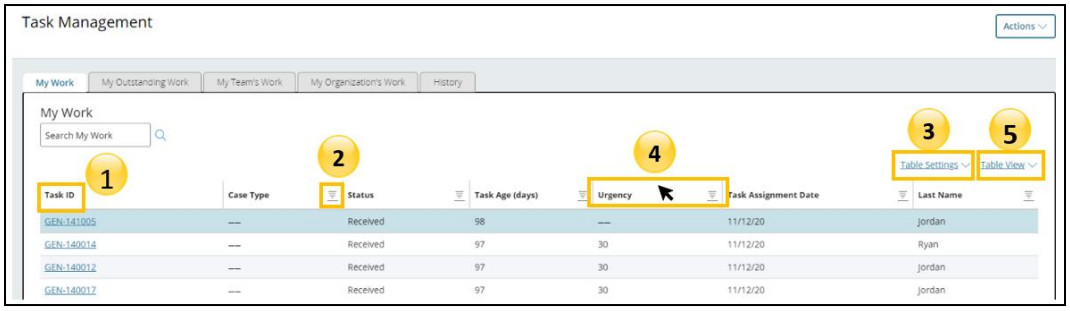


Figure 1-20: Table Configuration in Task Management

1. **Sort by Column** – Select the column header, like Task ID for example, to sort the table by the data in that column.
2. **Filter by Column** – Select the triangle icon to the right of the column header. A small pop up will appear where you can choose values in that column to filter the table by.

For some tables, the ability to customize the view is available. If so, then you will see the **Table Settings** and **Table View** links on the table.

3. **Customize Columns Visible** – Select **Table Settings** to view a list of all the columns available for the table. You can check or uncheck to change the columns that are visible.
4. **Rearrange Columns** – Click anywhere inside the column header and drag to reposition the columns in a different order.
5. **Save Customized Table View** – Select **Table View** and then **Save Table** to save the columns that you configured for the table. You can also select Delete Saved Table to revert to the default view and remove your configurations.

Other Tables throughout the application may have additional actions built in like delete, expand/collapse functionality, or additional actions.

Delete – Select the trashcan icon to delete an entry in a table.

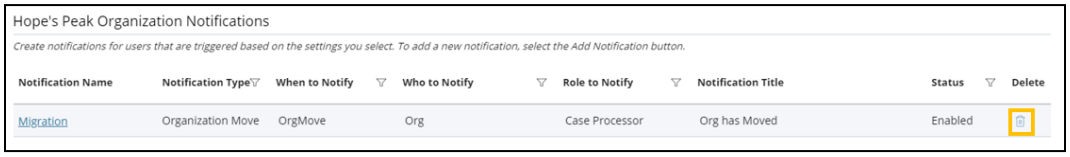


Figure 1-21: Notifications Showing Delete

Expand/Collapse – Select the expand icon to expand a table entry. Select the collapse icon to collapse the group.

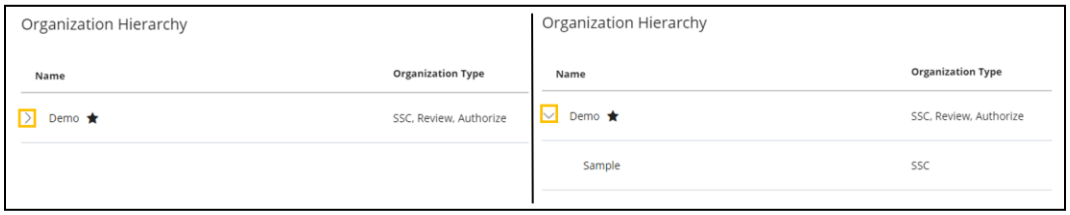


Figure 1-22: Org Hierarchy Showing Expand/Collapse

Additional Actions – Select the ellipses icon for more actions on a table entry.

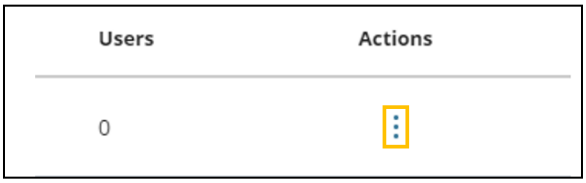


Figure 1-23: Actions Icon in Table

2 Task Management

Task Management can be accessed from the left navigation menu. It is where case operators (**Reviewers, Authorizers, and Case Processors, Subject Managers, Initiators, FSO**) can view the work assigned to them and review the cases they have worked on previously. It is also where managers can view the work assigned to their organization or teams. All tables in the tabs are customizable and additional columns can be added to show case or alert specific details. See Tables section for how to customize table layouts.

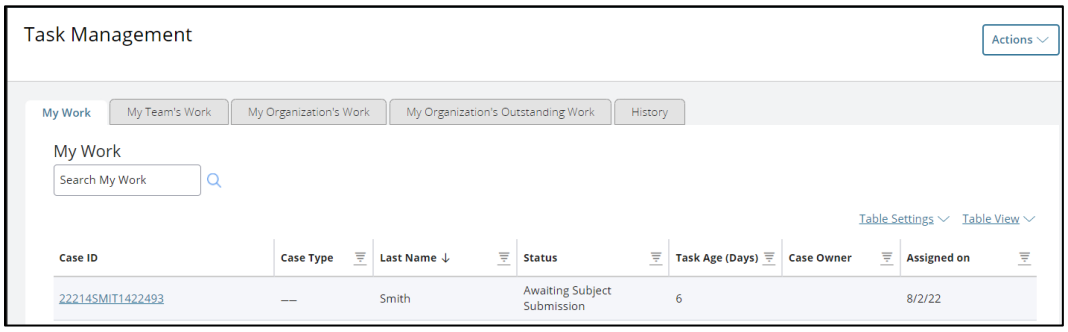


Figure 2-1: Task Management

2.1 Tabs within Task Management

There are multiple tabs within Task Management that allow for different purposes. The tabs visible to you varies based on your assigned roles.

My Work – This displays a list of all tasks currently assigned to you.

My Outstanding Work – This displays a list of cases where you are the case owner.

My Team's Work – This tab only applies to non-agency cases and is only visible when you are a **Team Manager**. Cases will only display if you are assigned to a team. This tab will display a list of tasks assigned to your team well as sub-teams' work.

My Organization's Work – This tab is only visible when you are an **Organization Workload Manager**. This tab will display a list of all cases or items in the organization currently (assigned or unassigned) as well as cases within the organization hierarchy. There will be a drop-down to select the organization you want to display.

My Organization's Outstanding Work – This tab is only visible when you are an **Organization Workload Manager**. The tab will display a list of adjudication cases pending subtask completion. There will be a drop-down to select the organization you want to display.

History – This tab will display a list view of cases you have worked on.

2.2 Reassign a case from Task Management (Bulk Reassignment)

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

1. While in **Task Management**, select **My Team's Work, My Organizations Work** or **My Organization's Outstanding Work**.
2. From the **Actions** drop-down, select **Reassign Tasks**.
3. Select the **checkboxes** of desired cases/tasks to reassign or select the **Select All Tasks** checkbox.

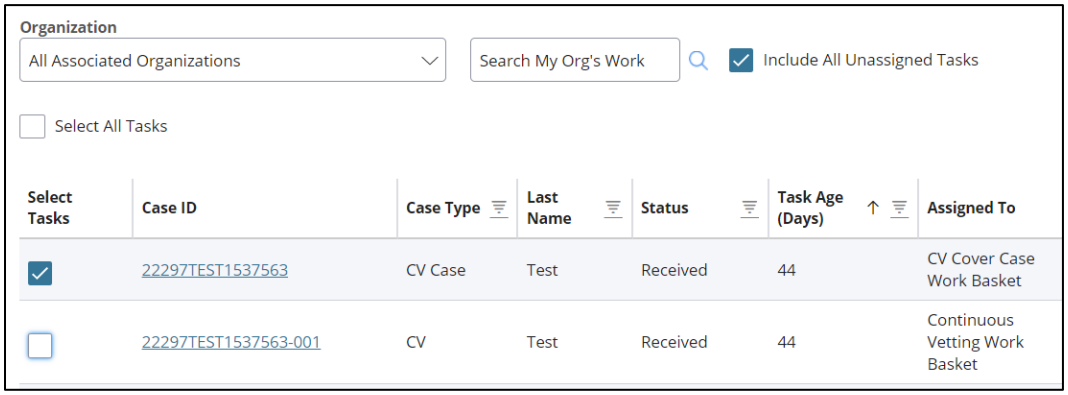


Figure 2-2: Reassign Task Selection

4. Select **Reassign** at the bottom of the page.

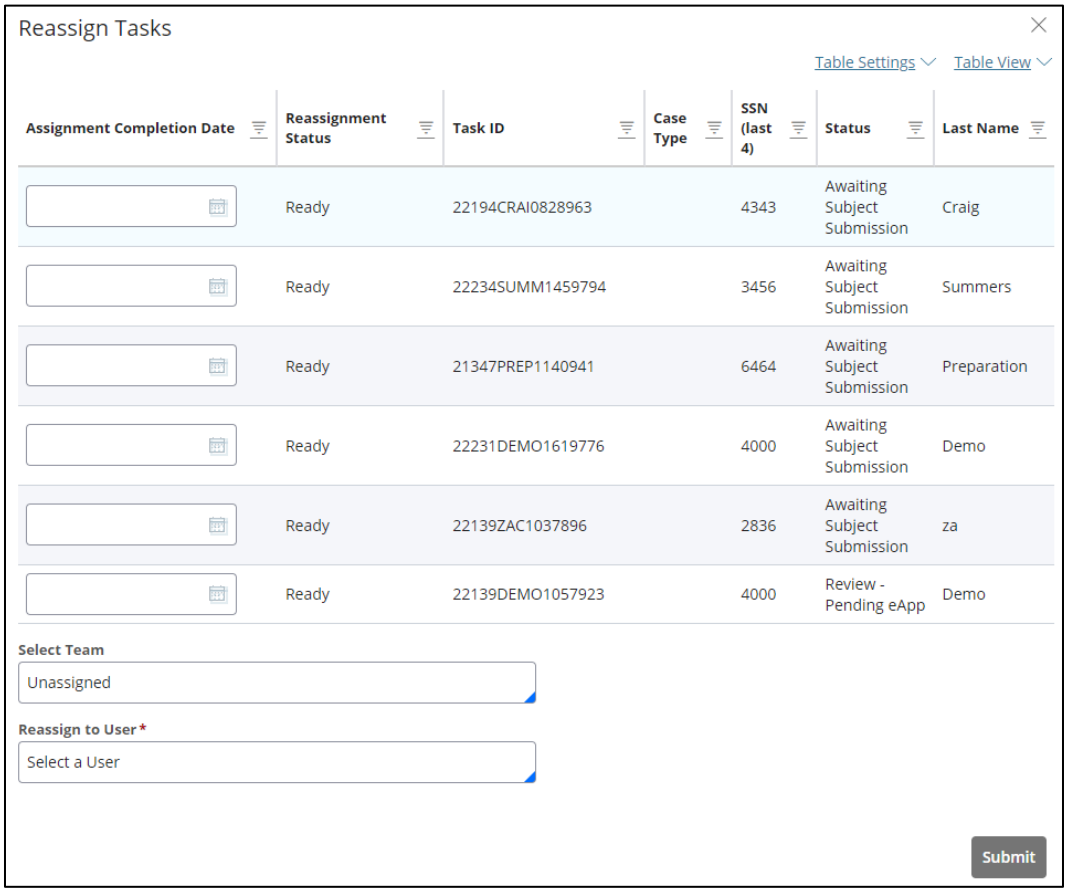


Figure 2-3: Reassign Task

Note: The **Select Team** field does not apply to SSC, FSO, Review, or Authorize organizations and cases. When applicable, your team will be pre-populated in the **Team Name** field in read-only mode when reassigning from **My Teams Work**. Users in your team will be populated in the **User** drop-down.

Note: The **Org Workload Manager** is able to select an **Assignment Completion Date** (ACD) when conducting a reassignment for Leads cases. The ACD box will be disabled for all other case types.

5. From the **Reassign to User** drop-down, select a desired user or the workbasket to reassign the case request.
6. Select **Submit**.

   A success or failure message will appear. Once you close the modal, the case list will repopulate reflecting the reassignment.

3 User Management

User Managers create and manage users in their specific organization. User management is accessed from the **Org Management** tab in the left navigation menu.

3.1 Create a User

This section will cover creating a new user in NBIS. If the user (SSN) already exists, the existing user record will display.

3.1.1 ADD USER

1. From the left navigation menu, select **Org Management**.
2. Select the **Users** tab.

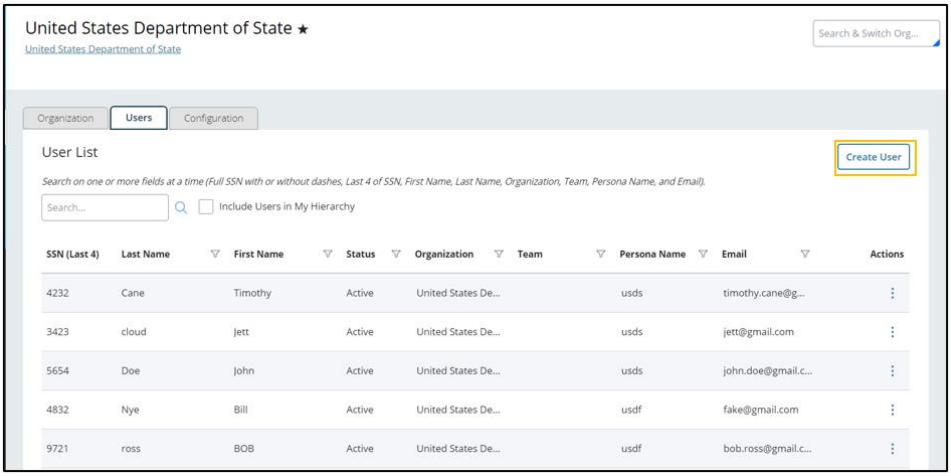


Figure 3-1: User Management

3. From the right, select **Create User** button.
4. In the SSN Search text box, enter the user's social security number and select **Continue**. If the user *does not* exist in the system, the Create User screen displays.

   Note: If the user already exists, the existing user record will display, see View User for more information. If you need to add a new persona to the user, please proceed to the Add Persona section.

5. Fill in the required user information under **User Profile.**

   Note: The SSN and Date of Birth are required for the user's initial enrollment. Please ensure they are entered correctly to prevent further issues. User Managers will be able to modify the SSN and DOB after the user is created.

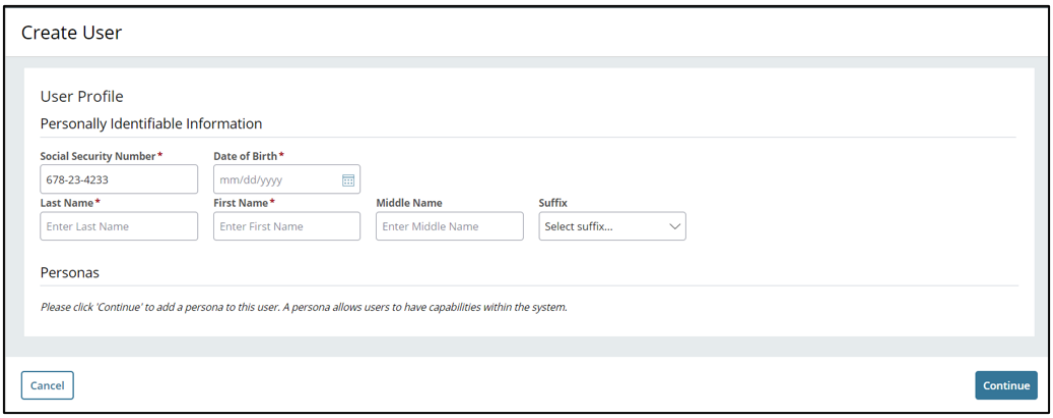


Figure 3-2: Create User

6. After filling out all user information, select **Continue** to create a persona to add a user.

   Note: A Persona represents an account with its roles and privileges that the user will have for the org(s) associated to the persona. A persona will also represent an account the user will use to login to the system. A user can have multiple personas that are associated to multiple orgs.

3.1.2 ADD PERSONA

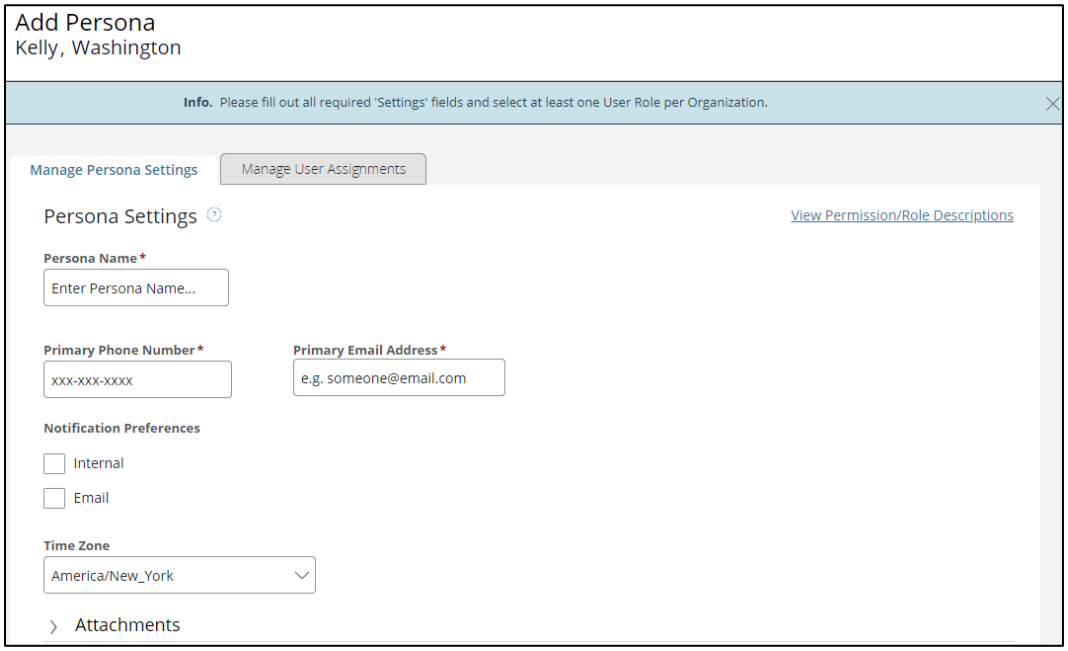


Figure 3-3: Manage Persona Settings

1. In the **Manage Persona** tab, a user manager can enter the required information for the Persona.

   Note: Persona Name cannot be changed once the Persona is created.

2. Select a **Notification Preference** option. The **Internal** option displays notification alerts in the top right corner of the application. The **Email** option will route notifications to the primary email address entered for the user.
3. Select the **Time Zone** drop-down below notification preferences and ensure the correct time zone is set for the persona.
4. Select **Add Attachment** to upload required documents for the persona, and then fill in the required attachment fields.

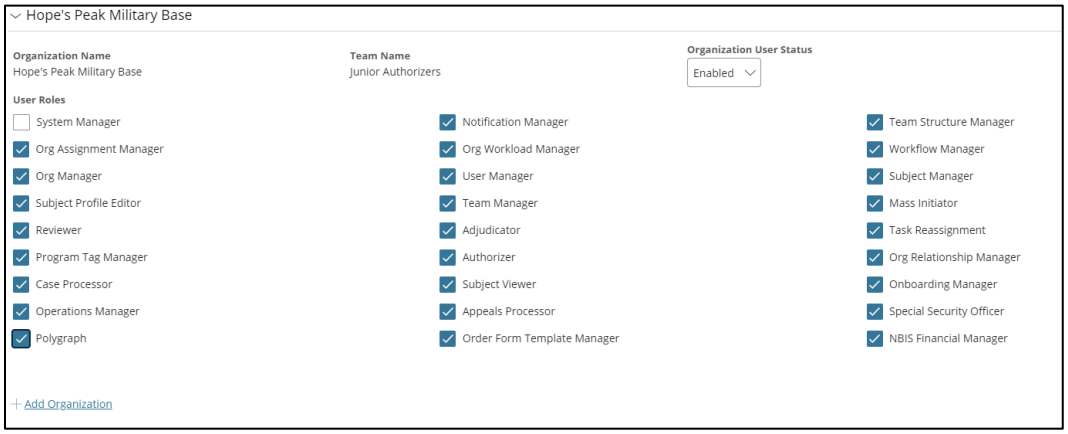


Figure 3-4: Manage Persona Settings

5. The organization context should be pre-populated based on the org in which the User Manager is creating the Persona. Select the **roles** the user will be granted within the organization.
6. To add the user to an additional organization, select **Add Organization**. A modal will appear where you can search for an organization to add. The list of available roles within the organization will display to be selected.

   Note: You must select at least one role for each organization.

   Note: The **Org User Status** is enabled by default.

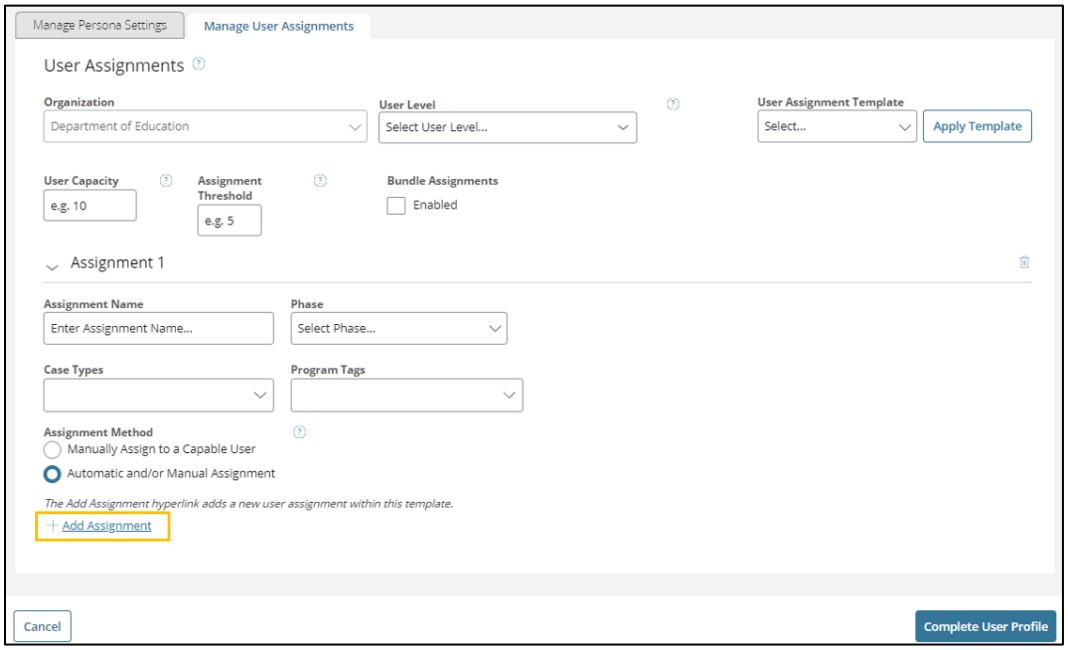


Figure 3-5: Manage User Assignments

7. Select **Manage User Assignments** tab and fill in the required information related to managing the types of tasks users can be assigned based on certain task attributes.
8. From the **Organization** drop-down select your desired organization. This allows you to specify capabilities for each of the organizations a persona is associated.
9. For the selected organization, select a **User Level**, if applicable.

   Note: User Level does not apply to Agency users.
10. Select and apply any **User Assignment Templates**, if applicable.

    Note: Multiple user assignment templates can be applied to a user. However, if the user already has a user assignment for a particular phase, the assignment for that phase in the template will not be applied. See User Assignment Templates for reference.
11. If the receiver will be receiving automatically assigned work, configure the **User Capacity** and **Threshold Values**.

    Note: **User Capacity** sets the maximum number of cases a persona may be automatically assigned. **Threshold** sets the minimum number of cases a persona can have in their worklist until the system queries for cases that match the persona's capabilities and adds cases to the user's worklist up to the capacity. These fields are required if **Automatic and/or Manual Assignment** method is selected for an assignment.

    Note: A user can be manually assigned cases that may exceed their User Capacity amount if the **Manually Assign to a Capable User** button is selected.

12. For users working CV alerts and cases, select the **Bundle Assignments** checkbox to group assignments for each subject.
13. Select **Add Assignment** to add an assignment to the persona. Multiple assignments can be added per organization.
    a. Select the **Phase** for the assignment. The phase determines what phase of the case the user can work on.

       Note: Additional fields will populate depending on the phase selected.

       For CV Alert, Continuous Vetting, and Adjudication phases an Affiliation Category drop-down will appear for the user's organization affiliation category.

    b. Select the **Assignment Method** for the user assignment. Capable means that the persona can access and work on a case with certain attributes, but only if they are manually assigned the case, not through automatic assignment. System Assigned means that the persona can work on and will be automatically assigned the case or task.

    c. Select the appropriate **Case Type** and **Workflow Status** options for the persona. These sections indicate the types of cases or tasks you want the user to be capable of working on.

    d. Select any applicable **Program Tags** needed for this assignment configuration. See the Program Tag Management section for more information about their applications.

Note: For Investigation organizations, user assignments will be configured in the Investigation control organization and will be inherited by sub-organizations.

14. At the bottom right of the User Profile, select **Complete User Profile** to finish creating the persona and add the user to your organization.

    After creation, the user will receive two emails to the primary email address entered in the Manage Persona Settings section. The emails will contain instructions and links for the user to complete Certificate Enrollment procedures and gain access to the NBIS Enterprise Portal. See section Logging In for additional information.

3.2 Viewing a User

1. In Org Management, select the **Users** tab to view a list of users within the selected Organization.

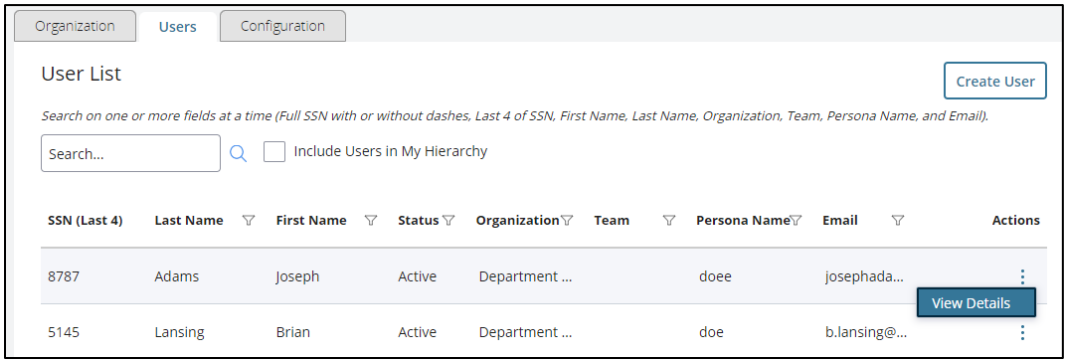


Figure 3-6: User Management

2. From the **Actions** column, select the **ellipses** next to the user row you wish to view, then select **View Details**.
3. Select the **Persona Name** to view the specific persona details.

3.2.1 RESET AUTHENTICATION FOR PERSONAS

Persona authentication resets are required if enrollment fails or if a CAC/PIV card is changed.

4. From the **Actions** column, select the **ellipses** next to the persona.
5. Select **Reset Authentication** to re-enroll a persona and restart their authentication process if necessary. If the emails are sent to the persona successfully, there will be a message indicating so. Otherwise, a failure message will appear.

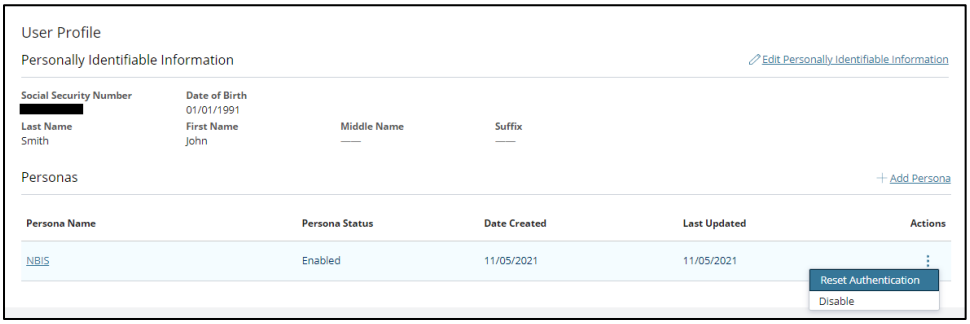


Figure 3-7: User Profile Ellipses Menu

3.2.2 DISABLE PERSONA

6. From the **Actions** column, select the **ellipses** next to the persona.
7. Select **Disable** to disable a persona, which will apply to all organizations they are part of. The **Enable** option will appear once a persona is disabled if you want to re-enable it. A pop-up will appear displaying all tasks assigned to the persona
8. From the **Reason for Disabling Persona**, select a **Reason** and enter an **Explanation**.

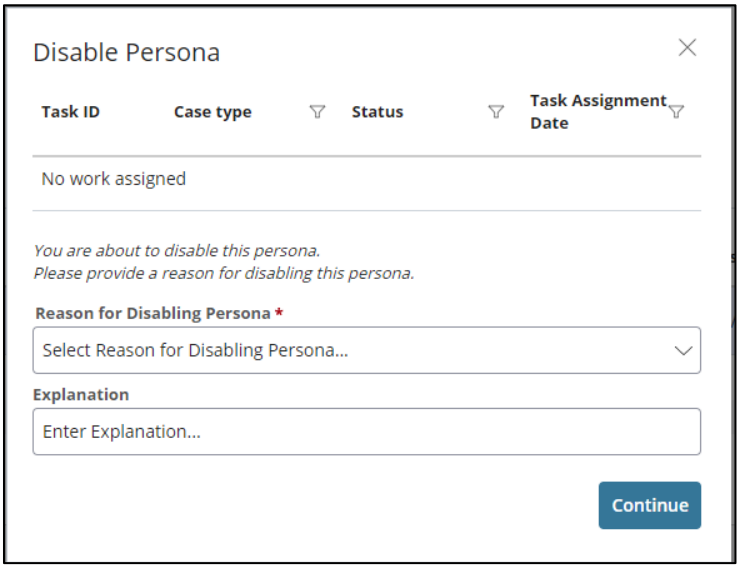


Figure 3-8: Disable Persona Pop-up

Note: If you Disable a persona, all cases in that user's worklist for their organization will return to their respective organization workbasket

9. Select **Continue**.

3.3 Editing a User

3.3.1 EDIT USER PII

1. In the **User Profile**, select **Edit Personally Identifiable Information**.

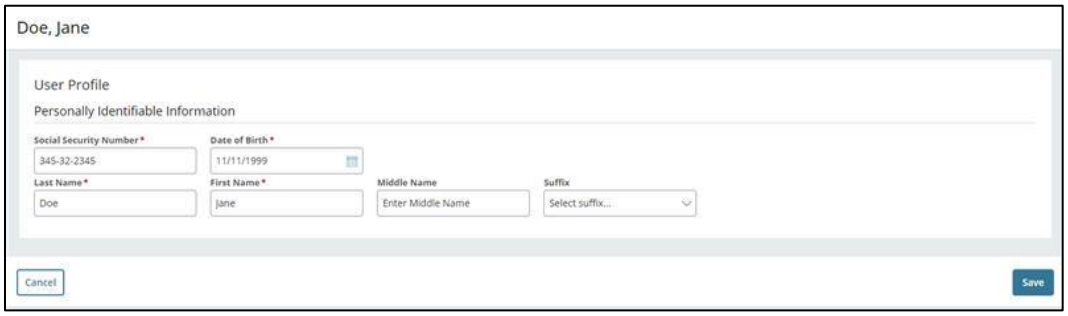


Figure 3-9: Edit User Profile PII

2. Make the changes and select **Save**.

3.3.2 EDIT USER PERSONA INFORMATION

1. In the User Profile, select a **Persona Name** to edit.
2. From the bottom right of the Persona screen, select **Edit** to edit the persona details, add attachments, edit the org associations and roles, or edit the assignments.

   Note: A persona can be removed from an organization if they have no pending or assigned tasks. A persona is required to have at least one org and one role within the org.

   Note: When editing user assignments, it is up to the **Org Workload Manager** to remove any cases from the user they should no longer be able to access. See Reassign a case from Task Management (Bulk Reassignment) for more information on how to reassign cases.
3. Select **Save** to save the changes.

4 User Configurations at the Organization Level

The **User Manager** has access to two configuration tabs within **Organization Management**. The **User Levels** and the **User Assignment Templates** are additional configurations for managing the work users are capable of.

4.1 User Levels

The **User Manager** can create User Levels within Org Management that can be applied to users. User levels dictate which workflow actions are available for a given task within your organization. See Add Persona for application of user levels.

User Levels are not applicable to SSC, Review, Authorize, and FSO Organization types.

To view all User Levels:

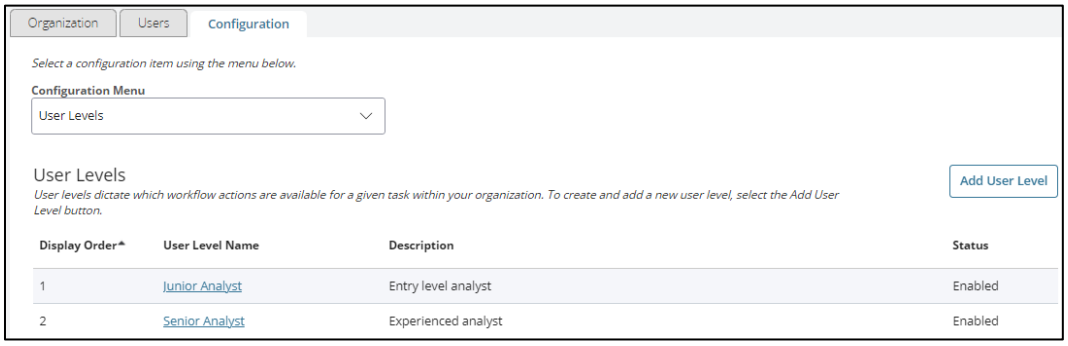


Figure 4-1: Org Management - User Levels

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the Configuration Menu, select **User Levels**.

To add a User Level:

1. Select **Add User Level.**

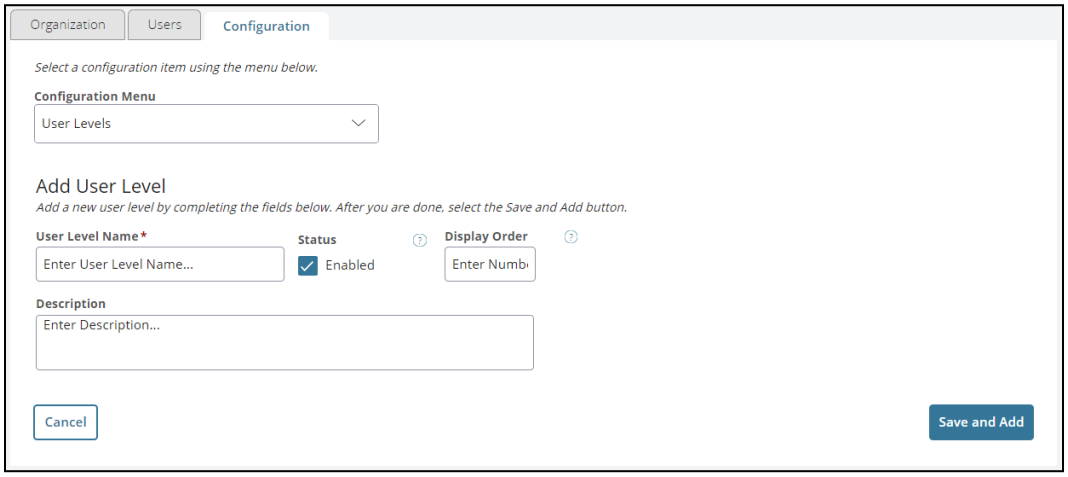


Figure 4-2: Add User Level

2. Complete the required fields and select **Save and Add**.

To view a User Level:

3. From the **User Level Name** column, select a **User Level**.

To edit a User Level:

4. From the **Actions** drop-down, select **Edit User Level** and Update as needed.
5. Select **Save User Level**.

To delete a User Level:

6. From the **Actions** drop-down, select **Delete User Level**.

4.2 User Assignment Templates

User Assignment Templates can be used to apply assignment attributes to multiple personas. User Assignments determine a user's capabilities and are managed by the **User Manager** role. Multiple assignments for the same phase can be configured. See Add Persona for information on the application of user assignment templates.

Multiple user assignment templates can be applied to a user. However, if the user already has a user assignment for a particular phase, the assignment for that phase in the template will not be applied.

To view all User Assignment Templates:

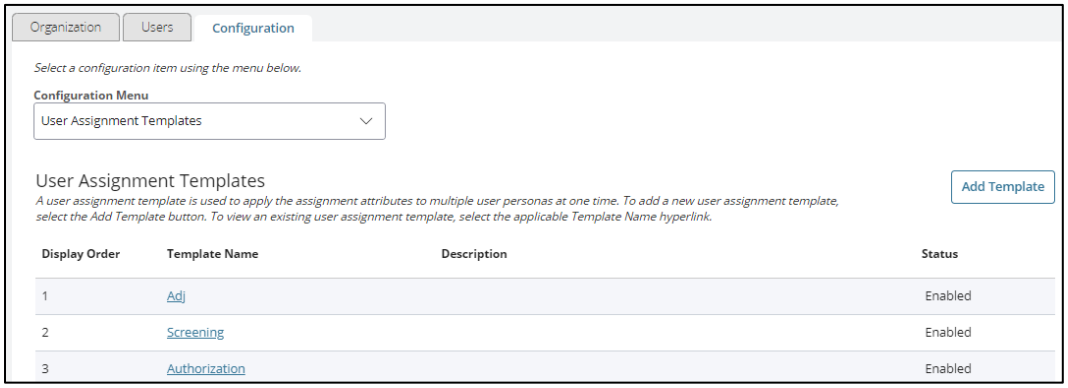


Figure 4-3 User Assignment Templates Landing Page

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the Configuration Menu, select **User Assignment Templates**.

To add a User Assignment Template:

4. Select **Add User Level.**

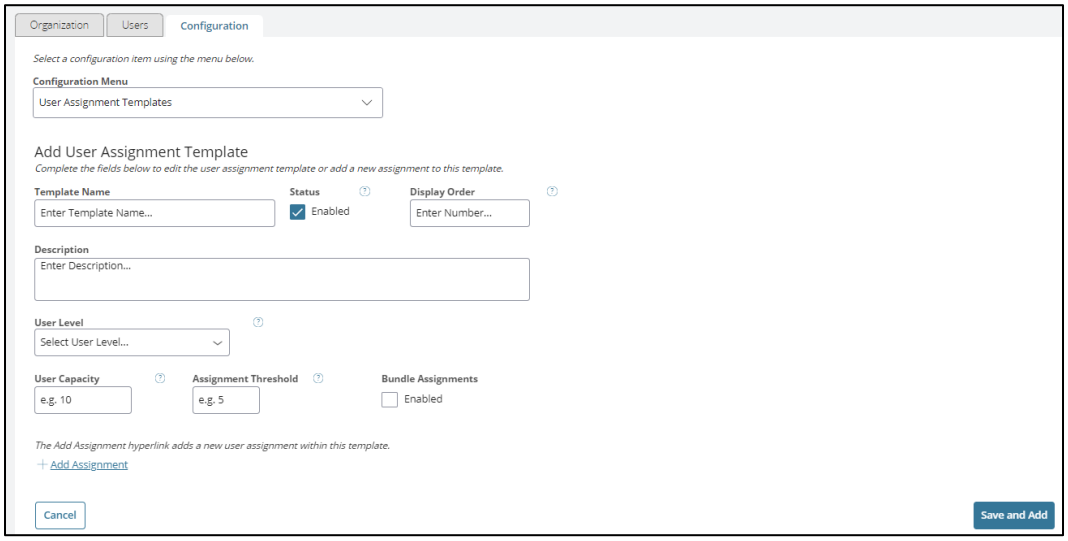


Figure 4-4: Add User Assignment Template

5. Provide the Template information.
6. To allow automatically assigned work, configure the **User Capacity** and **Threshold Values**.

   Note: **User Capacity** sets the maximum number of cases a persona may be automatically assigned. **Threshold** sets the minimum number of cases a persona can have in their worklist until the system queries for cases that match the persona's capabilities and adds cases to the user's worklist up to the capacity. These fields are required if **Automatic and/or Manual Assignment** method is selected for an assignment.

   Note: A user can be manually assigned cases that may exceed their User Capacity amount if the **Manually Assign to a Capable User** button is selected.
7. Optionally check the **Bundle Assignments checkbox** to enable CV alert bundling for this user. When this is enabled and an alert is assigned, all other unassigned alerts for the same subject will be assigned to this user, regardless of User Capacity.
8. Select **Add Assignment** to add an assignment to the persona. Multiple assignments can be added per organization.
   a. Select the **Phase** for the assignment. The phase determines what phase of the case the user can work on.

      Note: Additional fields will populate depending on the phase selected.
   b. Select the **Assignment Method** for the user assignment. Capable means that the persona can access and work on a case with certain attributes, but only if they are manually assigned the case, not through automatic assignment. System Assigned means

that the persona can work on and will be automatically assigned the case or task.

c. Select the appropriate **Case Type** and **Workflow Status** options for the persona. These sections indicate the types of cases or tasks you want the user to be capable of working on.

d. Select any applicable **Program Tags** needed for this assignment configuration. See the Program Tag Management section for more information about their applications.

9. Complete the required fields and select **Save and Add**.

To view a User Assignment Template:

10. From the **Template Name** column, select a **User Assignment Template**.

To edit a User Assignment Template:

11. From the **Actions** drop-down, select **Edit Template** and Update as needed.
12. Select **Save**.

To delete a User Assignment Template:

13. From the **Actions** drop-down, select **Delete Template**. A confirmation window will appear.
14. Select **Delete** to delete the template.

5 Configuring Different Organization Types

This chapter should be referenced when configuring the different org types found in NBIS. Each section contains a summary explanation of the org type and the required user roles for the org. Organization configurations are separated into required and optional within each section. Both the required and optional configurations tables contain links to other chapters/sections in the guide. These links will direct users to the appropriate instructions for each configuration type. To see what configurations are available for a given org type, see Org Configuration Reference Table for more information.

5.1 Sections and Roles Applicable to All Organization Types

Table 5-1: Basic Requirements for Org Configuration

Topic	Link
Create the Organization	Creating and Organization
Create the Users	Create a User
Defining Org Relationships	Organization Relationships

Table 5-2: Basic Required Roles for Org Configuration

Role	Purpose
Org Manager	Responsible for managing organization types and functions.
User Manager	Responsible for adding users and modifying their user assignments so they can work on cases.
Org Workload Manager	Responsible for assigning cases through the Actions drop-down for either bulk reassignment or in case reassignment.

5.2 Initiate, Review, and Authorization (Agency) Organizations

Submission orgs are separated into four distinct types: SSC, Review, FSO, and Authorize. SSC/FSO org type and function allows for subject affiliation and initiation into the NBIS system through the Subject Manager role and FSO role respectively. Review/Authorize (R/A) org types need to have either the R/A function or the R/A provider function. To complete a submission case the SSC/FSO Org must also have a form routing configured. SSC Organizations may also receive Interim cases (SAC or NAC) to grant subjects an interim clearance while their background investigation is processing.

The Provider function allows the Organization to be seen by outside orgs to preform R/A for cases. R/A functions allow the org to perform those services on a case.

Required Roles:

Table 5-3: Required Roles for Agency Organizations

Role	Purpose
Subject Manager / Facility Security Officer	Responsible for adding affiliation to subjects and initiating their cases
Reviewer	Tasked with verifying or filling out the submission form
Authorizer	Tasked with adding in billing details, verifying all information is correct, and that the case can be sent to investigations
Workflow Manager	Required to add or edit Form Routing for submission cases
Org Workload Manager	Required to assign work to users to complete assignments
User Manager	required to create new users in the system and edit the user assignments as needed.

Required Configurations:

Table 5-4: Required Configurations for Agency Organizations

Topic	Link
Standard Form (SF) Workflow	Form Routing
Defining Org Relationships	Organization Relationships

Optional Configurations:

Table 5-5: Optional Configurations for Agency Organizations

Topic	Link
Order Form Library	Order Form Template Management
Notifications	Notification Management
Assignment Rules	Assignment Rule Management
User Assignment Templates	User Assignment Templates

5.3 Adjudication/Appeals Organizations

Adjudication organizations require the "Adjudication" type under org details. They are further split into Adjudication Provider and Adjudication functions. Orgs with the Adjudication Service Provider function do not have the ability to implement the services themselves and instead use the services of an org with the Adjudication function in Org Relationships. To receive an Adjudication case from investigations, the org requires an SOI that is mapped in the system settings under SOI Org Mapping Tables. This SOI is input during the case creation or is attached to a subject coming in through investigations. An active workflow is also required in Workflow Builder under Configurations in Org Management.

Component Adjudication (CA) cases can only be created through phase transition from an Adjudication or Appeals organization. A summary of the previous adjudicator's guidelines is generated and attached to the case when it is sent to the Component Adjudication org. Case Processing is completed through a Global NBIS workflow shared by all component adjudication orgs. Routing to CA is determined by the scan of the subject's org affiliation hierarchies up to NBIS, looking for component adjudication orgs. If there are no CA orgs in the hierarchies, all CA providers in NBIS are shown. The results determined from the scan will populate the org selection drop-down in the Phase Transition module for the Case Processor. See **NBIS Agency User Guide** for more information.

Appeals organizations require the "Appeals" type under org details. They are further split into Appeals Request Service Provider and Appeals Request functions. Orgs with only Appeals Request Service Provider do not have the ability to implement the services themselves and use the services of an org with the Appeals function in Org Relationships. Appeals cases can be created on a subject profile, either manually by a Case Processor or through request by a Subject Manager after an unfavorable determination. An Active workflow is also required An Active workflow is also required in Workflow Builder under Configurations in Org Management.

Required Roles:

Table 5-6: Required Roles for Adjudication/Appeals Organizations

Role	Purpose
Case Processor	Primary role required to work on a case and should be paired with an Adjudicator role to access guidelines
Adjudicator	Responsible for selecting guidelines to complete an adjudication case and needs to be paired with the Case Processor role to adjudicate a case.
Operations Manager	Responsible for org configurations and can set up Automatic Assignments, Notifications, Adjudication Workflows, Local Products, Program Tags, and User Levels
User Manager	Responsible for adding users and modifying their user assignments so they can work on cases.
Org Workload Manager	Responsible for assigning cases through the Actions drop-down for either bulk reassignment or in case reassignment

Required Configurations:

Table 5-7: Required Configurations for Adjudication/Appeals Organizations

Topic	Link
Workflow Builder	Workflow Builder & Module Configuration
Defining Org Relationships	Organization Relationships

Optional Configurations:

Table 5-8: Optional Configurations for Adjudication/Appeals Organizations

Topic	Link
Notifications	Notification Management
Assignment Rules	Assignment Rule Management
User Assignment Templates	User Assignment Templates
User Levels	User Levels
Service Catalog	Service Catalog
Teams	Team Management
Program Tags	Program Tag Management

5.4 Continuous Vetting Organizations

Continuous Vetting organizations require the Continuous Vetting org type under Org Details, with the Continuous Vetting and Continuous Vetting Service Provider org functions. To implement CV, there must be an org that implements the CV function or the CV provider function in the hierarchy. If the CV implementor is not the parent organization, it will be routed to the appropriate CV implementor based on the parent organization's internal org relationships. To receive CV cases, subjects must be enrolled in the org's CV Program. An active workflow is required for both the CV Alert and Continuous Vetting phases.

Required Roles:

Table 5-9: Required Roles for CV Organizations

Role	Purpose
Case Processor	Primary role required to work on a case and should be paired with CV Analyst role to view CV alerts and cover cases
CV Analyst	Responsible for processing CV alerts and CV cover cases and needs to be paired with Case Processor to access the case.
User Manager	Responsible for adding users and modifying their user assignments so they can work on cases.
Operations Manager	Responsible for org configurations and can set up Automatic Assignments, Notifications, Adjudication Workflows, Local Products, Program Tags, and User Levels
Org Workload Manager	Responsible for assigning cases through the Actions drop-down for either bulk reassignment or in case reassignment

Required Configurations:

Table 5-10: Required Configurations for CV Organizations

Topic	Link
Workflow Builder	Workflow Builder & Module Configuration
Defining Org Relationships	Organization Relationships
Managing Case and Form Types at an Organization Level	Managing Case and Form Types at an Organization Level
Case Categories	Case Categories

Optional Configurations:

Table 5-11: Optional Configurations for CV Organizations

Topic	Link
Case Progression Exception Rules	Case Progression Exception Rules
Notifications	Notification Management
Assignment Rules	Assignment Rule Management
Service Catalog	Service Catalog
User Assignment Templates	User Assignment Templates
User Levels	User Levels
Teams	Team Management
Program Tags	Program Tag Management

5.5 Screening Organizations

Screening organizations have the Screening org type and have the Screening org function. In order to share screening services externally, the org must also have the Screening Service Provider function. The subjects of any organizations that you share screening services to will appear in your organization's subject management when the **Include Subject in my Hierarchy** checkbox is selected. Screening orgs require an active workflow configured in Workflow Builder. All screening cases from case types configured in the service catalog.

Required Roles:

Table 5-12: Required Roles for Screening Organizations

Role	Purpose
Case Processor	Primary role required to work on a case and should be paired with Screener role to process interim determinations.
Screener	Responsible for processing interim determinations for industry subjects and needs to be paired with Case Processor to access the case.
User Manager	Responsible for adding users and modifying their user assignments so they can work on cases.
Operations Manager	Responsible for org configurations and can set up Automatic Assignments, Notifications, Adjudication Workflows, Local Products, Program Tags, and User Levels
Org Workload Manager	Responsible for assigning cases through the Actions drop-down for either bulk reassignment or in case reassignment

Required Configurations:

Table 5-13: Required Configurations for Screening Organizations

Topic	Link
Workflow Builder	Workflow Builder & Module Configuration
Defining Org Relationships	Organization Relationships
Service Catalog	Service Catalog

Optional Configurations:

Table 5-14: Optional Configurations for Screening Organizations

Topic	Link
Notifications	Notification Management
Assignment Rules	Assignment Rule Management
User Assignment Templates	User Assignment Templates
User Levels	User Levels
Teams	Team Management
Program Tags	Program Tag Management

5.7 Investigation Organizations

Investigation organizations require the Investigation org type under Org Details. Specific org functions for this organization type will vary based on each organization's role in the investigative process. There must be an Investigation org with the ISP function with an Investigation Control sub-organization below it or the Investigation org can have both the ISP and Investigation Control functions. The Control organization will be responsible for all organization level configurations for its distributed sub-organizations (ARC, CRC, and/or Field).

The Investigation Control organization's Distribution Rules will determine how investigation cases are routed. The required roles below may vary based on the specific functions added to the Investigation org type in Org Details.

Required Roles:

Table 5-15: Required Roles for Investigation Organizations

Role	Purpose
Case Processor	Primary role required to work on a case and should be paired with Validator, Preparer, Investigator, Leads Analyst, Field Investigator, and/or Quality Reviewer to work cases or leads in the applicable phases.
User Manager	Responsible for adding users and modifying their user assignments so they can work on cases.
Operations Manager	Responsible for org configurations and can set up Automatic Assignments, Notifications, Adjudication Workflows, Local Products, Program Tags, and User Levels.
Org Workload Manager	Responsible for assigning cases through the Actions drop-down for either bulk reassignment or in case reassignment.
Validator	Responsible for working cases in the Validation phase. Must be paired with the Case Processor role.
Preparer	Responsible for working cases in the Preparation phase. Must be paired with the Case Processor role.
Investigator	Responsible for working cases in the Investigation phase. Must be paired with the Case Processor role.
Quality Reviewer	Responsible for working cases in the Quality Review phase. Role has access to cases across all investigative phases. Must be paired with the Case Processor role.
Leads Analyst	Responsible for completing leads. Must be paired with the Case Processor role.

Field Investigator	Responsible for completing field leads. Must be paired with the Case Processor role.
Distribution Manager	Responsible for configuring and managing an organization's Distribution Rules.
Scoping Manager	Responsible for configuring and managing an organization's Scoping Rules.

Required Configurations:

Table 5-16: Required Configurations for Investigation Organizations

Topic	Link
Workflow Builder	Workflow Builder & Module Configuration
Defining Org Relationships	Organization Relationships
Case Categories	Case Categories
Service Catalog	Service Catalog
Distribution Rules	Distribution Rules
Scoping Rules	Scoping Rules

Optional Configurations:

Table 5-17: Optional Configurations for Investigation Organizations

Topic	Link
Case Progression Exception Rules	Case Progression Exception Rules
Notifications	Notification Management
Assignment Rules	Assignment Rule Management
User Assignment Templates	User Assignment Templates
User Levels	User Levels
Teams	Team Management
Program Tags	Program Tag Management

6 Organization Management

An **Organization** is a government entity and/or an investigation service provider that is used to initiate requests, receive requests, conduct investigations, and adjudicate cases. An **Organization Manager** can view, edit, add new organizations, and configure organizations under the **Org Management** tab. The **Org Manager** cannot edit their organization type or organization functions.

This section will detail these configurations which can be utilized by an organization with any of the existing NBIS Org Types available (SSC, Review, Authorize, Adjudication, Appeals, Screening, FSO, Component Adjudication, and Vetting).

6.1 Organization Context

The Organization tab contains Hierarchy, Details, and Teams sub tabs. The Users tab lists users added to your organization or hierarchy. The Configurations tab contains several organization configurations covered throughout this section. The Organization Context is your current organization showed in the header of the application.

Note: The Configuration tab visibility is dependent on the roles assigned to your persona. See Organization Level Configurations for more information about this tab.

6.1.1 ORGANIZATION NAVIGATION

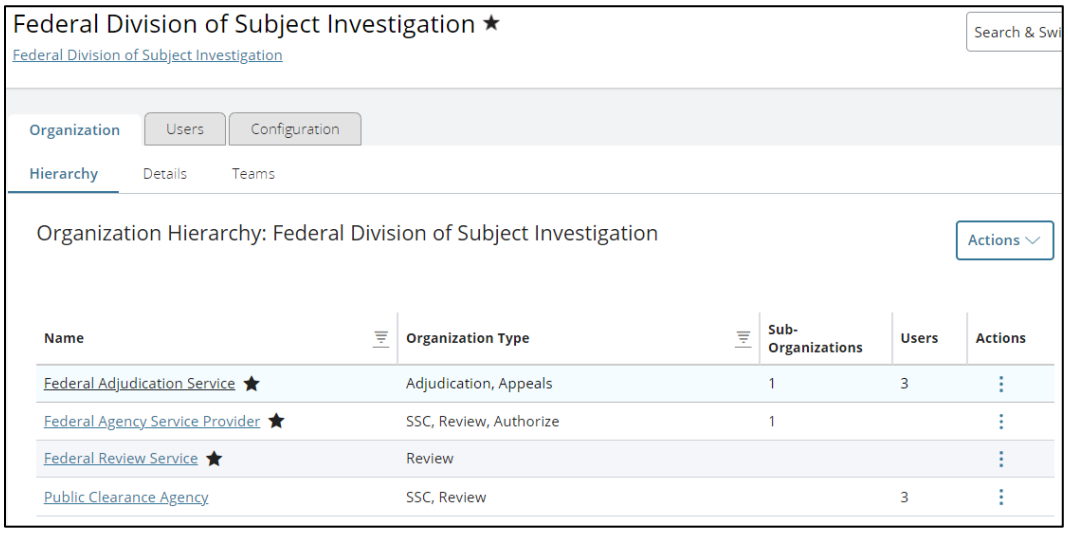


Figure 6-1: Organization Hierarchy

1. From the left navigation menu, select **Organization Management.**

Note: Org Managers are not able to manage the user and team tabs unless granted appropriate roles to manage them. These tabs will be in read-only mode. Teams do not apply to agency organizations.

The organization title and breadcrumb (link below organization title) will tell you which organization's attributes you are viewing. The breadcrumb is a link that will move to that organization's page if you navigate to a different organization level.

2. Select the **Hierarchy** tab to view the organizations one level down from the current organization context.
3. From the **Name** column, select an **Organization Name** to switch context to that sub-organization.

6.1.2 SWITCH ORGANIZATION CONTEXT

There are two ways to switch organization context:

- From the **Name** column, select an **Organization Name** to switch context to that sub-org and view its details, users, and hierarchy.
- From the **Search & Switch Org** field, enter an organization's name, Org Path, or Org Code to find and select a different organization to view its details, users, and hierarchy.
- In the **Actions** column, select the **ellipsis** to display the action options for the sub-org. Select **Switch Organization Context** to view the sub-org's details, users, and hierarchy.

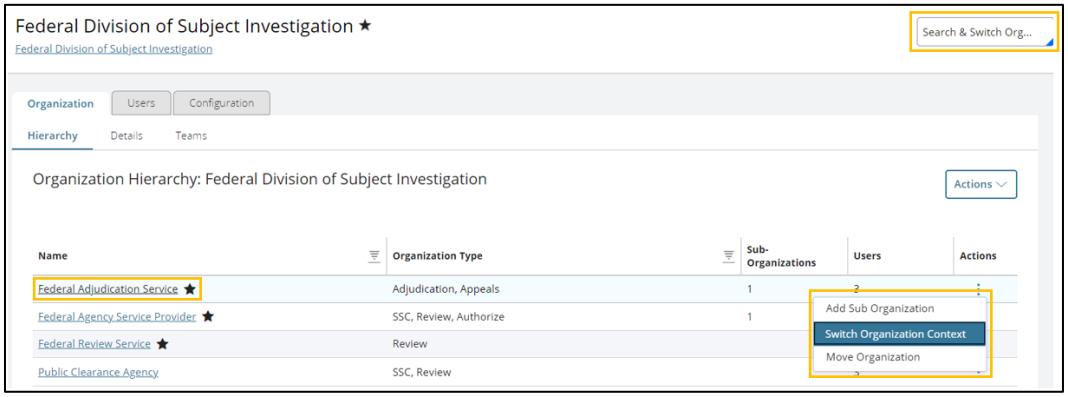


Figure 6-2: Org Management – Hierarchy

6.2 Managing an Organization Hierarchy

The organization hierarchy is extremely important to the base functionality of NBIS. Every organization requires a name and a unique org abbreviation within its hierarchy.

The organization has fields that define the Org Types, Org Roles, and Org Functions. When defining a hierarchy, it is important to be aware of the impact these values are defining for all sub organizations.

Onboarding Managers, **System Managers**, and **Org Managers** can edit the org level of their sub-organizations. Org Managers can only select non-grouped levels, while Onboarding and System Managers can select any level. No role is able to edit the org level for the organization they are a part of.

There is a feature called inheritance built into the organization data. Org Types, Org Roles, and Org Functions are inherited by all suborganizations. When a role/type/function is removed, it will be unavailable for all sub organizations. This can be changed mid-hierarchy by the **Onboarding Manager** because they can add any missing roles/types/functions back into the organization.

Inheritance also supports certain configurations, such as Order Form Templates and Notifications. Sub-organizations can copy or inherit these configurations from their parent to reduce configuration time.

6.3 Organization Details

This section details how to add, view and edit the details of your organization as an **Org Manager**. The Onboarding Manager also has abilities to manage org details, see Org Management Configurations by Onboarding Manager for more information.

6.3.1 VIEWING AN ORGANIZATION'S DETAILS

1. From the left navigation menu, select **Org Management**.
2. Open the Details sub-tab within the Organization tab.

All information displayed will be in read only format. The **Actions** drop-down will grant you access to the appropriate actions for your role.

6.3.2 CREATING AN ORGANIZATION

1. From the left navigation menu, select **Org Management**. You should be displaying the Organization tab and Hierarchy sub-tab.

There are two ways to add a new organization:

- From the **Actions** drop-down, select **Add Organization** to create an organization at your current position in the hierarchy.
- Select the **ellipses** for the desired organization and select **Add Sub Organization** to create a sub organization at this location.

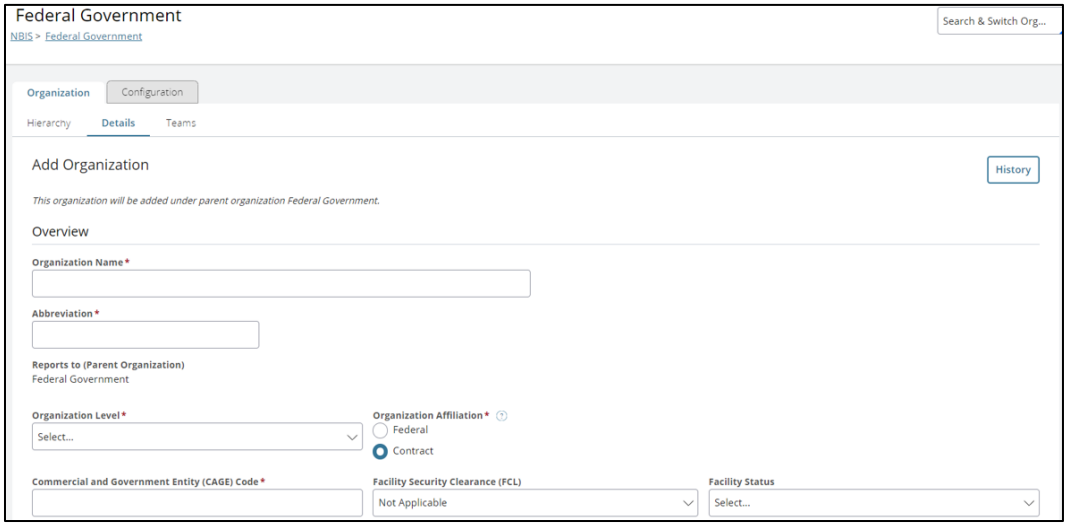


Figure 6-3: Add an Organization

Note: The steps for creating a sub organization are the same as creating an org in your current org context.

2. Enter the Organization's details as needed.

Overview Details Information:

- Organization Name – name of the org or sub-org
- Organization Abbreviation - must be unique within their hierarchy and cannot be changed once the organization is created.
- Organization Level - drop-down list will be populated based on the Org Level table in system settings. Only the **Onboarding Manager** can create grouped level orgs. The Org Level field can be edited under certain conditions, see Managing an Organization Hierarchy for more information.
- Organization Affiliation – If **Contract** is selected, you will be required to enter the organization's Commercial and Government Entity (CAGE) code. An optional Facility Security Clearance drop-down and Facility Status drop-down will be available. Only the **Onboarding Manager** can make these selections. Once the organization is created, the **Org Affiliation** field cannot be edited.
    - After a CAGE code is entered, the fields will populate based on the configuration in System Settings. Under the KMP field, a hyperlink to view details will appear. Selecting this will provide a pop-up modal, where you can select the subject's SSN and it will hyperlink to the subject profile.
- 'Grouping' field – Displayed a check box field for "Grouping" which is disabled by default and only editable by Onboarding Manager.
- Automatically Enroll in CV checkbox – If checked "Yes", subjects in this org will automatically be enrolled in CV when granted a favorable determination.

3. Select the applicable **Organization Types, Functions, and Roles**.
4. Complete the **CV Settings**.

The CV Settings section appears only for org levels marked with the Continuous Vetting Program flag.

- **CV Program Eligibility** – to indicate whether the org is CV Enabled to (Yes/ No /Inherited). The default will always be **Inherited**. If not selected, show Inherited. If yes, the Organization Department Type drop-down field will appear below. Only **Onboarding Manager** can make these changes.

  Note**:** Currently, the selection made for this drop-down will not drive CV enrollment. Current logic looks for enrollment type and if a CV Provider is attached. If found, that Provider ID will be chosen.
- If **Yes** is selected for **CV Program Eligibility**, an **Organization Department Type** drop-down will appear to select whether the org is DoD and where CV enrollments should be sent:
  a. DoD/Mirador – subjects in this org will receive CV services from Mirador
  b. Non-DoD/NBIS CV – subjects in this org will receive CV services within NBIS (Subject

Central)

c. DoD/NBIS CV – subjects in this org will receive CV services within NBIS (Subject Central)

5. Complete the remaining Organization details.
6. Select **Save.**

Notes:

- See Organization Levels table in the Appendix for more information on Org Levels.
- See Org Type, Function, and Roles Reference Table for more information about the drop-downs.
- You need to add the SON, SOI, and DISS Mapping (DISSInternalSMOID for file ingest) codes in the Legacy Systems section of Org Details so that data can be passed downstream to DISS and CVS.

6.3.3 EDITING AN ORGANIZATION

3. From the left navigation menu, select **Org Management**.
4. Open the Details sub-tab within the Organization tab.
5. From the **Actions** drop-down, select **Edit Organization.**
6. Edit the Organization's details as needed and then select **Save.**

6.3.4 DELETING AN ORGANIZATION

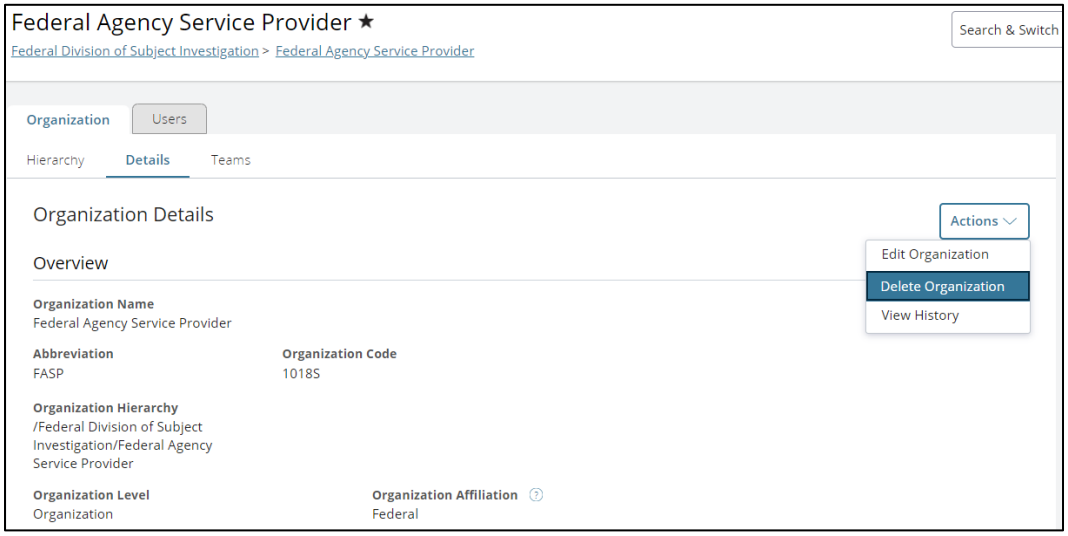


Figure 6-4: Delete an Organization

1. Navigate to the Organization details tab.

2. From the **Actions** drop-down, select **Delete Org**.

   Note: You can only delete an organization once *all* users, workflows, teams, sub-organizations, and organization relationships are removed from the organization.

The Delete Org option from the Actions drop-down should only appear once all these conditions have been met.

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

6.4 Org Management Configurations by Onboarding Manager

The **Onboarding Manager** user role is responsible for managing org levels and in some cases, the individual org details. This role has specific permissions when managing org details that the Org Manager role does not have.

Onboarding Managers can select any of the org types, org functions, and org roles from the parent organization without restriction. The Onboarding Manager has *no restrictions* by the parent organization when viewing the Org Details screen. Upon viewing the same Org Details, an Org Manager can remove the Onboarding manager edits. If the edits are not associated with the parent organization, the edits cannot be restored.

6.4.1 CREATING A GROUPED LEVEL ORG

Grouped level organizations (also known as top level organizations) are determined by the organization level in the org details. If an organization is grouped, it will be marked by a star within Org Management. Grouped level organizations are used when configuring external organization relationships.

A **NBIS System Manager** and an **Onboarding Manager** are the only roles that can create an organization with a Grouped Org Level. The organization needs to be a Grouped Level Organization to be enabled for Continuous Vetting, this is determined by System Settings configuration. Grouped level organizations are denoted with a star in Org Management. Refer to the Organization Level table in the Appendix for additional details about each org level.

Grouped level organizations display as selection options in External Organization Relationship Management.

To edit the Org Level:

1. From the left navigation menu, select **Org Management**.
2. Under the Organization tab, select the **Details** sub-tab.
3. From the **Actions** drop-down, select **Edit Org**.
4. The **Organization Level** field is editable, with all grouped org levels as available options for the System Manager and Onboarding Manager.

Note: Org Managers will not have all options available when selecting an organization level.

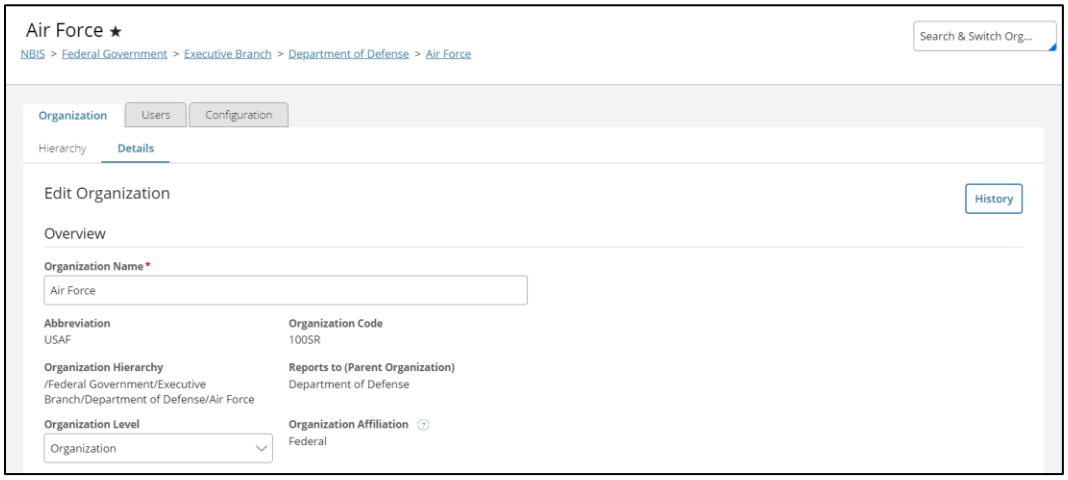


Figure 6-5: Org Details in Edit Context

6.4.2 PROVIDING SPECIFIC ORG TYPES, FUNCTIONS, AND ROLES

The **Onboarding Manager** can add all org types to an organization. The **Org Manager** can only add the **SSC**, **Review**, and **Authorize** org types to an organization.

Figure 6-6: Org Types, Functions, & Roles

To edit the Org Types, Org Functions, and Roles:

1. From the left navigation menu, select **Org Management**.
2. Under the Organization tab, select the **Details** sub-tab.
3. Select **Actions**, then **Edit Org**.
4. Based on the Org Type selected, specific roles will populate for the Org. After roles are selected, certain functions will be available based on the roles chosen.

   Note: There are also multiple roles (for example, **NBIS Financial Manager**) that are not tied to a specific Org Type that only Onboarding Managers can add to an org's roles. See the Role Matrix for more information.

6.5 Organization Migration

Org Managers can move organizations within their hierarchy and external to their hierarchy. For external migrations the Receiving and Migrating organization need to work together on the migration. For detailed steps see External Organization Migration.

Migration Notifications can be configured and sent to users affected by the migration. Migration Notification messages will be automatically sent to organizations affected by the migration. See Notification Management section for additional details.

Due to hierarchical inheritance, sub-orgs cannot have roles/types/functions which the parent organizations do not have. If the moving organization has certain roles/types/functions that the receiving organization does not have, these will be automatically dropped during the migration. If a user's roles were removed through migration, the user will no longer have access to the navigation and page options when logging into the system.

The **Reviewer** and **Authorizer** roles are protected, and therefore retained during migration to prevent interruptions to active cases.

Note: It is the **Org Manager**'s responsibility to manually update the organization details and configurations post-migration. The **User Manager** may need to update user personas and their assignment configurations depending on the org's new location and functionality within the hierarchy.

6.5.1 INTERNAL ORGANIZATION MIGRATION

Org Managers can move organizations within their hierarchy context. The migration needs to be started from a parent organization that can see the migrating org and its new location.

1. From the left navigation menu, select **Org Management** and locate the specific organization you want to move.

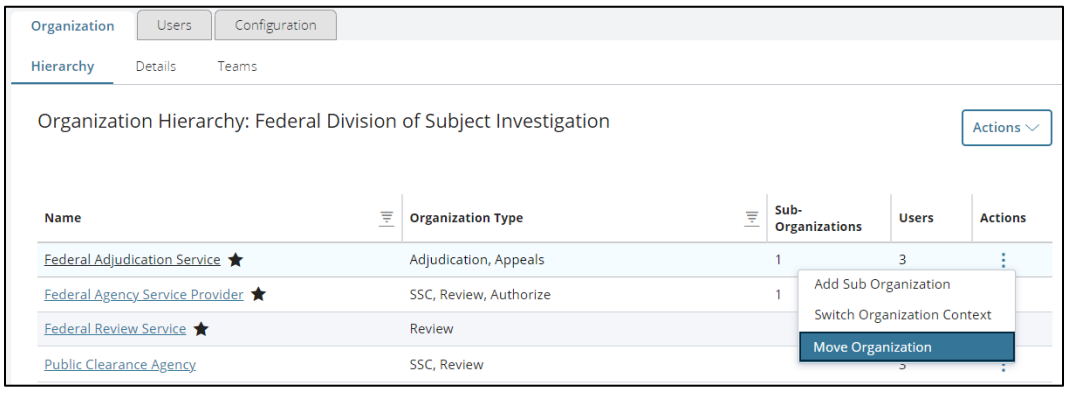


Figure 6-7: Move Organization Action

Note: Your organizational context determines your options for Org Migration. You can only migrate to orgs below your current context. If the org needs to move above your current hierarchy, a higher level Org Manager will need to perform the migration.

2. Under the **Actions** column for the specific organization, select the **ellipses**, and then select **Move Organization**.

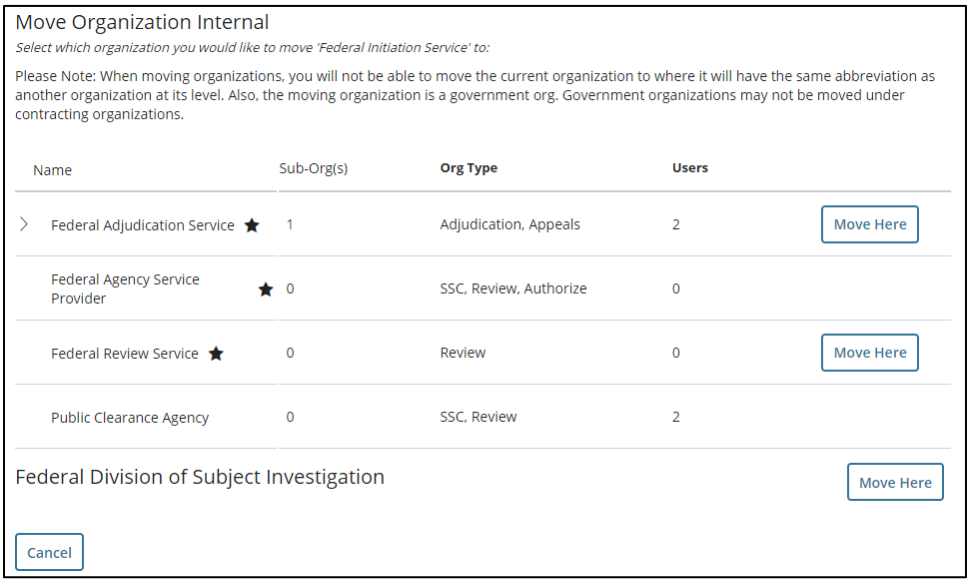


Figure 6-8: Org Migration - Location Selection

3. Choose the receiving org and select **Move Here**. You cannot move to the same parent org.

   Note: You cannot move government organizations under contractor organizations.

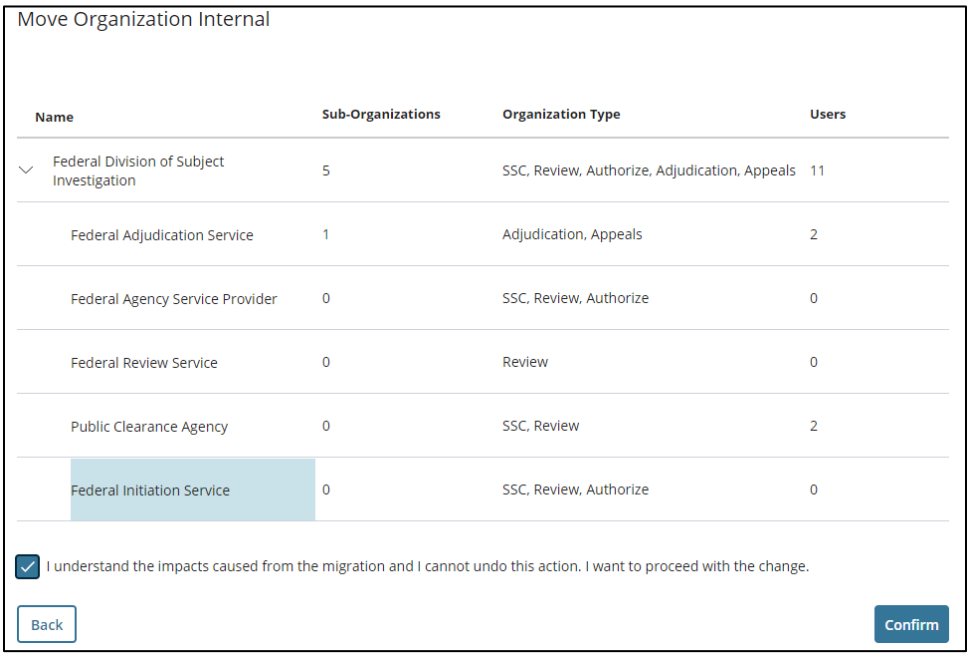


Figure 6-9: Move Organization - Confirmation

4. The confirmation page displays the preview of the new hierarchy after confirming the organization migration. Select **Confirm** to proceed with the migration.

   Note: If there are Warnings, please review the warnings and the relevant information about Migration Impacts and Warnings. You may need to resolve the User/Role warning before the migration can take place. If impacted workflows are the only warnings, you can **Confirm** the migration and the workflow will be disabled.

6.5.2 EXTERNAL ORGANIZATION MIGRATION

Similar to Internal Migrations, External Migrations are performed by the **Org Manager**. External Migrations allow for organizations to migrate out of their immediate organization's hierarchy. Migrations must be completed in the context of the organization that will be migrating. Parent organizations cannot perform external migrations for their sub-orgs.

The steps for migration require both organizations, receiving and migrating, to work together to complete the process. The Receiving organization will be the new parent of the moving organization. The migrating org will be leaving its hierarchy and moving to a new one within NBIS.

Preparation is recommended prior to initiating the three step migration process to avoid complications. Org Type, Functions, and Roles need to be compared and edited to prevent warnings during the migration. The migrating org cannot have Roles, Types, or Functions the parent org does not have.

Note: The Onboarding Manager can modify the Org Type, Functions, and Roles after migration to repair the functionality lost by the migration that the Org Manager cannot fix. See Org Management Configurations by Onboarding Manager for more information about their functionality

6.5.2.1 GENERATE THE IMPORT CODE - RECEIVING ORGANIZATION

1. From the left navigation menu, select **Org Management**.
2. Switch context to the receiving organization within the Organization Hierarchy.

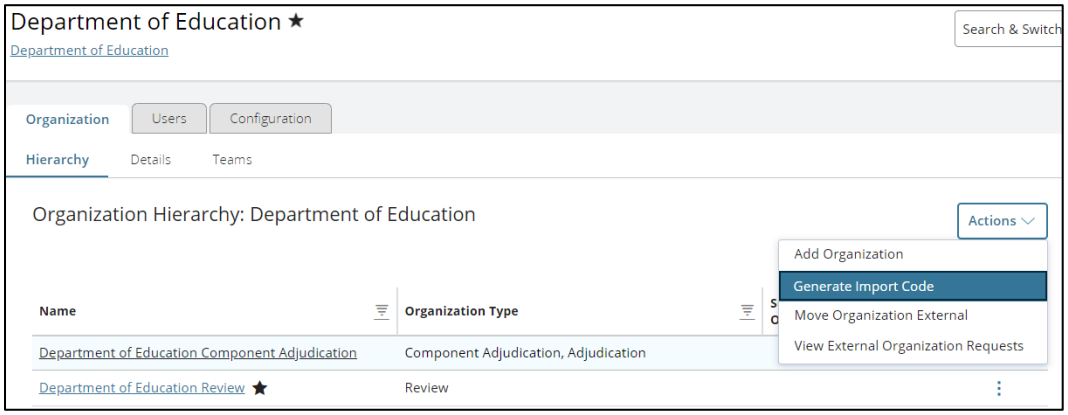


Figure 6-10: Org Management - Generate Import Code

3. As the receiving org, under the **Actions** drop-down, select **Generate Import Code** to produce the code to provide to the migrating org.

Figure 6-11: Generate Organization Import Code

Note: The expiration date is automatically set to 90 days, but it can be adjusted by selecting the calendar icon.

4. Select **Generate Code.**

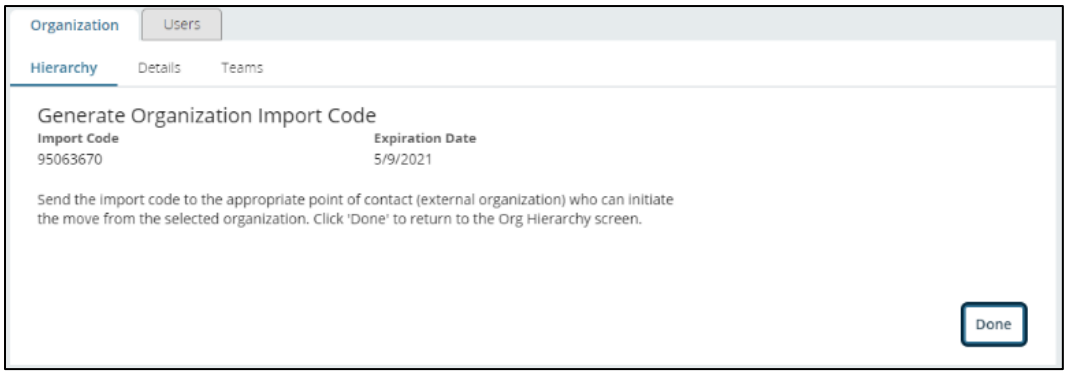


Figure 6-12: Import Code and Expiration Date

Note: Make a note of the Import Code and Expiration date and provide the code to the migrating org. They need this information to complete their portion of the migration.

5. Select **Done** and provide the migrating org the Import Code.

To view or cancel the Import Code:

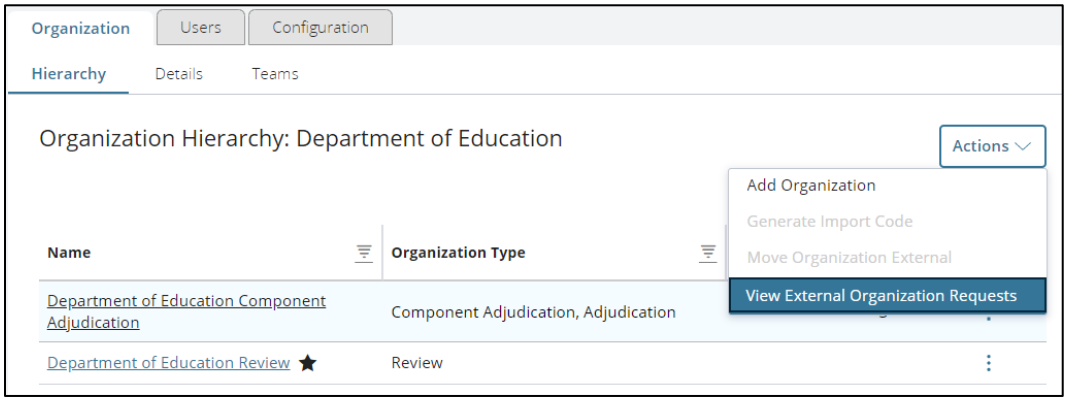


Figure 6-13: View External Org Requests Action

1. Under the **Actions** drop-down, select **View External Organization Requests** to see Code history.

   Note: Only one organization migration can be in process at a time. Other migration actions will not be available until the code is cancelled.

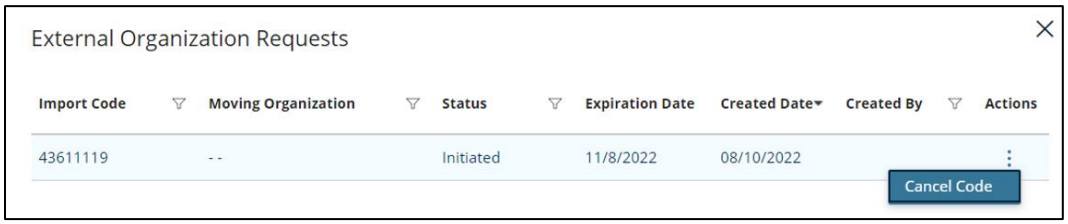


Figure 6-14: External Organization Requests - Cancel Code

2. Under the **Actions** column, select the **ellipses** and select **Cancel Code** if you no longer want to proceed with the migration.

6.5.2.2 ENTER MIGRATION CODE - MIGRATING ORG

1. As the migrating org, from the left navigation menu, select **Org Management**.
2. Switch context to the organization that will be receiving the migrating Organizations within the Organization Hierarchy.

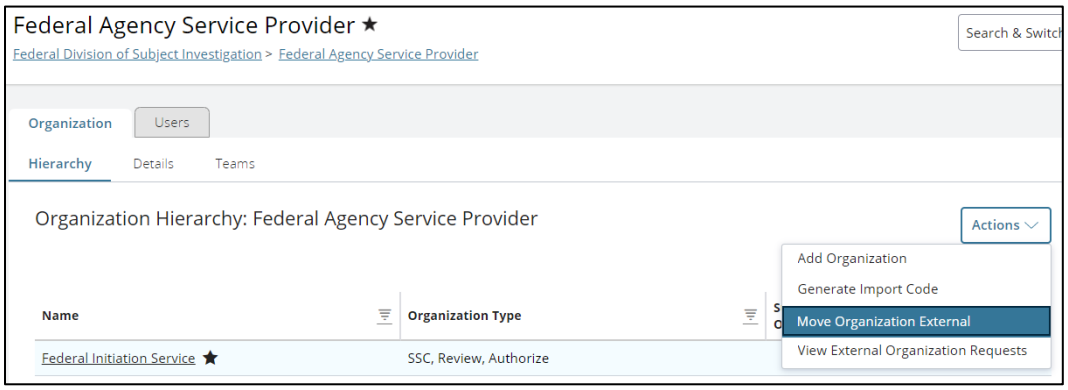


Figure 6-15: Org Management - Move Organization External

3. Under the **Actions** drop-down, select **Move Organization External** to input the Import Code provided by the receiving organization

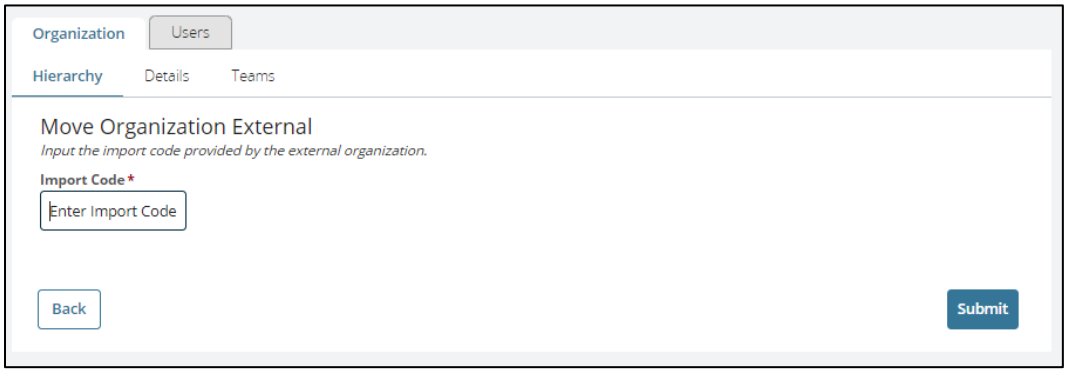


Figure 6-16: Enter Import Code

4. Enter the Import Code and select **Submit**.

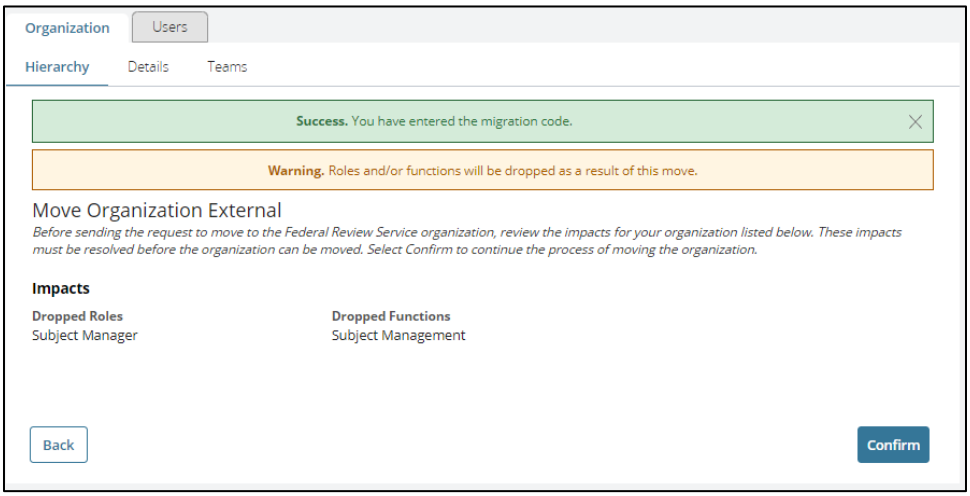


Figure 6-17: Move Organization External - with Warnings

5. It may give you a warning of impacted workflows or affected users. Select **Back** to adjust workflows, users, or roles/functions. Select **Confirm** to proceed.

   If you choose to go back and adjust the configuration, you will need to repeat Steps 1-4 to continue.

   Note: If there are Warnings, please review the warnings and the relevant information about Migration Impacts and Warnings. You may need to resolve the User/Role warning before the migration can take place. If impacted workflows are the only warnings, you can **Confirm** the migration and the workflow will be disabled.

6.5.2.3 CONFIRM THE MIGRATION – RECEIVING ORG

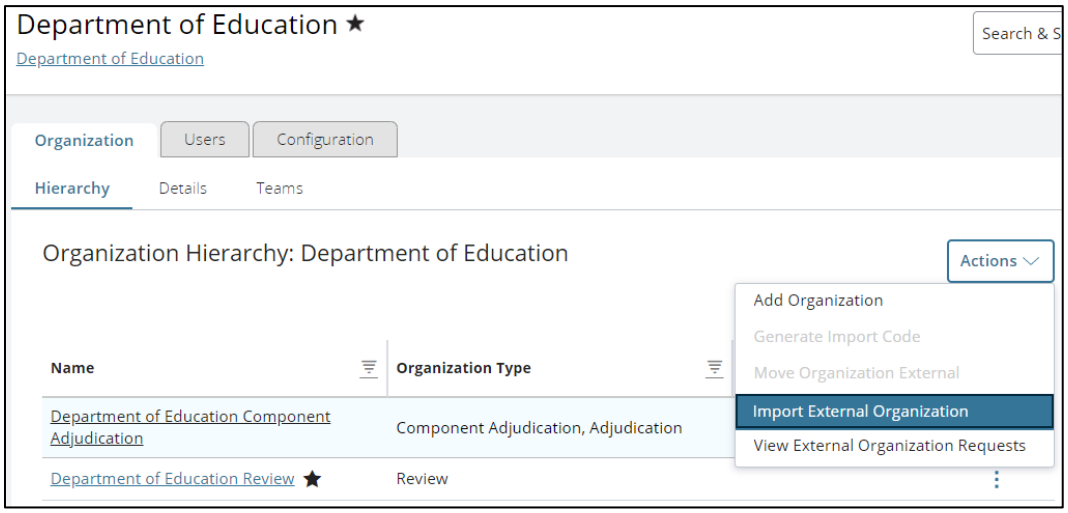


Figure 6-18: Import External Organization Action

1. To complete the migration, the Receiving Org must confirm the migration; Switch context to the receiving organization

   Note: This is the org that generated the code for the migrating org.

2. Under the **Actions** drop-down, select **Import External Organization.**

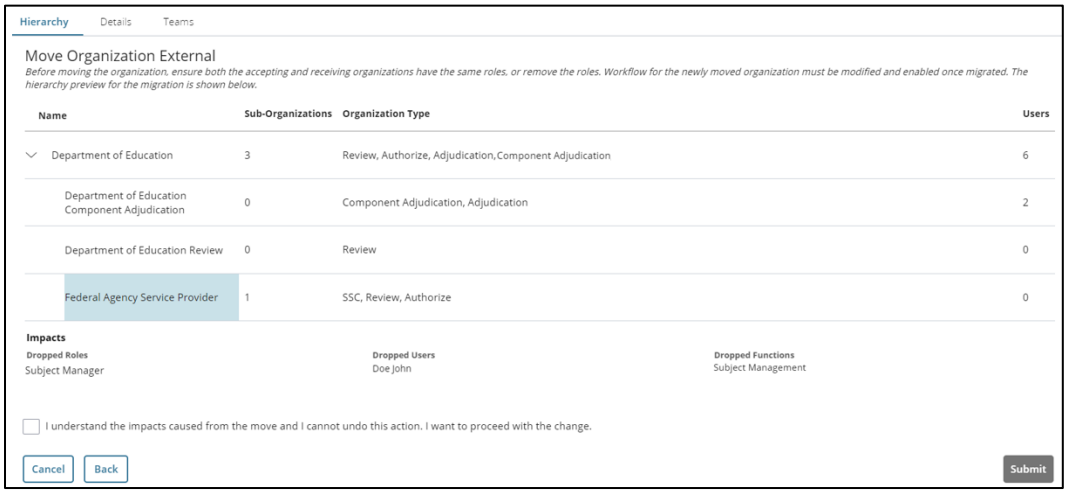


Figure 6-19: Organization Hierarchy Preview

3. Confirm the location of the migrating org is correct in the receiving org's hierarchy and select the **checkbox,** confirming the impacts and change.

   Note: See section Migration Impacts and Rules if you are not able to **Move Organization** due to warning messages.

4. Select **Submit** to receive the migrating org. Once complete, the org will appear in the new hierarchy position. If you do not want to move ahead with the migration, select **Cancel** to restart the entire process.

6.5.3 MIGRATION IMPACTS AND WARNINGS

On the confirmation screen of the migration. The Warnings will be displayed to the Org Manager. It will list all Roles, Users, and Org Functions affected by the migration. If you choose to proceed with warnings, please visit the user profile for listed user(s) and ensure that the user(s) is(are) associated to the organization with expected role(s). If impacted workflows are the only warnings, you can proceed with the migration and the workflow will be disabled.

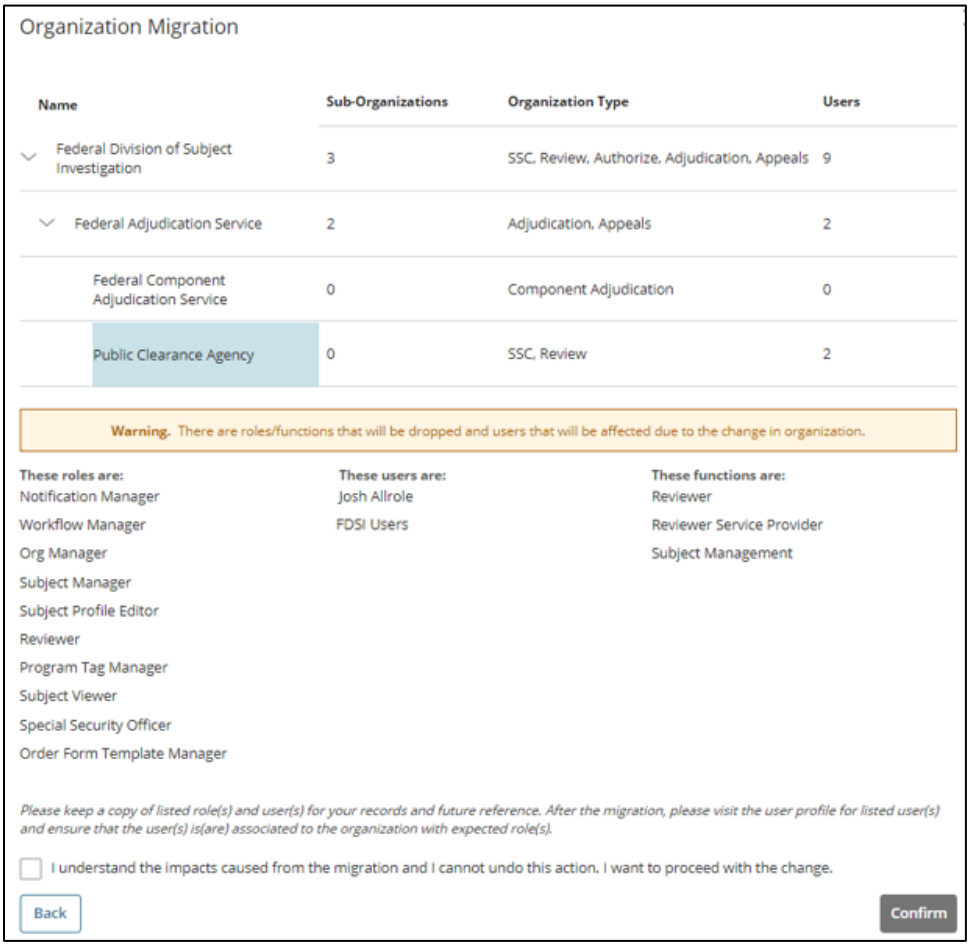


Figure 6-20: Org Migration with Warnings

Roles to be dropped (Affected Users also) - If there are any roles to be dropped from the Migrating Org, the external org migration will not happen. Similarly, if there are users affected by roles to be dropped, this would imply that roles are still dropped from the Migrating Org, so the migration will not happen if either (A) only roles need to be dropped from moving org or (B) roles need to be dropped from the org and users in the affected organization. See Edit User Persona Information and Managing an Organization Hierarchy for more information.

Functions affected - If there are any org functions that need to be dropped from the Migrating Org, the external org migration will not happen. These functions used to be the same as Roles as in they shared the same ID, but with the change of ID for the Org Functions, they are now separated. Still, if any Org Functions are to be dropped, the external migration is not possible.

Workflow Configurations affected - All workflows will be disabled. The external migration can still take place even if there are workflow configuration impacts.

Federal under Contract Org impact - If the moving org is Federal and is attempting to move under a contracting org, the external org migration will not happen. This is similar to the internal migration process.

7 Organization Level Configurations

Depending on user roles granted, Organization Management configuration tasks may include:

- Assignment Rules
- Notification Management
- Program Tag Management
- Organization Relationships
- Service Catalog
- Case Categories
- Ingest Management
- Order Form Template Management
- Form Routing
- Case and Form Type Association
- Distribution Rules
- Question Configuration

This section will detail these configurations which can be utilized by an organization with any of the existing NBIS Org Types available (SSC, Review, Authorize, Adjudication, Appeals, Screening, FSO, Component Adjudication, and Vetting). This chapter does not include all organization level configurations, other configuration sections are located throughout the guide.

7.1 Assignment Rule Management

The **Org Assignment Manager** can create and manage Assignment Rules for their organization. Assignment Rules define custom priorities for automatically assigned work within an organization.

Assignment rule configurations are optional for an organization but are recommended to appropriately prioritize their case work. By default, NBIS will automatically assign a default priority of 999 to all cases/tasks. Without any assignment rules configured the system will automatically queue the work to be assigned to users as "First in First Out".

Assignment Rules are always applied to cases to give them capability requirements. Cases are then automatically assigned to a user's worklist based on the configured Assignment Rules and a user's defined capabilities, capacities, and thresholds. See User Management for more information.

Note: Users in the system will automatically receive cases only if they are set to receive work automatically. This applies to the default case priorities as well.

Once you add, edit, or delete an Assignment Rule, you must reprioritize the rules within the system. This allows the system to immediately apply the updates to the cases that are in flight in an Organization's unassigned workbasket. This will not affect cases already assigned to users. If **reprioritize** is not selected, the system will automatically reprioritize cases overnight to reflect any changes. Reprioritizing does not visually change anything on the assignment rules table, it only impacts the in-flight cases as described above.

Note: In the Assignment Rule table, the system will automatically sort the rules based on the Task Priority entered.

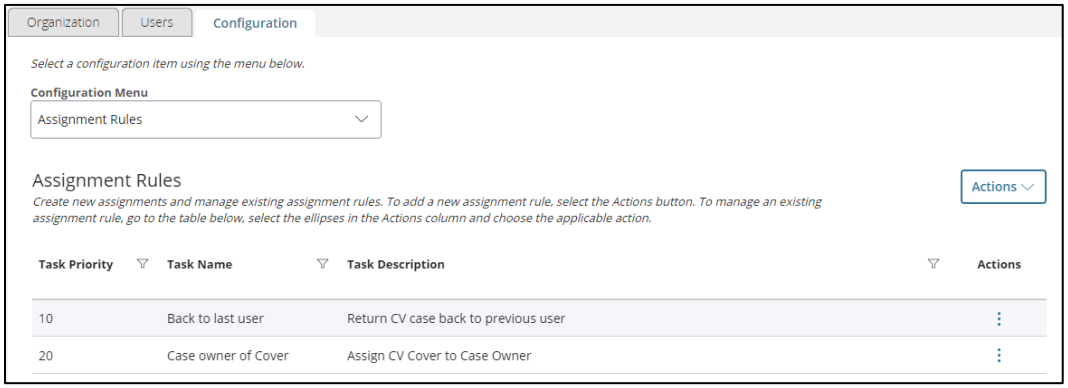


Figure 7-1: Assignment Rules

To add an Assignment Rule:

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab to view the configuration options.
3. From the Configuration Menu drop-down, select **Assignment Rules**.

There are two ways to add a new Assignment Rule:

- From the **Actions** drop-down, select **Add Rule**. This will add the rule to the bottom of the list.
- Under the **Actions** column, select the **ellipses**. You can select **Add Above** or **Add Below** according to the priority of the new rule.

  The system will apply the Assignment Rules in the order of **Task Priority** – the lower the number, the higher the priority. No two assignment rules can be the same. However, multiple assignment rules can have the same task priority value.

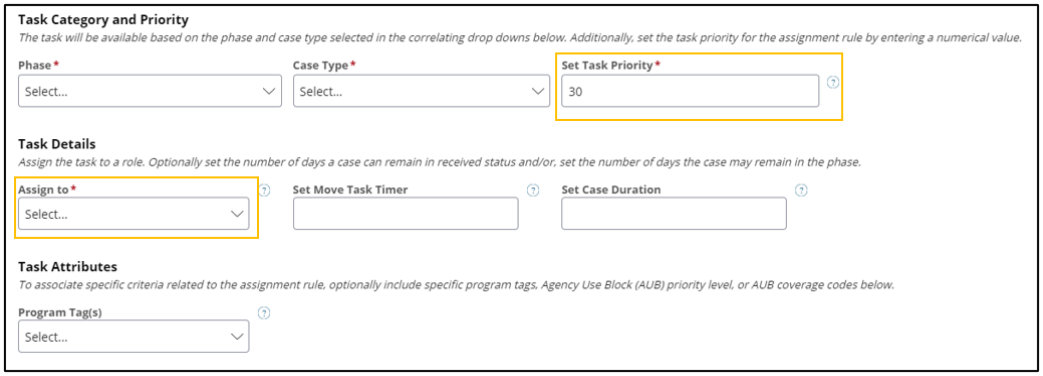


Figure 7-2: Add Assignment Rule

4. Complete all required fields. See the Assignment Rule Fields Table for more information about Assignment Rule fields.

   Notes:

   - Depending on the **Phase** selected, additional fields may appear.

     For CV Alert, Continuous Vetting, and Adjudication phases an Affiliation Category drop-down will appear for the organization's affiliation category for this assignment rule.
   - The **Set Task Priority** should already be assigned to the rule according to the method by which you added the Assignment Rule.
   - If you choose **Previous Owner** under **Assign To**, a **Set Assignee Duration** field appears. This field determines how long the task will remain untouched in the previous task owner's workbasket until it is automatically reassigned to another capable user.
   - Selecting **Any** from the Case Type drop-down allows the system to search for any options when executing the rule.

- If a **Program Tag** is added, the assignment rule will only trigger for cases with the program tag.

5. Select **Save and Add.**
6. From the **Actions** drop-down, select **Reprioritize**.

To view an Assignment Rule:

7. In the table of **Assignment Rules,** under the **Actions** column, select the **ellipses** for the specific rule and then select **View Details**.

To edit an Assignment Rule:

8. Under **View Assignment Rule**, select **Edit**.
9. Make any changes and select **Save** when completed.
10. From the **Actions** drop-down, select **Reprioritize**.

To delete an Assignment Rule:

11. In the table of **Assignment Rules,** select the **ellipses** under the **Actions** column.
12. Select **Delete** to remove the desired rule.
13. From the **Actions** drop-down, select **Reprioritize**.

7.1.1 ASSIGNMENT RULE FIELDS TABLE

Table 7-1: Assignment Rule Fields

Assignment Rule Fields	Description
Task Name	Name of the Assignment Rule.
Task Description	A description of the Assignment Rule.
Phase	The Phase the case is currently in.
Case Type	Investigation Tiers available to choose.
Case Category	This field appears when either a Continuous Vetting or BI phase with the appropriate workflow is enabled for the Organization that is selected. A case type needs to be selected to enable this field. The option presented will be determined by what categories are configured to be associated to the selected case type from the user's Organization as well as any parent organization that has categories configured.
Show Active Workflow Statuses	This field appear when a phase is selected that has the appropriate workflow enabled in Workflow Builder. This field controls what option are shown in workflow status field. When checked all statuses that are currently being used by cases will appear. When unchecked, all configured statuses for that phase will appear.
Workflow Status	This field appears when a phase is selected that has the appropriate workflow enabled in Workflow Builder. The option in this field is determined by the Show Active Workflow status check box, and what statuses are currently created for the workflow of the phase selected.
Task Priority	System auto generated numeric value to determine order of Assignment Rule processing.
Assign to	Who to route the case to base on assignment rule criteria selected? See Task Reserve Period for Previous Owner option.
Set Move Task Timer	The number of days the task can remain untouched with the current assignee in the received status before it is routed to another user.
Set Case Duration	The number of days to prioritize the case based on when the case was first created or initiated.
Set Assignee Duration	Only Appears if **Route To**: Previous Owner is selected. Field determines how long the task will remain untouched in the previous task owner's workbasket until it is automatically reassigned to another capable designated user.

Assignment Rule Fields	Description
Program Tag	A label on the subject used by the organization.
Display Order	Include a number to display on the template list to order the templates within the table. The order will be displayed sequentially starting with one.
Template Name	The name of the template which is created by the user.
Status	If enables is not checked, the user assignment template will not be available to your organization.
User Levels	This template will override any existing assignments associated with the user level selected.
User Capacity	Define the maximum number of assignments a user can automatically be assigned. Note: Users can still be assigned a case manually which may exceed the user's capacity.
Assignment Threshold	Define the number of assignments a user owns before the system automatically assigns additional tasks.

7.2 Notification Management

The **Notification Manager** can create notifications for a specified organization. Notifications can be sent to users within that organization or to the subjects. When a notification is created, it can be inherited (copied) by all organizations in the hierarchy below it, if the notification is enabled in the parent. Notifications *cannot* be sent to users outside your organization or to external organizations, including your parent organizations.

Notifications for Interim and Component Adjudication are configured at a system level by the **NBIS System Administrator.** Implementing organizations must open the desired notification and copy them into their organization to implement.

7.2.1 TYPES OF NOTIFICATIONS

There are five different types of notifications that can be triggered:

- **Status/Assignment** – Alert users when a case request moves to a different status within the workflow and when a case is assigned to a user or workbasket depending on the phase.
- **Stagnant Case** – Alert users when a case has been delayed in a phase for a determined amount of time. This notification only applies to SSC, Review, and Authorize organizations currently.
- **Case Expiration** – This feature sets the timing for how long cases remain open after the standard form (SF) is received by the agency as well as the notification. Optionally, you may choose to send a case expiration reminder by entering the number of days a reminder will be sent before the case expiration. This notification only applies to SSC, Review, and Authorize organizations.
- **Organization Move** – Alert users when a team or an organization is moved internally or externally.
- **CV Enrollment** – Alert users when a subject's CV enrollment status has changed.

7.2.2 NOTIFICATION DELIVERY

Notifications are delivered to users via in-system alerts or emails. This preference is configured in the user Manage Persona Settings tab of a persona. See Add Persona for more information.

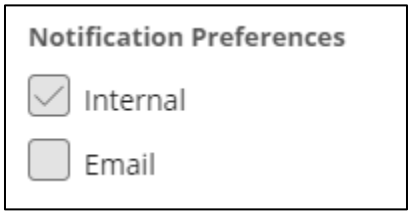


Figure 7-3: User Persona - Notification Preferences

In-system messages are delivered to the notification icon located in the header next to the Subject Search Bar. When the notification icon is selected, a popup will appear showing the most recent 10 notifications for a user. If more are available, a **Show More** button will be displayed.

Note: Notifications that your user triggers, will not be delivered to your user, regardless of configurations.

Case related notifications may have the link disabled if the user does not have the correct roles/permissions to view the case. The user can open the case from the notification if the hyperlink is enabled.

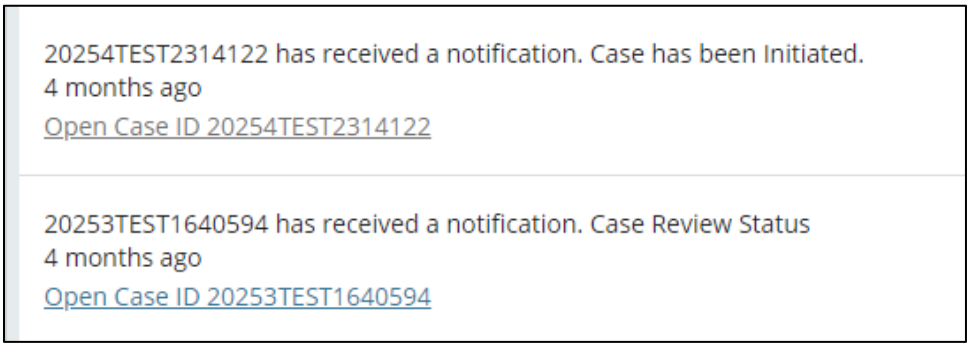


Figure 7-4: Enabled/Disabled Hyperlink Case Notifications

Email notifications will only display the provided information. No links to the cases or software will be provided.

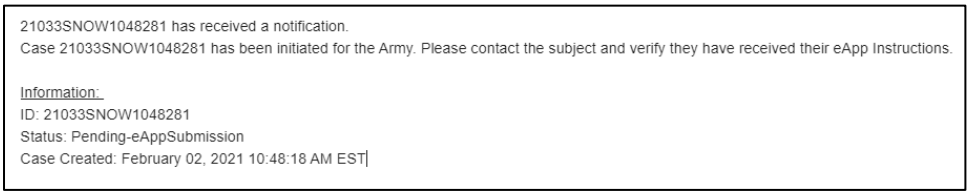


Figure 7-5: Email Notification

7.2.3 VIEWING NOTIFICATIONS

1. From the left navigation menu, select **Org Management.**
2. Select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **Notifications**.

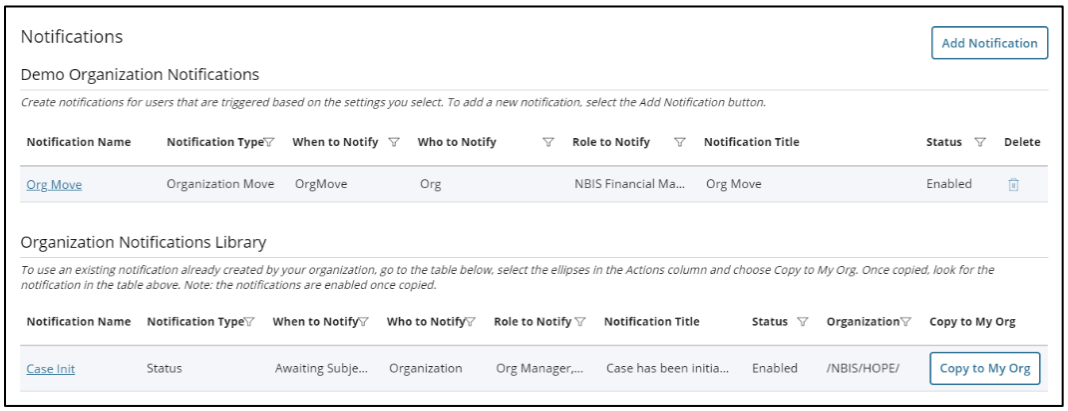


Figure 7-6: Notifications Tables

There will be two tables displayed.

- **Organization Notifications** – Notifications enabled for your organization.
- **Organization Notification Library** – All enabled notifications from the orgs above you in the hierarchy.

4. Select the trashcan to delete notifications in your organization or select the **Copy to My Org** button to inherit a notification from the Organization Library.

   Note: For Interim and Component Adjudication Orgs, you need to open the desired notification and copy them into your organization to implement. The **Copy** button on the table will not work.

5. Select the **Notification Name** to open the details of the selected notification.
6. From this screen you can **Edit Notification** or **Copy to My Org** depending on which table you are viewing notifications.

7.2.4 EDITING NOTIFICATIONS

1. From the Notifications screen in Org Management, Select the **Notification Name** to open the details of the selected notification.
2. Select **Edit Notification** to switch to edit mode.
3. Once changes are made, select **Save** to update the notification.

7.2.5 NOTIFICATION FIELDS REFERENCE TABLE

Table 7-2: Notification Configuration Fields Reference

Notification Configuration Reference Chart				
	Fields Required For this Notification Type?			
Field Name	**Status/Assignment**	**Stagnant**	**Organization Move**	**Case Expiration**
Phase to Notify	Yes	Yes	Yes	Yes
Notification Type	Yes	Yes	Yes	Yes
When to Notify	Yes	Yes	Yes	No
Program Tags	No	No	No	No
Notification Name (Internal)	Yes	Yes	Yes	Yes
Who to Notify	Yes	Yes	Yes	Yes
Days Before Notification	No	Yes	No	No
Days for Case Expiration and Notification	No	No	No	Yes
Notification Title (External)	Yes	Yes	Yes	Yes
Notification Message	Yes	Yes	Yes	Yes

7.2.6 CREATING A GENERIC NOTIFICATION

1. From the left navigation menu, select **Org Management.**
2. Select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **Notifications**.
4. From the Notifications main page, select the **Add Notification** button
5. Select the **Phase** for the notification.

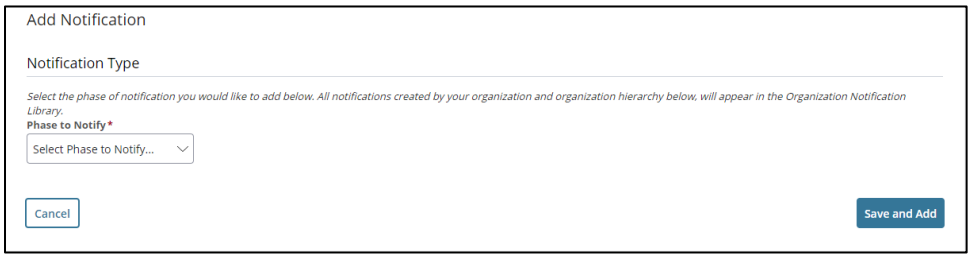


Figure 7-7: Add Notification

6. Select the **Notification Type**.

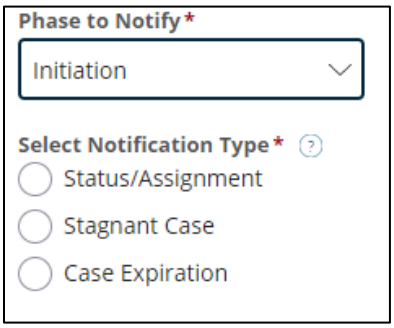


Figure 7-8: Phase to Notify

Note: Select **None** in the Phase field for the Organization Move or CV Enrollment notification type.

7. Fill in the required information:
    a. Notification Name (not seen by recipients)
    b. When to Notify, Who to notify

        Note: Selecting the Current Assignee's Team, Last Assignee's Team, or Organization options from the Who to Notify field, will display the Roles to Notify and User Levels to Notify fields. This will allow the Notification Manager to refine further the group of users that they want to receive the notification, based on their role and user level.

    c. Title of Notification to Recipients
    d. Notification Message

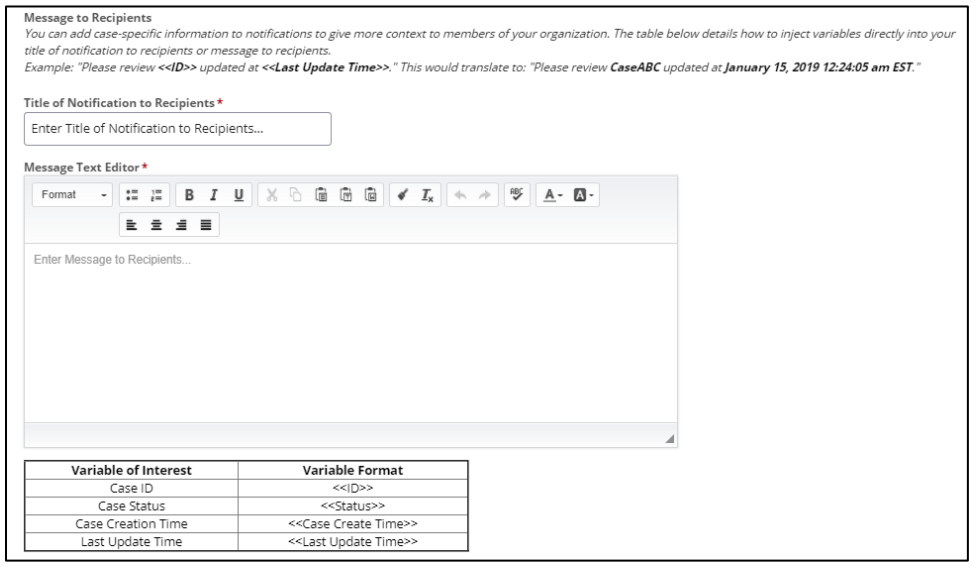


Figure 7-9: Notification Message to Recipients

8. Select **Save and Add** to create the notification.

7.2.7 SPECIFIC CONFIGURATIONS

7.2.7.1 STATUS/ASSIGNMENT SPECIFIC CONFIGURATIONS

When configuring a **Status/Assignment** notification, if you choose an assignable status (e.g., Review or Authorize) for **When to Notify**, the **Assignment to Notify** drop-down will appear, where you can configure a notification to trigger when a case is in a user worklist, or a specific role's workbasket.

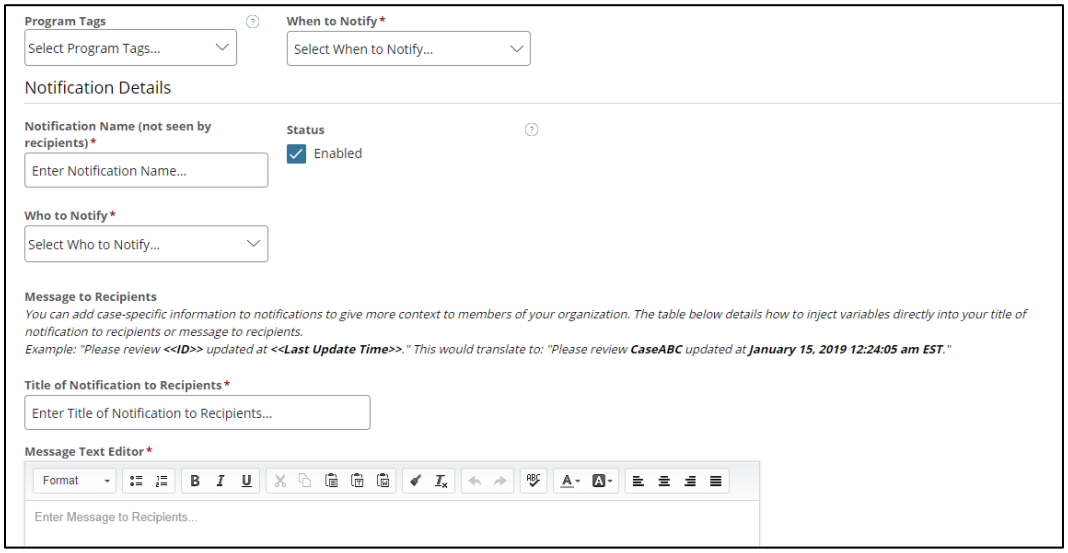


Figure 7-10: Status/Assignment Notification Configuration Fields

7.2.7.2 STAGNANT CASE SPECIFIC CONFIGURATION

Within each **Stagnant Case** notification, you have the option to schedule three instances of notifications. For each notification, choose the recipient, and the specific role if applicable. For the first two instances, specify the amount of time you want the case to be stagnant in the phase before the notification is sent. If you choose to configure the third instance, it is preset to send the notification every 15 days for a maximum of four times, or until the case is moved out of the specific phase.

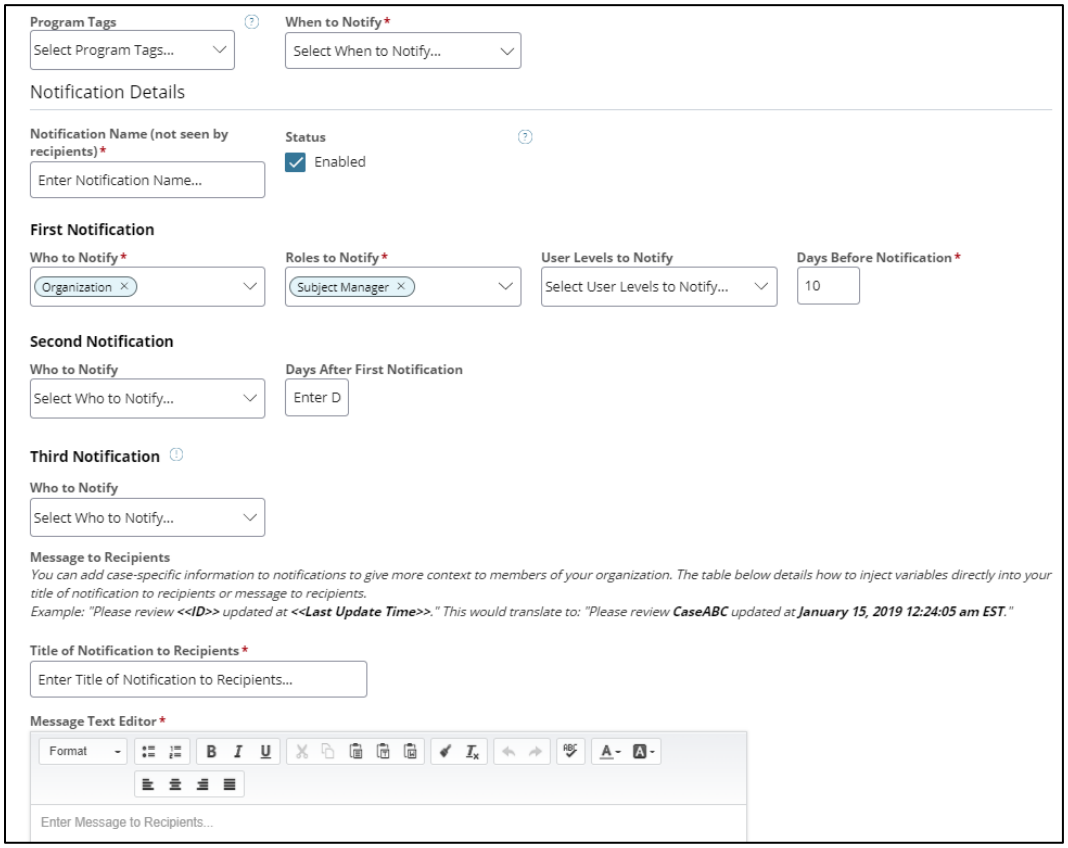


Figure 7-11: Stagnant Case Notification

7.2.7.3 CASE EXPIRATION SPECIFIC CONFIGURATIONS

When configuring a **Case Expiration** notification, the **Days for Case Expiration and Notification** defines the number of days a case can be active. The case expiration (case timer) will start once the system receives a standard form. Once the case timer counts down to 0, the case will be marked as **Expired.** The **Case Expiration** notification only applies to **Initiation**, **Review, Authorization**, and **Returned from ISP** phases.

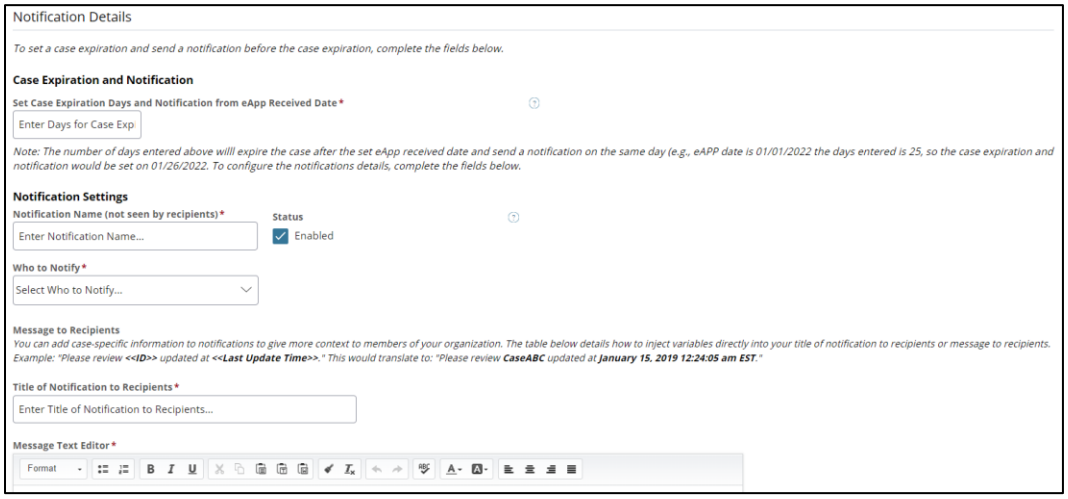


Figure 7-12: Case Expiration Notification Selection

When configuring a **Case Expiration** notification, a reminder message can be sent before the expiration notification is sent.

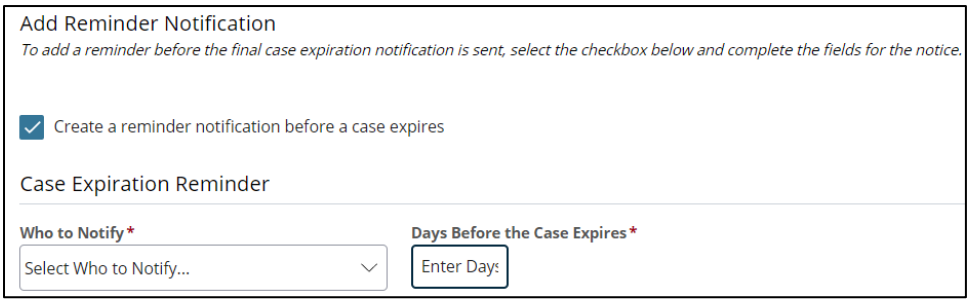


Figure 7-13: Case Expiration Reminder

7.2.7.4 ORGANIZATION MOVE SPECIFIC CONFIGURATIONS

After selecting **Organization Move**, you can choose to trigger a notification for an organization or team being moved. To configure this notification type, **None** must be selected as the **Phase to Notify**. If you select **An Organization is Moved** in the **When to Notify** field, the **Who to Notify** field will auto-populate to **Organization**. You will then be able to further refine the search by selecting **Roles to Notify** and **User Levels to Notify**.

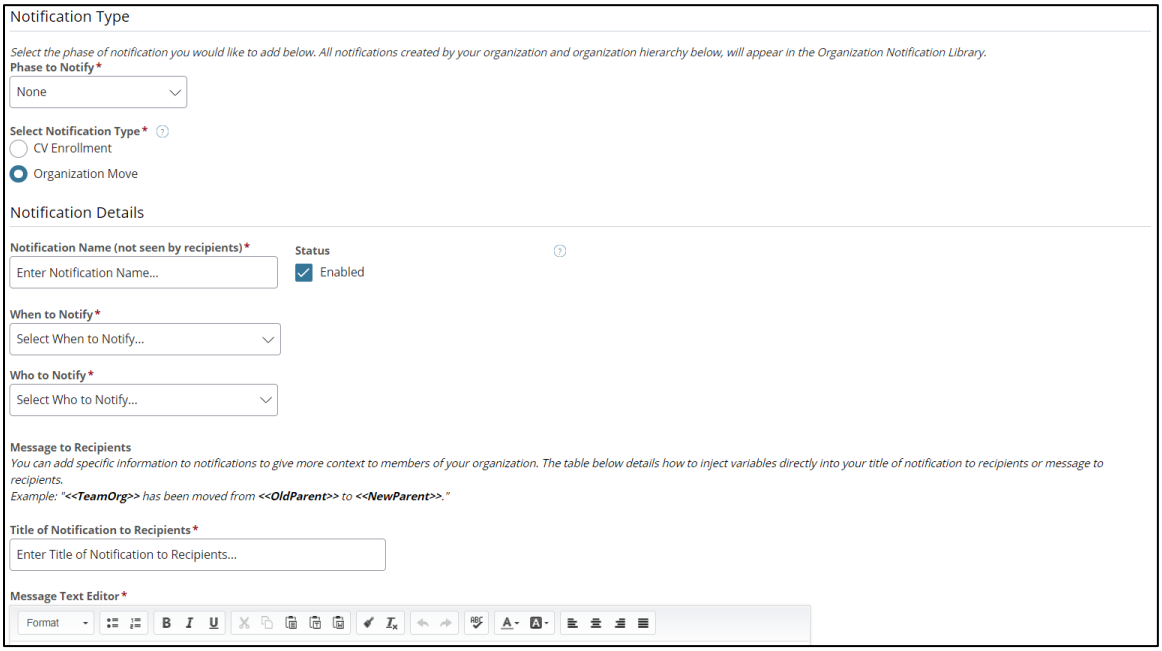


Figure 7-14: Migration Notification

For **External Organization Migrations**, Notifications will automatically be sent out to affected organizations. Everyone in the migrating and gaining organizations, and Organization Managers of the losing organization (parent of migration organization) will be notified.

7.2.7.5 CV ENROLLMENT SPECIFIC CONFIGURATION

After selecting **CV Enrollment**, you can choose to trigger a notification for a change in a subject's CV enrollment status. To configure this notification type, **None** must be selected as the **Phase to Notify**. The **Who to Notify** field is automatically populated to **Organization**. Select an enrollment status for **When to Notify** and further refine the recipients by selecting **Roles to Notify** and **User Levels to Notify**.

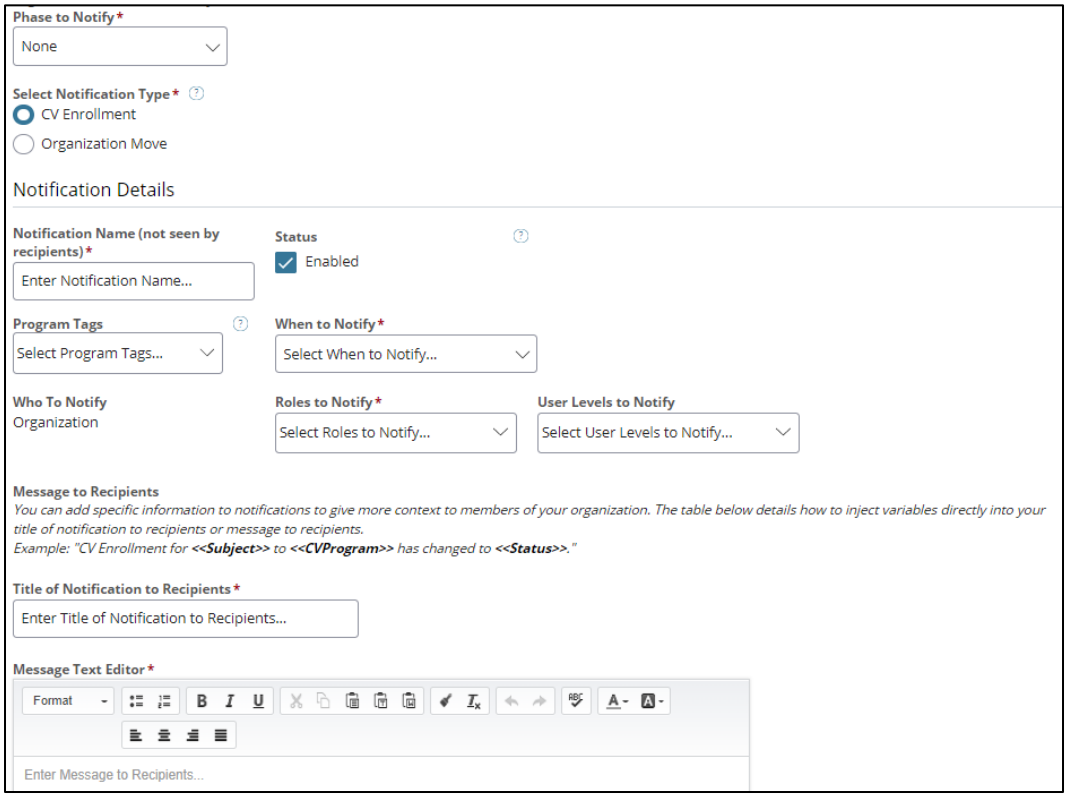


Figure 7-15: CV Enrollment Notification

7.3 Program Tag Management

Program tags are created and managed at the organization level and are not inheritable. They are used to provide additional restrictions for users and org level configurations when interacting with subjects and cases. To access the Program Tags page, you will need to have the **Program Tag Manager** or **Operations Manager** role.

How program tags are used:

- Users utilize the program tag in their User Assignment Capabilities to grant them access to view or work on cases/tasks. Only Non-Restrictive program tags can be used in assignment capabilities. See Add Persona for more information.
- Cases/tasks automatically have the program tags of the subject added. It is the organization's responsibility to implement the tag for it to have any effect on the view/assignment permissions or workflow.
- Subjects have their respective organizations' program tags added to their profile. These add visibility/assignment permissions to all cases related to this subject.
- Certain system engines and configurations for an organization (notifications, assignment rules, Workflow Builder, etc.) can use program tags to further expand their capabilities.

7.3.1 CREATING A PROGRAM TAG

1. From the left navigation menu, select **Org Management**.

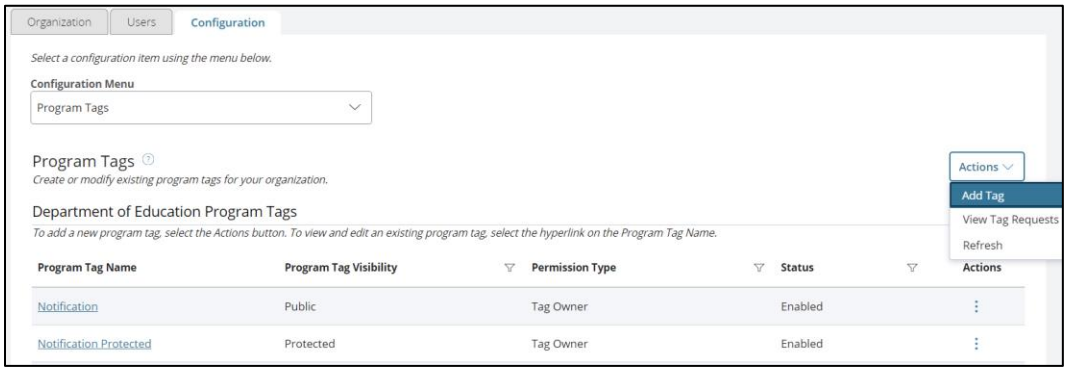


Figure 7-16: Org Management - Add Tag Action

2. Select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **Program Tags**.
4. To create a new tag, from the **Actions** drop-down, select **Add Tag.**

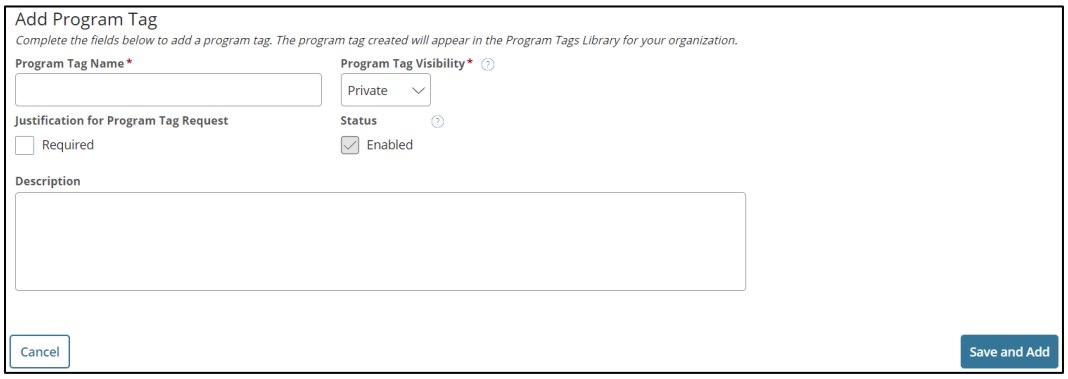


Figure 7-17: Add Program Tag

5. Fill in the program tag information.

   Note: The system will generate a unique ID to serve as the program tag abbreviation.

   The **Program Tag Visibility** determines if other organizations can join the tag and use it.

   - Private: Other organizations cannot request to join the tag. It will only be available to this organization.
   - Protected: Other organizations must request to be a Tag Modifier or Tag Owner
   - Public: Other organizations can join as a Tag Modifier without going through the requesting process. Organizations must still request to be Tag Owner.

6. Select **Save and Add**. The Program Tag you created will appear in the list of Program Tags for your Organization.

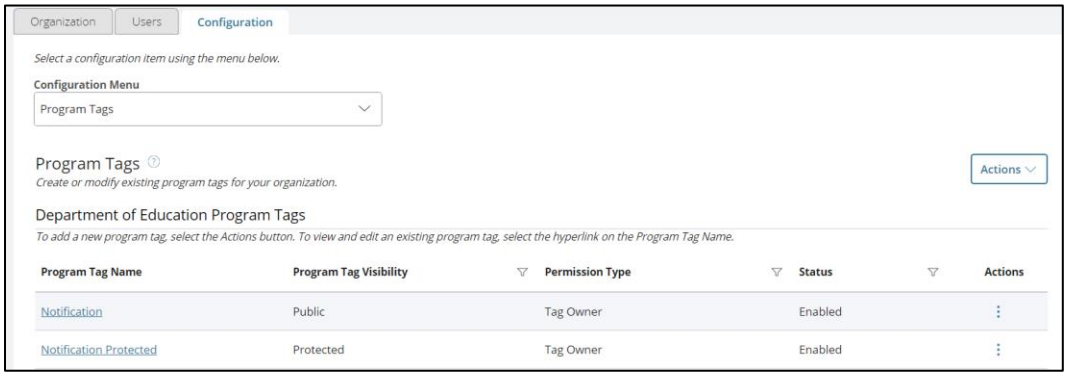


Figure 7-18: Org Management - Program Tags

7.3.2 VIEW AND EDIT A PROGRAM TAG

1. From the Program Tag main page, select the **Program Tag** to view details for.

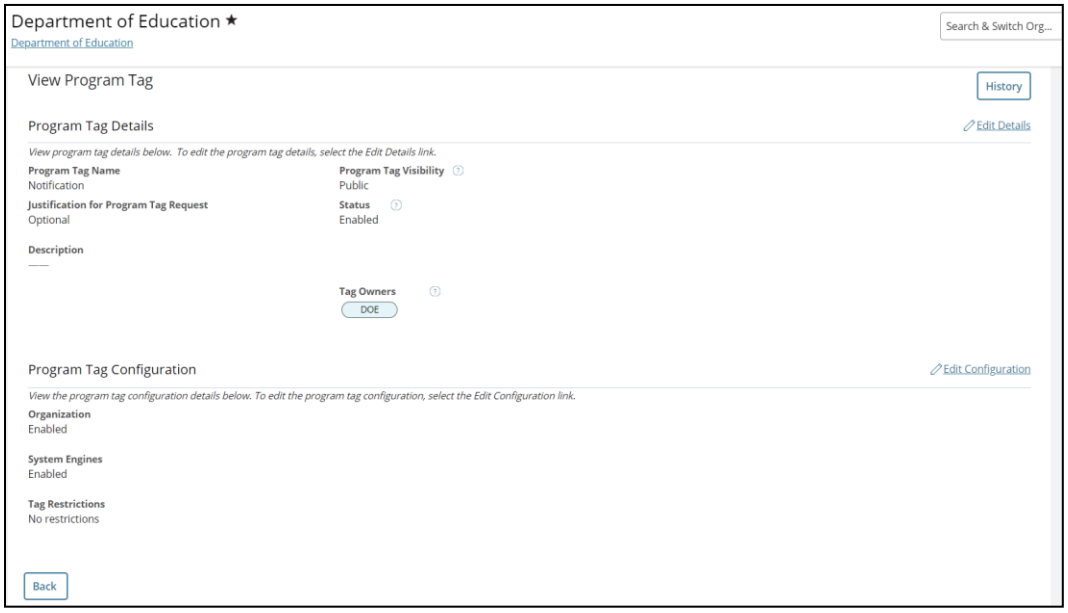


Figure 7-19: Program Tag Details

2. Select **Edit Details** to modify the tag's specific details.

   Note: Program tags are only editable by Tag Owners.

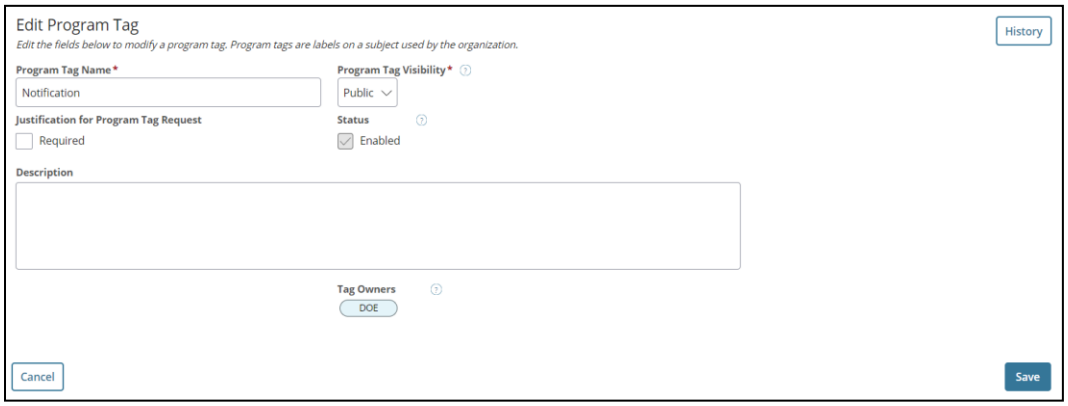


Figure 7-20: Edit Program Tag Details

3. Select **Save** when the changes are complete.

7.3.3 EDIT CONFIGURATIONS OF A PROGRAM TAG

1. Select a Program Tag to view details for.

2. Select **Edit Configuration** to modify the system configurations or restrictions for this program tag. See Program Tag Configuration Reference Tables for more information about the fields.

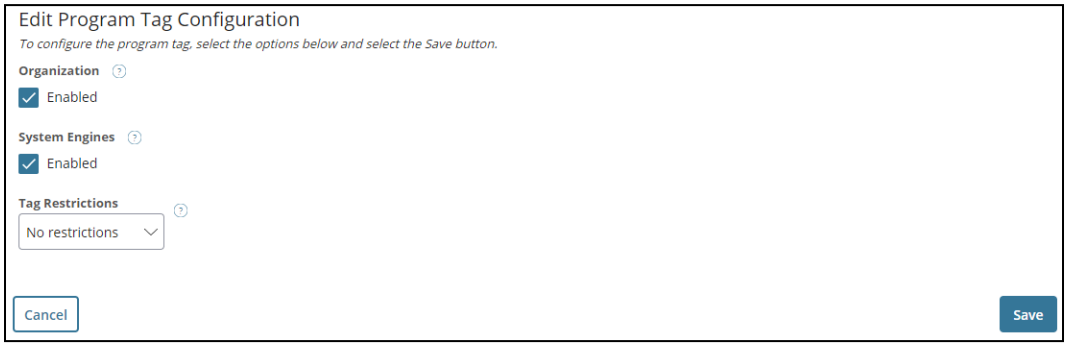


Figure 7-21: Edit Program Tag Configuration

3. Select **Save** when the changes are complete.

7.3.4 PROGRAM TAG LIBRARY

The Program Tag Library beneath the organization program tags contains all other program tags that are used by other organizations in the Protected or Public visibility. This is where the Program Tag Manager can become Tag Modifier and Owner of the other program tags.

Joining a public tag allows your organization to become a Modifier without having to go through the request process.

To Request Access to a Public Program Tag

Figure 7-22: Program Tag Library - Join

1. From the list of Available Program Tag(s), under the Actions column, select the **ellipses** and select **Join.**

7.3.5 REQUESTING TAG PERMISSIONS

Figure 7-23: Program Tag Library - Request Permission

1. From the Program Tag main page, locate the desired program tag and under the **Actions** column, select the **ellipses**, and select **Request Tag Modifier Permission** or **Request Tag Owner Permission**.

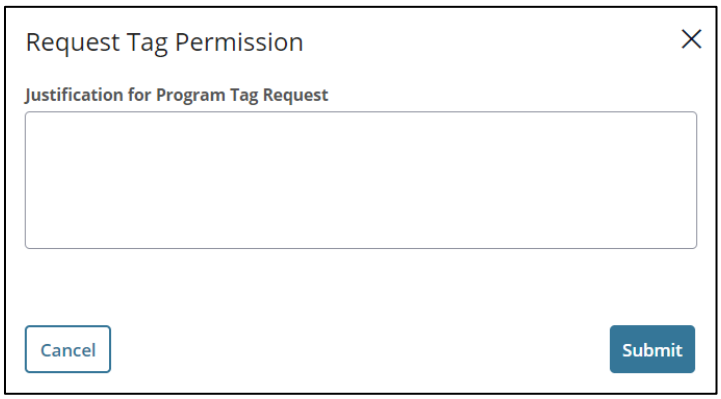


Figure 7-24: Request Tag Permission Pop-up

2. Enter the justification for the request and select **Submit**.

7.3.6 APPROVING/DENY A REQUEST

When other organizations request permission to one of your Program Tags, their request will appear on your Program Tag Requests page.

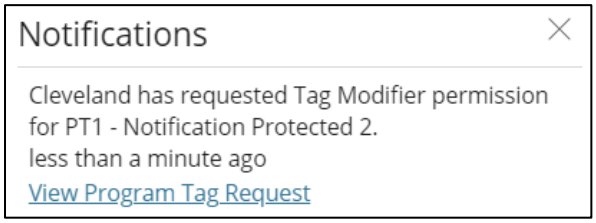


Figure 7-25: Program Tag Request Notification

You may also receive a notification with a link to display the details of the Program Tag Request.

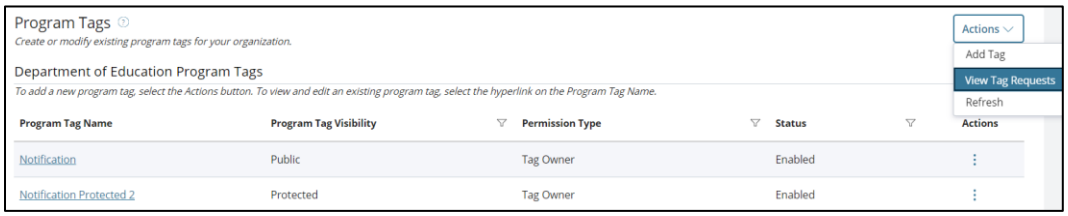


Figure 7-26 Program Tag Page- View Tag Requests

1. On the Program Tag main page, from the **Actions** drop-down, select **View Tag Requests**. The page will display all the Incoming and Outgoing Requests for your organization. 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 tags.

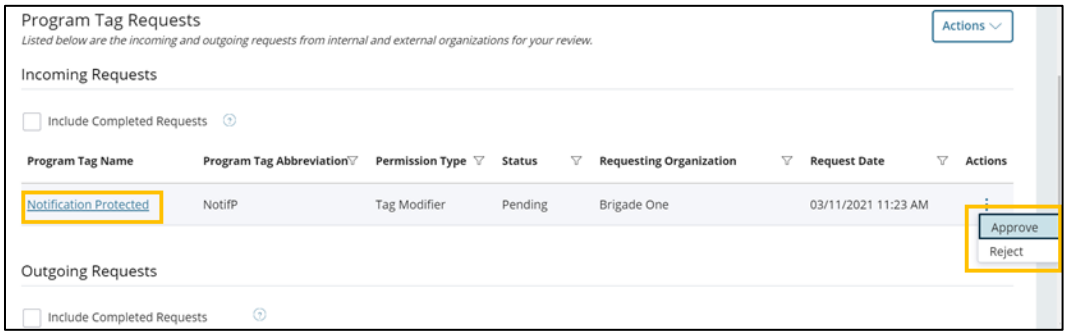


Figure 7-27: Program Tag Requests Page

2. 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.

Figure 7-28 Request Overview Details

3. Select **Reject/Approve**.

   Note: If a Program Tag Request is rejected, a pop-up will display asking you the reason for rejecting (this is optional) and the request will be moved into the rejected status. Approved requests will display the program tag in the list of My Program Tags and will allow the current organization access to the program tag.

7.3.7 PROGRAM TAG CONFIGURATION REFERENCE TABLES

Table 7-3: Program Tag Configuration Fields

Configuration Field Name	Description
Organization	Determines if the tag is enabled for the current organization
System Engines	Enables the tag to be used with notifications and assignment rules
Tag Restrictions	Determines if the tag can restrict a user's access to a case (see table below)

Table 7-4: Program Tag Configuration Restrictions

Program Tag Configuration Restriction	Description
No restrictions	No restrictions are placed on the case by adding this tag. This tag cannot be applied to user assignment capabilities.
Work on the case	The user must have this tag to be able to be assigned the case. This includes the permission to open and view the case.
Open the case	The user must have this tag to open the case even in read-only mode. This does not allow them to be assigned the case to work.
View the Subject	The user must have this tag to view the subject profile and search for the subject in the Global SSN Search. The Work on Case restriction is also implicitly included with this tag.

Note: The restrictions set on the program tag only apply to your organization's level of access on cases.

Note: If your user assignment has the program tag, you will be able to see and work on the case regardless of if the program tag configuration has restrictions.

7.4 Organization Relationships

The Organization Relationships page is a way for your organization to establish a connection with other organizations and distribute services for other organizations to utilize. The services your organization can provide are related to the Provider Org Functions your organization can have, which is determined by your Org Types. This information can be found in the Org Details page within Org Management. The **Organization Relationship Manager** is the only user that can configure these relationships.

Using the Org Relationship page to establish relationships will allow you certain privileges within the system, such as utilizing other organizations outside of your hierarchy in Form Routing. This will also allow you to access certain Services from other organizations, if available.

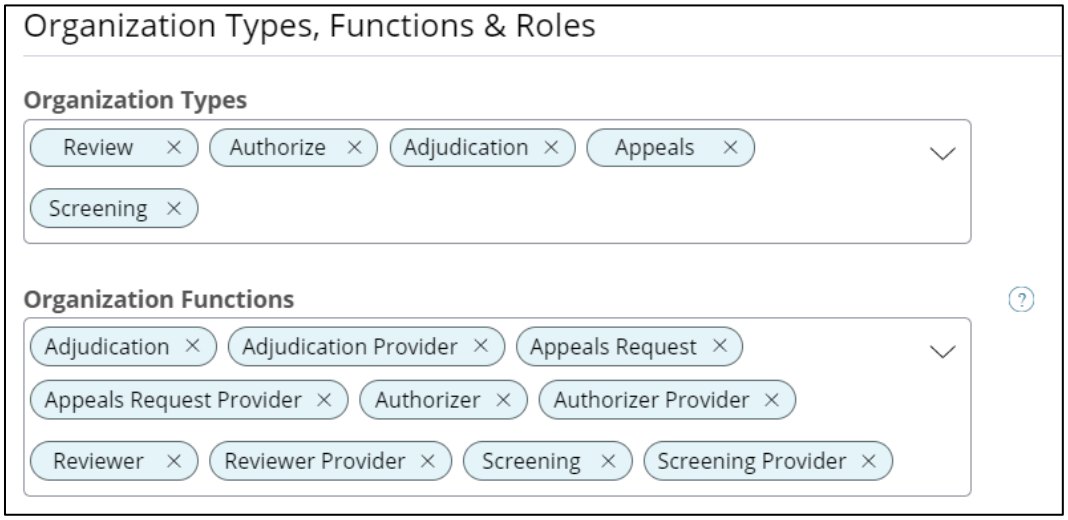


Figure 7-29: Org Types, Functions, and Roles

To edit the Organization Relationship page, your organization must contain one of the "Provider" functions for the respective service, under the list of Org Functions. As a Service Provider organization, you will be able to edit who you provide services to, and how you implement your organization's services on the "Internal Relationship Management" section of the screen. Once an internal relationship is configured for a service, external relationships can be established for that service.

7.4.1 INTERNAL RELATIONSHIPS

1. From the left navigate menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the **Configuration Menu** drop-down, select **Organization Relationships**.
4. Under the **Internal Relationship Management** section, select **Edit Relationships**.
5. Here, you can set your org as the **Service Provider Organization**. From there, you can designate one of your sub-organizations within your hierarchy to be the implementor responsible for carrying out the service.

   Note: The Service Owner Organization does *not* have to be your org.

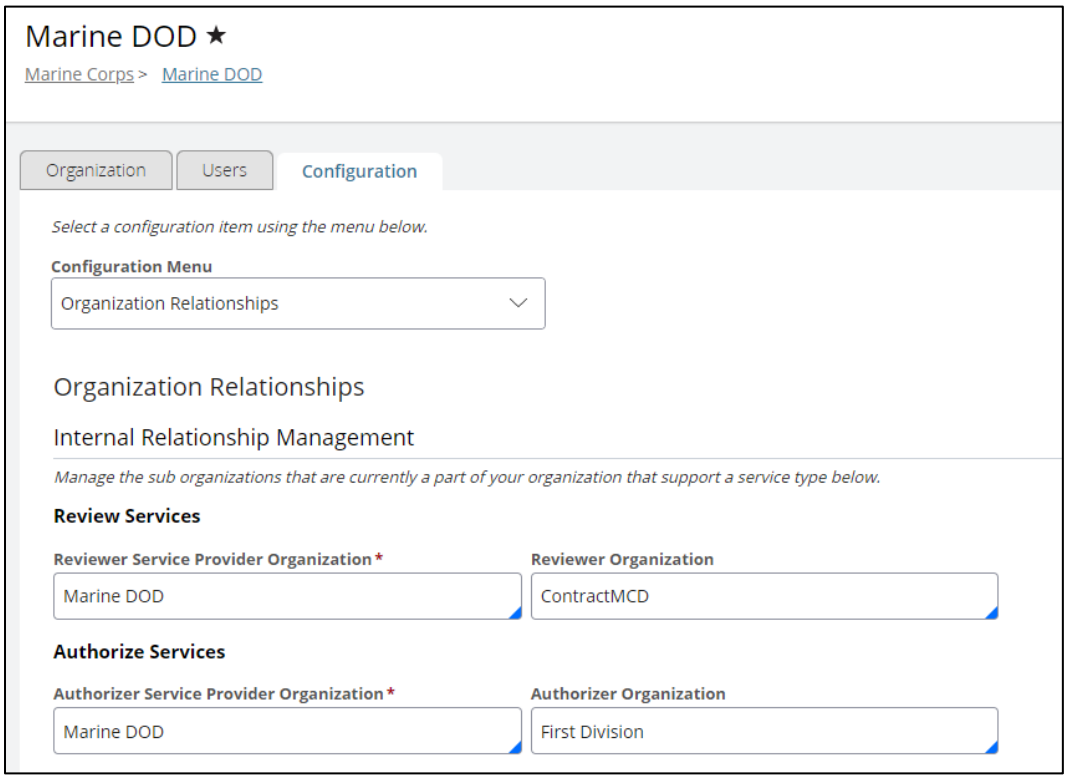


Figure 7-30: Internal Relationship Management

Note: Only sub-organizations that also have the corresponding Org Function, are selectable in this field item. This includes your organization.

6. Select **Save** after making your selections.

7.4.2 EXTERNAL SERVICE RELATIONSHIPS

The External Service Relationship Management section of the page displays the organizations you are providing services for. Once you have configured your internal relationships, you can share your configured services out to other orgs for them to utilize.

To provide your configured services to other organizations:

Figure 7-31: Org Relationships

1. Under the **External Service Relationship Management** section, select **Edit Relationships**.

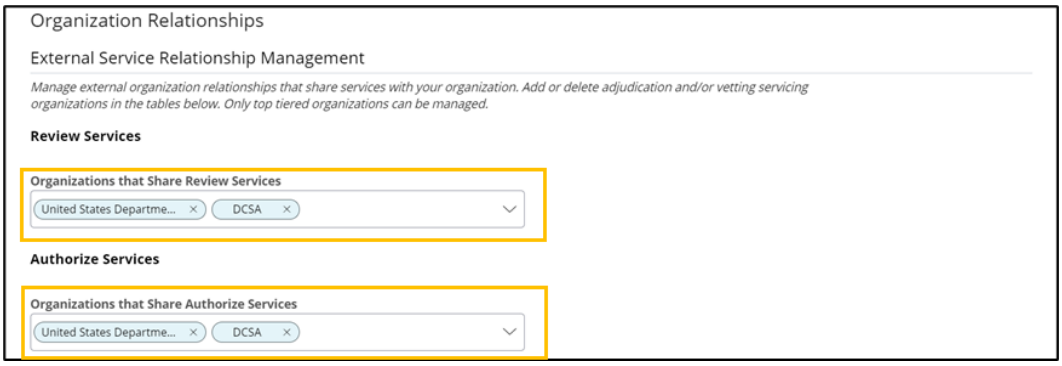


Figure 7-32: External Relationships Management

2. In the spaces provided under each service, you can enter organizations you would like to provide your services to.
3. Once you have made your selections, select **Save** at the bottom of the screen.

Note: As a consumer or receiver of these services, if you are an organization that does not have any of the "Provider" functions, then under Organization Relationships you will only see the tables displaying the relationships you currently possess for each service.

To view services provided to your organization:

The "Services Received" table displays the services being offered to your org by external service providers. This would be configured in the providing organizations' External Service Relationship Management.

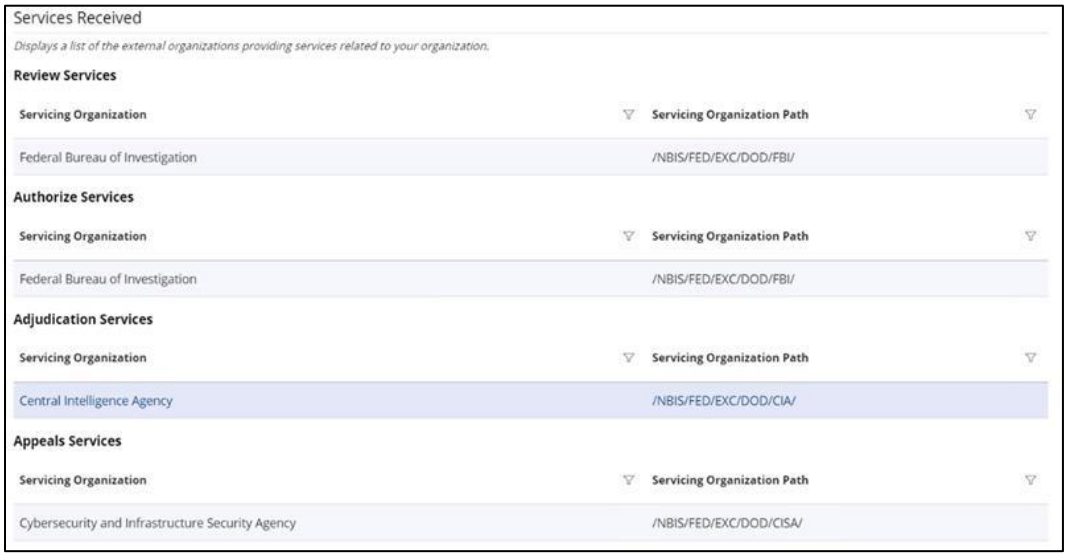


Figure 7-33: Services Received Table

7.5 Service Catalog

Operations Managers can use the Service Catalog to configure a service for **Adjudication, Appeals, Investigation, Screening,** and **Vetting organizations**. Operations Managers can access the Service Catalog via the **Configuration Menu** on the **Org Management – Configuration Tab** and can configure case types to provide services (for example, Incident Reports) for all internal organizations and some external organizations (including their sub orgs). The Operations Manager can connect a service from the Service Catalog to a workflow which is configured in the **Workflow Builder**. Once a service is connected to an active workflow in the Workflow Builder, a **Servicing Organization** can share their services based on the configurations in **Organization Relationships**. Workflow Builder and Organization Relationships can both be found in the Configuration Menu on the Configuration Tab. Based on the configured relationships, an organization can create a case or request for a service from the Service Catalog using the **Create Case or Create Request** options that are available within a Subject's Profile in **Subject Management**.

Note: Once a service is configured it cannot be deleted. If the service is no longer needed, it will need to be disabled.

7.5.1 CONFIGURING A CASE TYPE (SERVICE)

To view all Case Types (also known as Services):

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** Tab.
3. From the Configuration Menu drop-down, select **Service Catalog**.

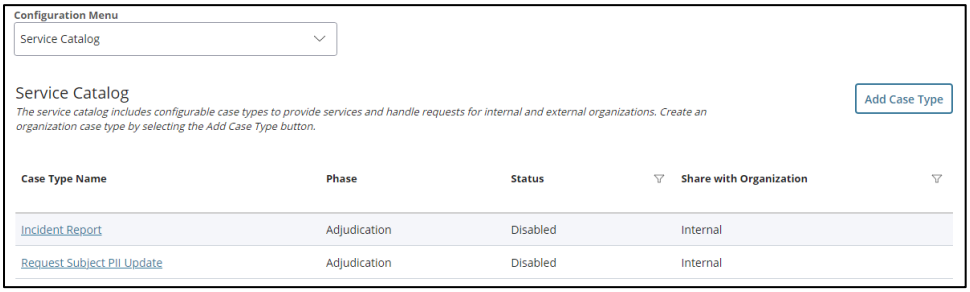


Figure 7-34: Org Management - Service Catalog

To add a Case Type (Service):

4. Select **Add Case Type**.
5. Complete the Add Case Type page:

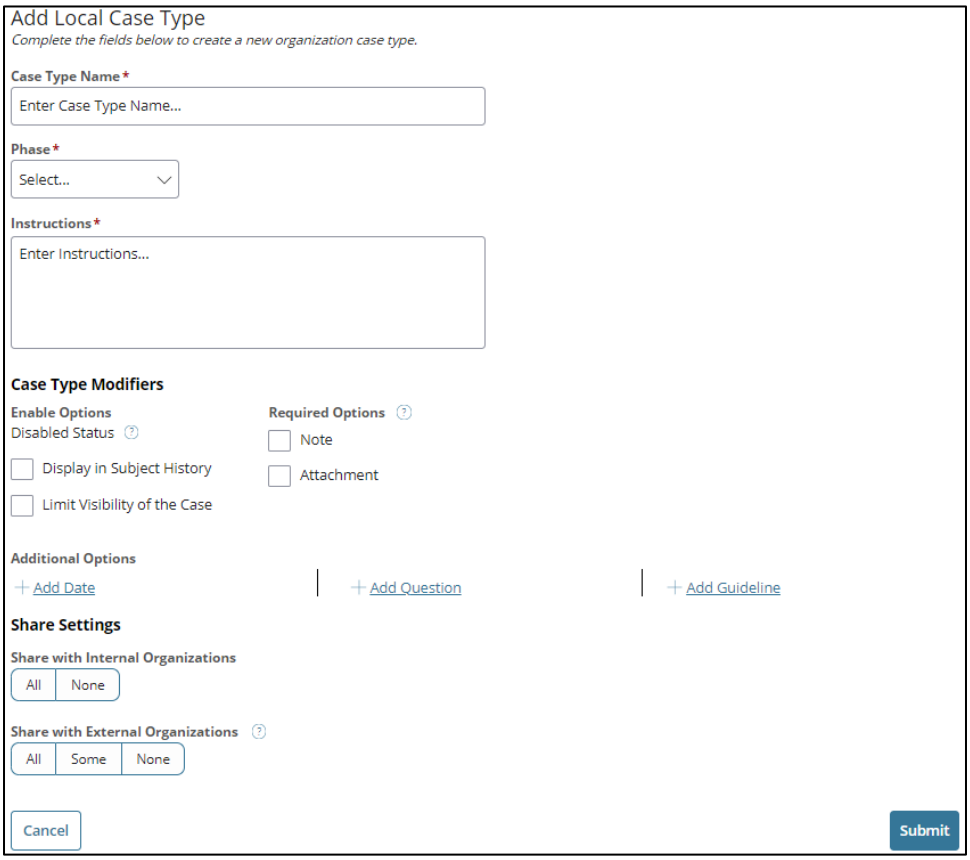


Figure 7-35: Add Local Case Type

6. Enter the **Case Type Name** and select the **Phase** you would like the Service to be a part of.
    - Additional fields may appear based upon the selected **Phase**.

      Note: If **Validation** is selected as the **Phase**, a **Related Phases** field will appear and populate with **Quality Review**, **Preparation**, and **Investigation**. The configured case type is able to phase transition between these related phases.

      A **Service Types** field will also appear to optionally associate Service Type(s) to the case. This drop-down is populated from the **Manage Priorities/Service Types** table in System Settings. See the **NBIS Admin User Guide** for more information.
    - For **Investigation** organizations, a **Case Product Case Type** field will appear to allow a user to select which type of investigation this case type will apply to so that the applicable Case Product is generated. Currently, only "RSI" is available.
    - Provide **instructions** for the requesting organization.
    - Select the **Display in Subject History** checkbox if the case type should appear in a subject's history.

- Select the **Limit Visibility of the Case** checkbox to limit the display of the case type. If selected:
    1. Users in Vetting, Investigation, Adjudication, Screening, and Appeals orgs will always see the presence of the case in the Subject Profile and History.
    2. Users in SSC, FSO, Review, Authorize, and Component Adjudication orgs or sub-orgs will only see the case on the Subject Profile and History if the user is in the org that created the case.
- Make **Enable** and **Required Options** if needed.

  Note: User cannot select **Enabled** checkbox until the Service has been tied to a workflow. Once the connection is made, the user must edit the Service to enable it.
- Add **Additional Options** for **Dates**, **Questions**, and **Guidelines** if needed.
- Select whether the local product will be used for **internal** or **external use**. If only some external orgs should have access to the product, select **Some.**

7. Select **Submit** to save the Case Type.

To view a Case Type (Service):

8. Under the Case Type column, select the desired **Case Type link** to view the details about the specific service.

To edit a Case Type (Service):

9. Select the **Edit** button. Make any changes as needed.
10. Select **Submit** to update the Case Type.

7.5.2 CONNECTING A SERVICE TO WORKFLOW BUILDER

11. Once the service is created, navigate to Workflow Builder from the Configuration Menu drop-down.
12. See the Manage Workflow Actions section on configuring workflow actions. Follow all steps in the section, making sure that your service is selected in **the case type dropdown.**
13. Return to Case type in the Service Catalog and enable it.

7.6 Case Categories

Case categories are a way to label and group continuous vetting alerts and investigative leads based on common properties. They are used to restrict who can work on cases and what actions can be taken on the case. The **Operations Manager** can configure Case Categories at the organization level to group business rules. Business rules are the criteria that cause a CV case be created.

For CV, case categories are configured by the CV Service Provider for the CV Implementor organization defined in org relationships. Case Categories cannot be configured in the Implementor organization unless they are also the provider.

For Background Investigation, case categories are configured by the Investigation control org and are inherited by its sub-orgs.

Case Categories are an additional filter for configuring Actions in a workflow and are determined by the organization creating the workflow in Workflow Builder. See Add a Workflow Action for more information on how case categories can be used in Workflow Builder Actions and Workflow 360 for how they are used for validation with Workflow 360.

See **NBIS Admin User Guide** for more information on Alert configurations.

Note: Once a case category is created, it cannot be deleted. To make the case category unavailable, the Operations Manager must disable it.

To view the Case Category List:

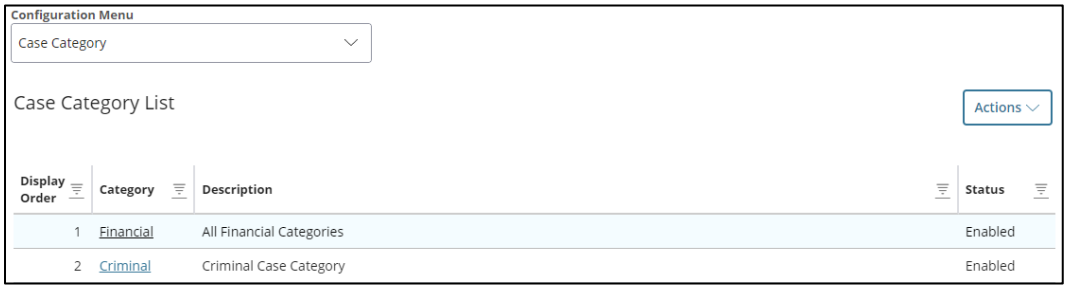


Figure 7-36: Org Management - Case Category List

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab to view the configuration options.
3. From the Configuration Menu drop-down, select **Case Category**.

To add a Case Category:

4. From the Actions drop-down menu, select **Add New Category**.

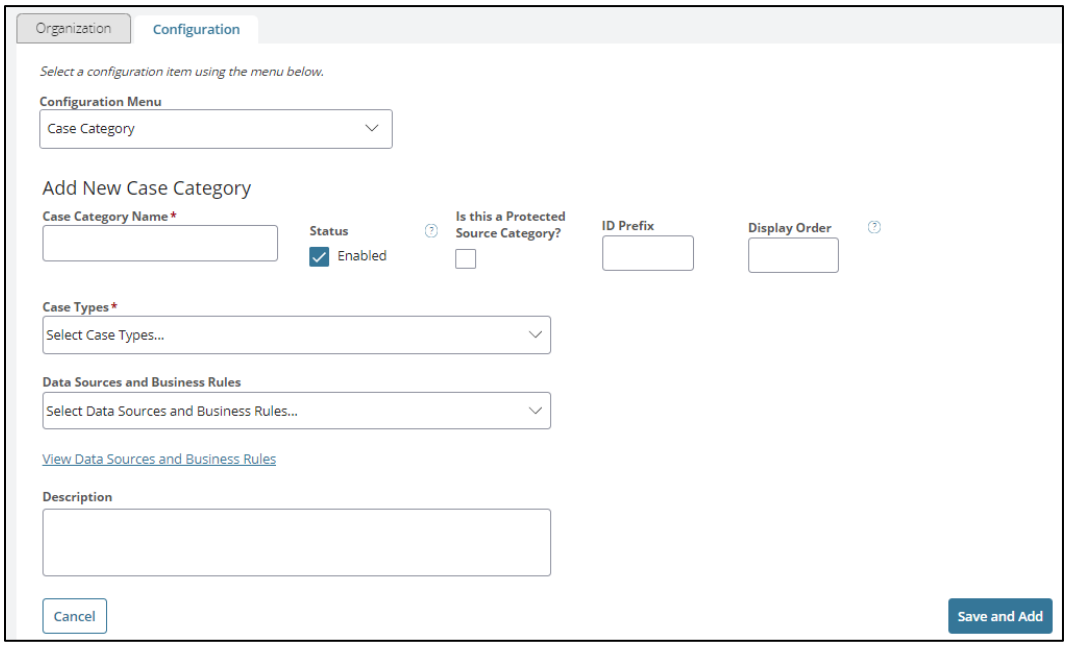


Figure 7-37: Add New Case Category

5. Complete the required fields.
    a. Case Category Name
    b. Status – Indicate whether this Category is enabled.
    c. Protected Source Category – Indicate whether this Category is a Protected Source. Only applicable to Background Investigation.
    d. ID Prefix - If the User is in an Investigation Org type, they are able to enter an ID Prefix. Any lead created for this category will contain this ID Prefix in the Lead ID.
    e. Display Order – Indicate the desired display order.
    f. Case Types – Select Case Types associated to this Case Category.
    g. For **Investigation** organizations, a **Case Product Item Group** field will appear. This allows for the sorting of Case Product documents. The selection made in this field will indicate the header and footer that will be used for the Case Product for this configured case (lead) category.

       The options available for selection are managed in System Settings, currently by Developer Admin.

6. Define the **Data Sources and Business Rules**.

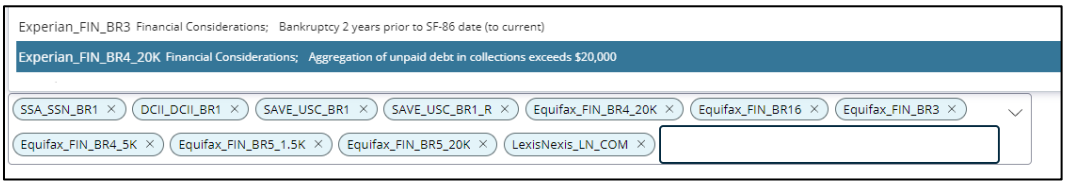


Figure 7-38: Data Sources and Business Rules Drop-down

Select the **View Data Sources and Business Rules** link to open a list of a data sources and business rules. This pop-up will show which data sources and business rules are already configured in an existing case category. A specific business rule cannot be configured to multiple case categories. The available options are configured in the Manage Data Sources table in System Settings.

The Data Sources and Business Rules are added to an organization to allow for the assignment and prioritization of alerts. The drop-down is only available to **Operations Managers** accessing organizations within their hierarchy. All options displayed in this drop-down may not apply to your organization.

7. Select **Save and Add**.

To edit a Case Category:

8. In the table of **Case Categories,** select a **Category**.
9. From the **Actions** drop-down, select **Edit Case Category**.
10. Make any changes and select **Save** when completed.

7.7 Ingest Management

When cases come in through File Ingest, they need to be routed to organizations for Adjudication. The configurations in the **Ingest Management** table determine the pathway for subject files that come into the system via **File Ingest**. The **Operations Manager** for an Adjudication organization can add, view, and edit this table.

The Ingest Management table uses the **SOI Org Mapping** table in System Settings to match subject files to an Org. The **System Manager** can add, edit, and view the SOI Org Mapping table. See the **NBIS Admin User Guide** for preliminary configuration assistance.

When subject files come into the system via **File Ingest**, the Ingest Management table checks the SOI Org Mapping table. If a mapping is found, then the actions the system will take depend on the configurations in the Ingest Management Table.

Based on the configurations in the **Ingest Management** table, files that have **SONs (Submitting Office Number Orgs)** or **SOIs (Security Office Identifier Orgs)** mapped to them in the system can have an adjudication case created and be routed to their associated organization for **Adjudication**. For example, when a **Special Agreement Check (SAC)** or **National Agency Check (NAC)** comes in, this table is referenced for an enabled **SON Org** (Submitting Office Number Org) mapping.

If the SON in the files is not mapped, then it can only match with records that use "all SON." If the actions configured are to create a case and reroute the case to the SON org, this *cannot* be completed because the org is not in the system. In this scenario, the file would go through the default actions and the case would be created in the associated SOI org.

The **Case Ingest 2.0 report** in the **Reports** tab will track the ingested files. Filters can be applied to view files by Organization, File Ingest Type, Investigation Type, SOI and Ingest Date.

If ingested files do not have a matching SON nor a SOI, then those files will be placed into an error queue so that they may be requeued later when an SOI has been mapped for the file. The files that do not have a match will be included in the **Ingest Rules Report** in the **Reports** tab. The Ingest Rules Report shows a status column which will indicate what action was taken on a file such as AdjCreated, NoCaseCreated, Eadj.

Once the mapping has been added for these files, they can be assigned correctly. See Reporting for more information.

Note: The rules process sequentially. If there is an issue with the processing order, the configurations will need to be deleted and recreated in the appropriate order. If configurations need to be added or edited, these modifications will only affect future ingest cases, not actively assigned cases. The **Add Ingest Configuration** will always add the configuration to the end of the list.

To view all Ingest Configurations:

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **Ingest Management**.

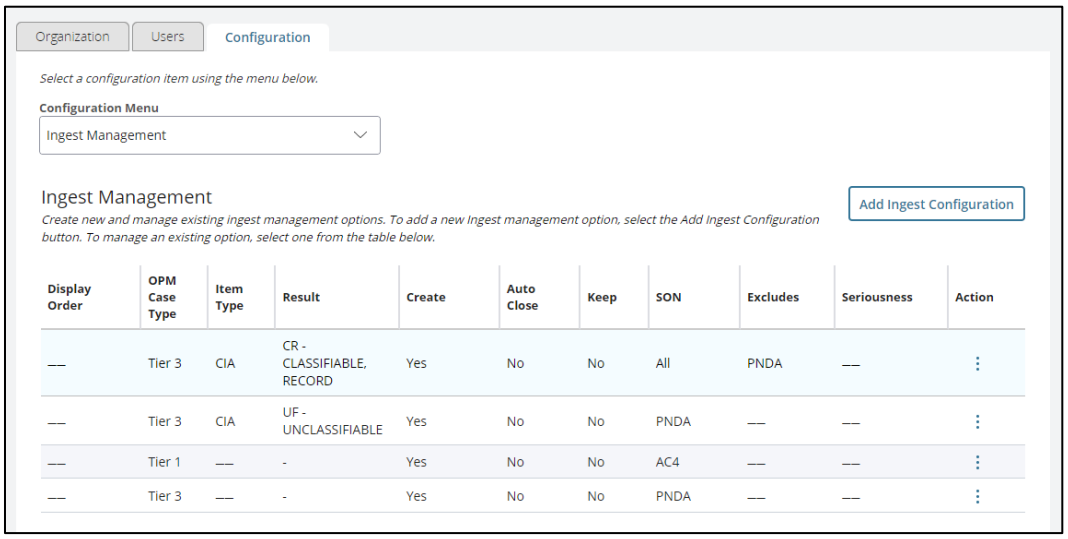


Figure 7-39: Org Management - Ingest Management Table

To add an Ingest Configuration:

4. Select **Add Ingest Configuration**.

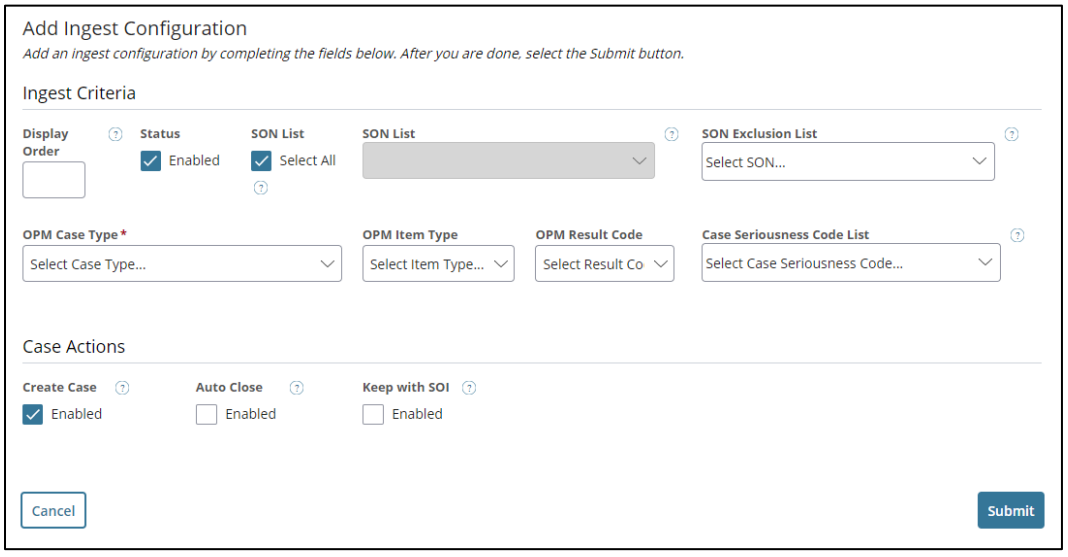


Figure 7-40: Add Ingest Configuration

5. Fill in the required fields.

   Ingest Criteria:

   a. **Display Order** – indicates the display order for this set of files

   b. **Status Checkbox** – checked for enabled will make the configuration active for your organization

   c. **SON List Checkbox** – checked will include all SONs configured in SON Org Mapping table in System Settings

   d. **SON List** – specific SONs that this configuration will apply to

   e. **SON Exclusion List** – specific SONs that will be excluded from this configuration

   f. **OPM Case Type** – case type that this configuration will apply to

   g. **OPM Item Type** – investigation items included on the DIF file

   h. **OPM Result Code** – result code of the investigation item included in the DIF file

   i. **Case Seriousness Code List** – multiselect field of codes to indicate case seriousness

   Case Actions:

   j. **Create case** – if checked, case will be created for cases matching the criteria selected under Ingest Criteria

   k. **Auto Close** – if checked, when incoming case matches the configured ingest criteria, the case will be immediately closed

   l. **Keep with SOI** – if checked, when incoming case matches the configured ingest criteria, the case will be kept by the configuring organization. If unchecked, the case will be routed to the SON and the SON must have an active workflow configured in Workflow Builder to ingest successfully.

6. Select **Submit**.

To edit an Ingest Configuration:

7. From the Ingest Management main page, locate the desired configuration and under the **Actions** column, select the **ellipses**.
8. Select **Edit Configuration**.
9. Select **Submit**.

To delete an Ingest Configuration:

10. From the Ingest Management main page, locate the desired configuration and under the **Actions** column, select the **ellipses**.
11. Select **Delete Configuration**. A confirmation pop-up will appear.
12. Select **Continue**.

7.8 Order Form Template Management

Order Form Templates can be configured to fill out some or all Order Form (Agency Use Block, AUB) information. These sections include Position Details, Optional Coverage, and Financial Details. The **Template Manager** can manage an organization's Order Form Templates from the **Order Form Library**. Sub-organizations can also inherit templates from their parent organization if the **Only My Organization** checkbox is left unchecked (disabled).

A user can **link** or **copy** an existing template 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.

To view all Templates:

1. From the left navigation menu, select **Order Form Library**.
2. From the **Organization** drop-down, select an **Organization** to view its Order Form Templates.

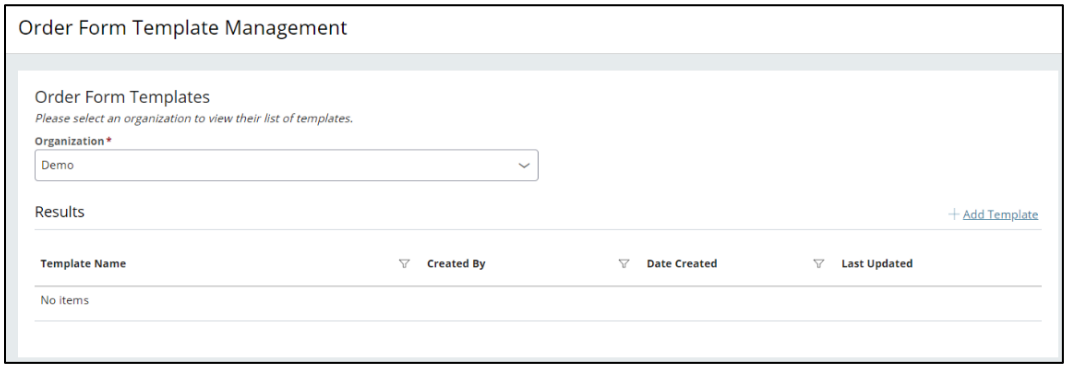


Figure 7-41: Order Form Template Management

To add a Template:

3. In the selected organization, select **+Add Template** to create a new Order Form Template.

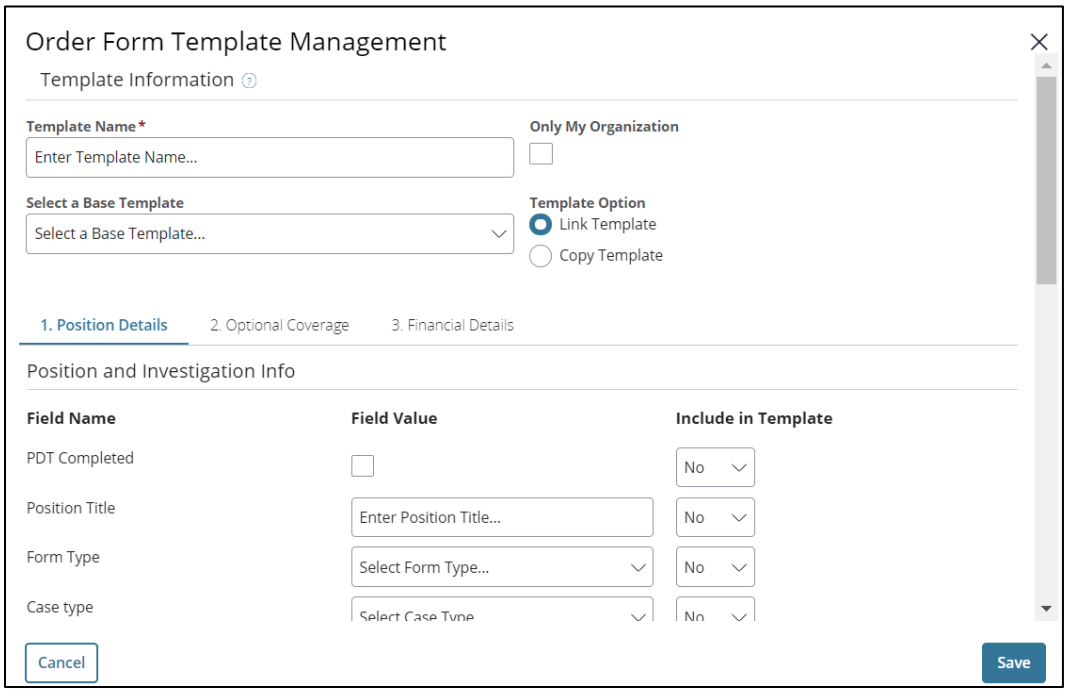


Figure 7-42: Add Order Form Template

4. Complete the **Order Form Template** fields including the Optional Coverage and Financial Details tab with desired values.

   Note: When entering data, change the **Field Value** for the value to be applied. If **Field Value** is set to no value, data will not be applied.

   Note: Change the **Include in Template** value to **Yes** to apply the field value to the template.

   Note: Select **Only My Organization** check box if you do not want the template to be automatically inherited by sub-organizations within your hierarchy.

5. Select **Save** to create the template.

To view a Template:

6. From the **Template Name** column, select a **Template**.

To edit a Template:

7. Select **Edit** to modify a template. Make all desired changes.
8. Select **Save** to save the modified template.

7.9 Form Routing

The **Workflow Manager** is responsible for managing the Agency Workflows in the **Form Routing** tab. A form routing **Workflow** determines which organizations will perform the review and authorization phases of the agency process for the Initiating Org.

Two tables will be displayed: one displaying all workflows for your organization, and one showing all workflows that you are a part of (including Organization Relationships). For reference on establishing a relationship, go to Organization Relationships.

To view all Workflows:

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** Tab.
3. From the Configuration menu drop-down, select **Form Routing.**

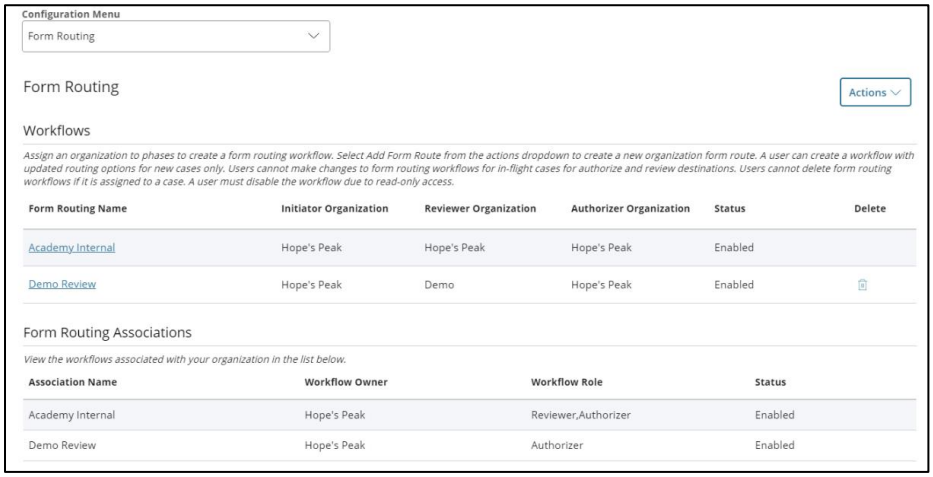


Figure 7-43: Configurations - Form Routing

Note: From the Actions drop-down you can access the table **History**.

Note: Users cannot delete a form routing workflow if it is assigned to a case. A user can disable a workflow to prevent further use.

To add a Workflow:

1. From the Actions drop-down, select **Add Form Route** and complete the form.

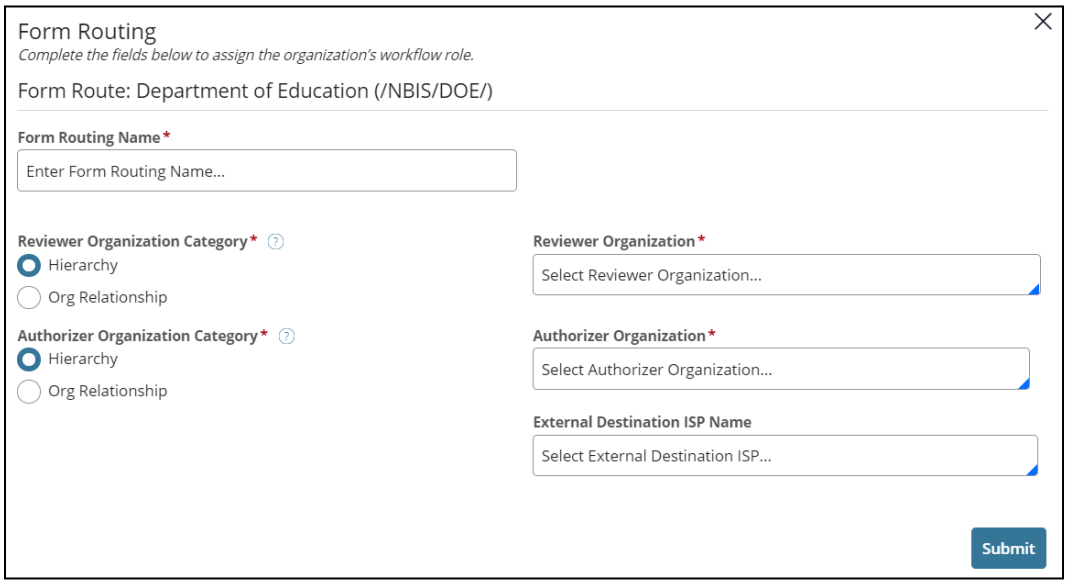


Figure 7-44: Add Form Routing Screen

2. Select a **Reviewer Organization Category** of **Hierarchy** or **Org Relationship** to indicate whether the organization will be from your hierarchy or from your configured organization relationships.
   - Select **Hierarchy** to choose the same organization in which you are creating the workflow or other organizations within your hierarchy to complete the phase.
   - Select **Org Relationships** to choose an organization you have established a relationship with, that is outside of your organizational hierarchy, to complete phase.

     Note: Organizations must have established an Organization Relationship during set up to appear in this selection. For reference on establishing a relationship, go to Organization Relationship.
3. Select a **Reviewer Organization**.
4. Select an **Authorization Organization Category** of **Hierarchy** or **Org Relationship** to indicate whether the organization will be from your hierarchy or from your configured organization relationships. See the above definitions for the selection.
5. Select an **Authorizer Organization**.
6. Optionally select an **External Destination ISP Name** for cases to be routed to once the submission is released.

   Note: External Destination ISP Names will be populated by the Manage External ISP Routing table in System Settings. See the **NBIS Admin User Guide** for more information.
7. Once all required fields are completed, select **Save** to create and save the new workflow.

7.10 Managing Case and Form Types at an Organization Level

This tab can only be accessed by an **NBIS System Administrator**. This configuration tab allows an organization to modify its enabled case types and respective form types. Disabled Case Types and Form Types will not be available to Subject Managers when initiating cases on Routing Details. Case and Form Type Associations are managed at an organizational level. See the **NBIS Admin Guide** to find information on how to manage this association at a system level.

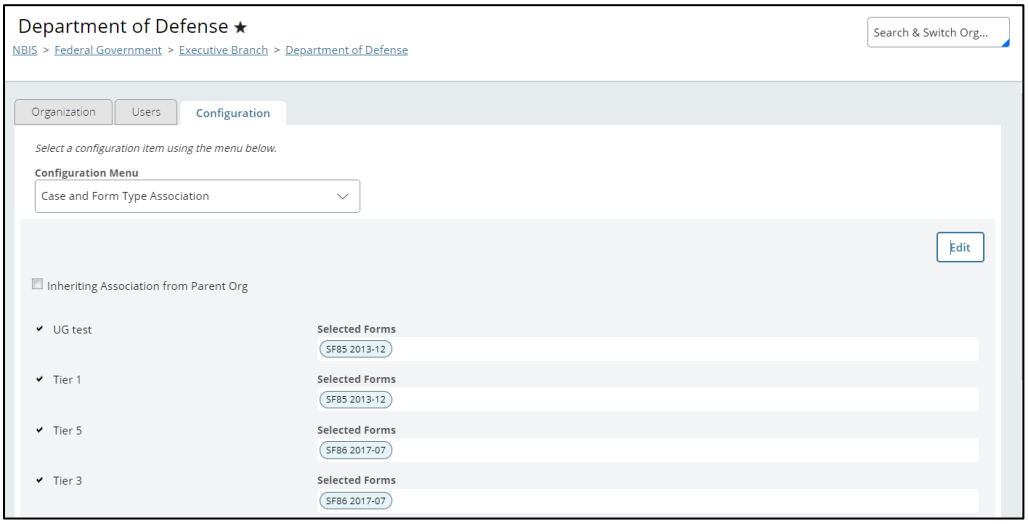


Figure 7-45: Case and Form Type Association

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **Case and Form Type Association**.

   Note: When you first view this page, you will see the default settings that have been inherited from your parent organization. All the tiers and forms present are ones that are enabled in System Settings.
4. Select **Edit**.
5. Uncheck **Inheriting Association from Parent Org** so that the fields below will become editable. You have the option to add or remove tiers and form types for your organization, which will affect any cases requests that are created going forward.

   Note: If the parent organization has any updates to this association, you will need to reselect the **Inheriting Association from Parent Org** checkbox to receive those changes.
6. Select **Save** once you have made all desired changes.

7.11 Distribution Rules

The **Distribution Rules** determine how the cases and tasks are distributed and routed throughout an organization's hierarchy. Rules are configured based on case phase and case type. The **Distribution Manager** for an organization with the Investigation Control function can add, view, and edit this table.

To view all Distribution Rules:

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. Select **Distribution Rules** from the **Configuration Menu** dropdown.

To add a Distribution Rule:

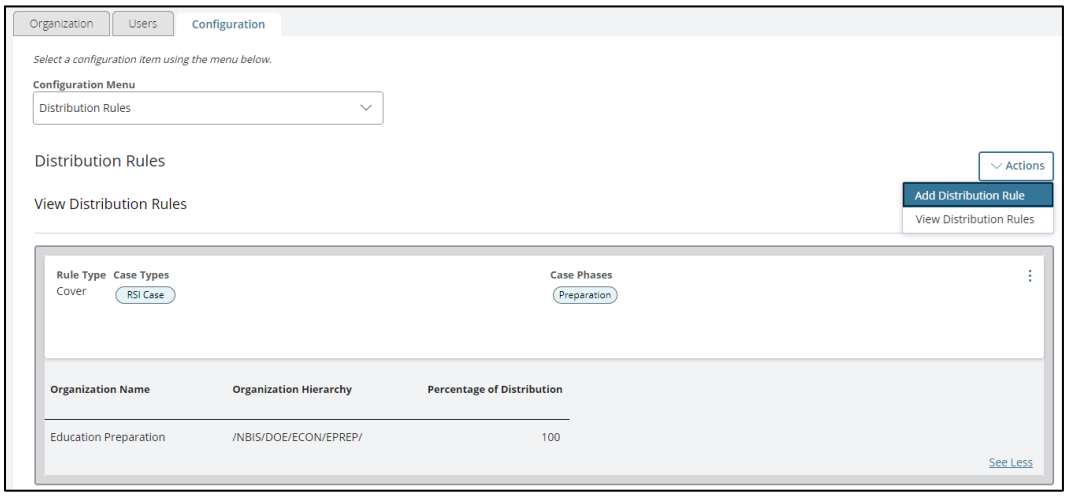


Figure 7-46: Org Management - Distribution Rules

4. From the **Actions** drop-down, select **Add Distribution Rule**.

Figure 7-47: Add Distribution Rule - Rule Type Dropdown

5. From the **Rule Type** drop-down, select **Cover** or **Lead**.

   Note: The **Rule Type** determines if the distribution rule applies to cover or lead cases. It also determines which fields will display.

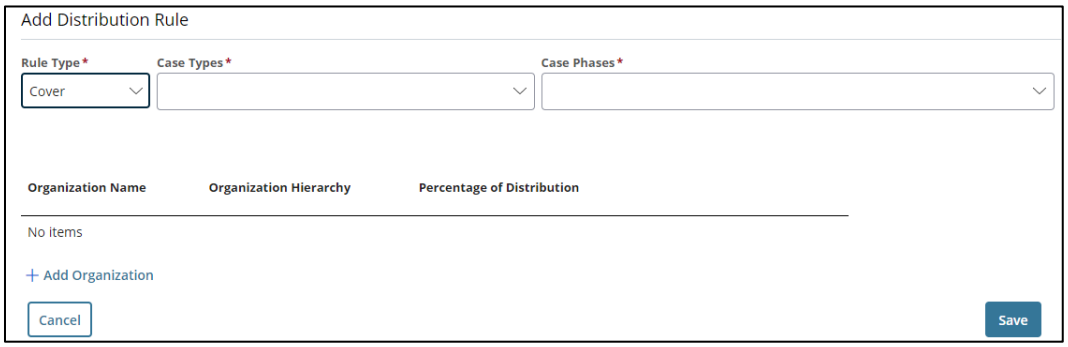


Figure 7-48: Add Distribution Rule – Cover Rule Type

6. Fill out the remaining required fields.
7. Select **Add Organization** to add additional organizations for distribution of this phase and case type.

   Note: When adding more than one organization, the **Percentage of Distribution** for the organizations must equal 100.
8. Select **Save**.

To edit a Distribution Rule:

9. Select the **Ellipsis** of the distribution rule you need to update.
10. Select **Edit Distribution Rule**.
11. Update the distribution rule and select **Save**.

To delete a Distribution Rule:

12. Select the **Ellipsis** of the exception rule you need to delete.
13. Select **Delete Distribution Rule**. A confirmation window will appear.
14. Select **Delete Distribution Rule**.

7.12 Question Configuration

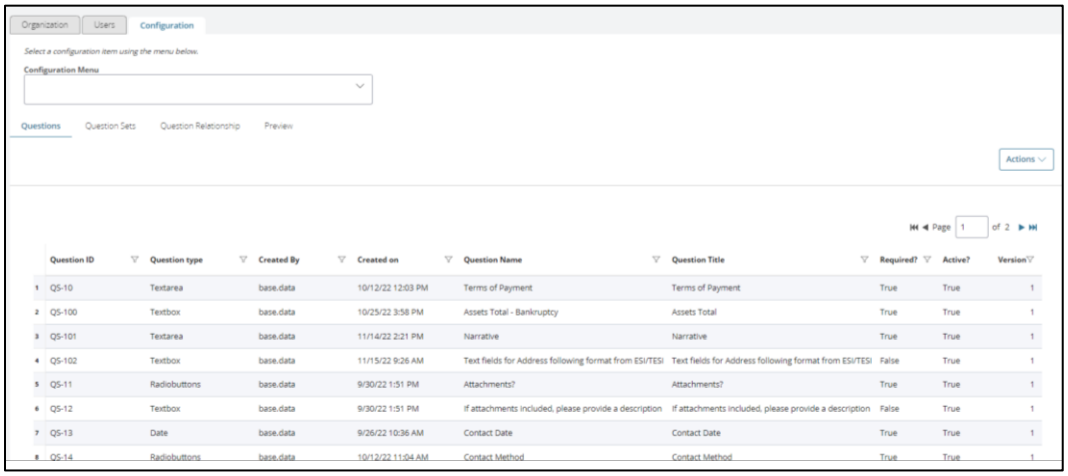
The **Question Manager** in an Investigation control organization can view, edit, and create question sets for their organizational hierarchy. Questions configured in Org Management will be used by the Analyst and/or Investigator when completing leads. Question sets configured here can be associated to Scoping Rules for a lead, see Series of Checks section for more information on associating question sets to lead categories.

When configuring your questions sets, the Question Manager will first create the questions, then the question set, and then pair them together in the Question Relationship tab.

All RSI Question sets will be prepopulated in Question Configuration for each investigation control organization.

Question Configuration

1. From the left navigation menu, select **Org Management.**
2. Select the **Configuration** tab.
3. From the configuration menu drop-down, select **Question Configuration**.

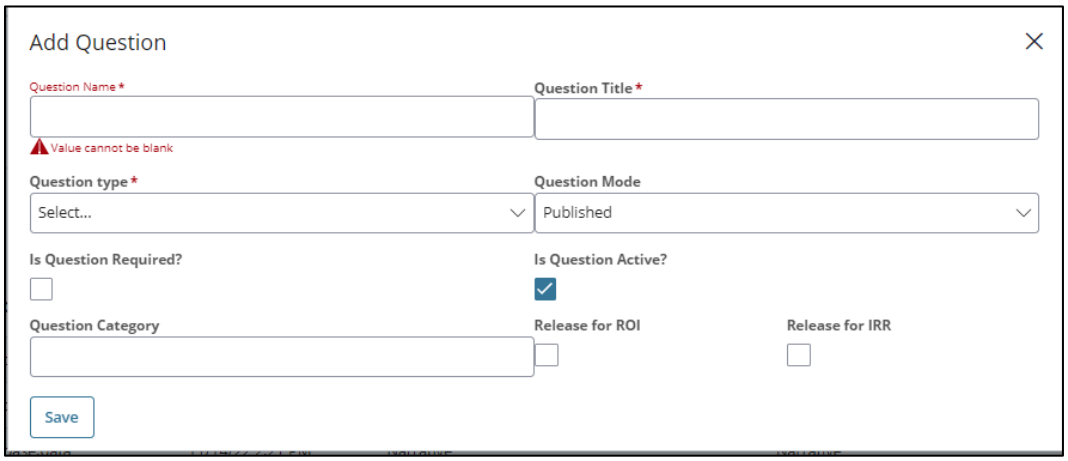


7.12.1 CREATING A QUESTION

On the Questions subtab, Question Managers can configure individual questions that can be assigned to Question Sets.

To add a Question:

1. From within the **Question Configuration** page, select the **Questions** subtab.
2. From the **Actions** drop-down, select **Add Question**.



3. Enter a **Question Name**, **Question Title**, and **Question Type**.

   Note: Question Name & Title are essentially the same. For ease of use recommendation is to put the same value in both.

4. Select the **checkboxes** to indicate whether the question is **Required** and if it is **Active**.

   Note: The **Active** checkbox is marked by default. Inactive questions cannot be added to Question Relationships.

5. Select the **checkboxes** for **Release for ROI** (Results of Investigation) or **Release for IRR** (Investigation Results Report) to indicate if this question can be included in the case products.

6. Select **Save**.

To edit a Question:

7. From within the **Questions** subtab table, double click the **row** of the question to be edited.
8. Make any necessary changes.
9. Select **Save**.

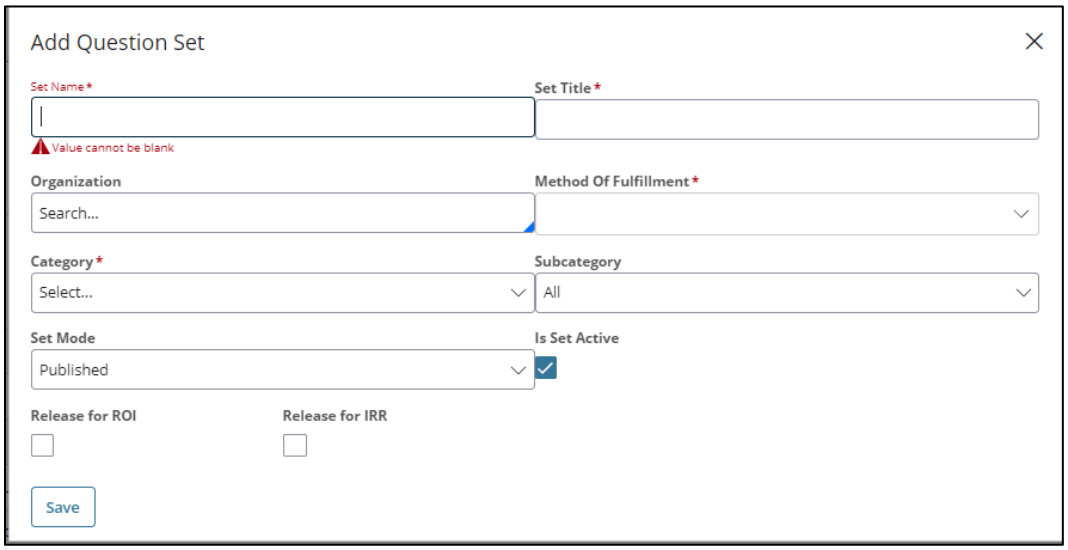
7.12.2 CREATING A QUESTION SET

Question Sets allow the user to organize individual questions into different sets.

The Question Manager can create, edit, and delete Question Sets. Once configured, they can be configured with a lead's checks so that during an investigation, an Analyst and/or Investigator can use those questions to conduct the investigation. For more information on selecting question sets in Scoping Rules, see Series of Checks section.

To add a new Question Set:

1. From within the **Question Configuration** page, select the **Question Sets** subtab.
2. From the **Actions** drop-down, select **Add Question Set**.



3. Complete the required fields.
    a. Set Name – the set name will not be visible to users completing the question set, but is used for configuration purposes by the Question Manager on the back end. For ease of use, recommended to put the same value as Set Title.
    b. Set Title – the title that will be visible to users completing the question set.
    c. Organization – the organization(s) that will utilize this question set.
    d. Category – pre-set values of Lead Categories
    e. Method of Fulfillment – CRC, ARC, Field
    f. Set Mode – should default to Published and have this selection if you want the question set to be visible and utilized.
    g. Set Active – should default as checked and have this selection if you want the question set to be visible and utilized.
4. Select the **checkboxes** for **Release for ROI** (Results of Investigation) or **Release for IRR** (Investigation Results Report) to indicate if this question can be included in the case products.

To edit a Question Set:

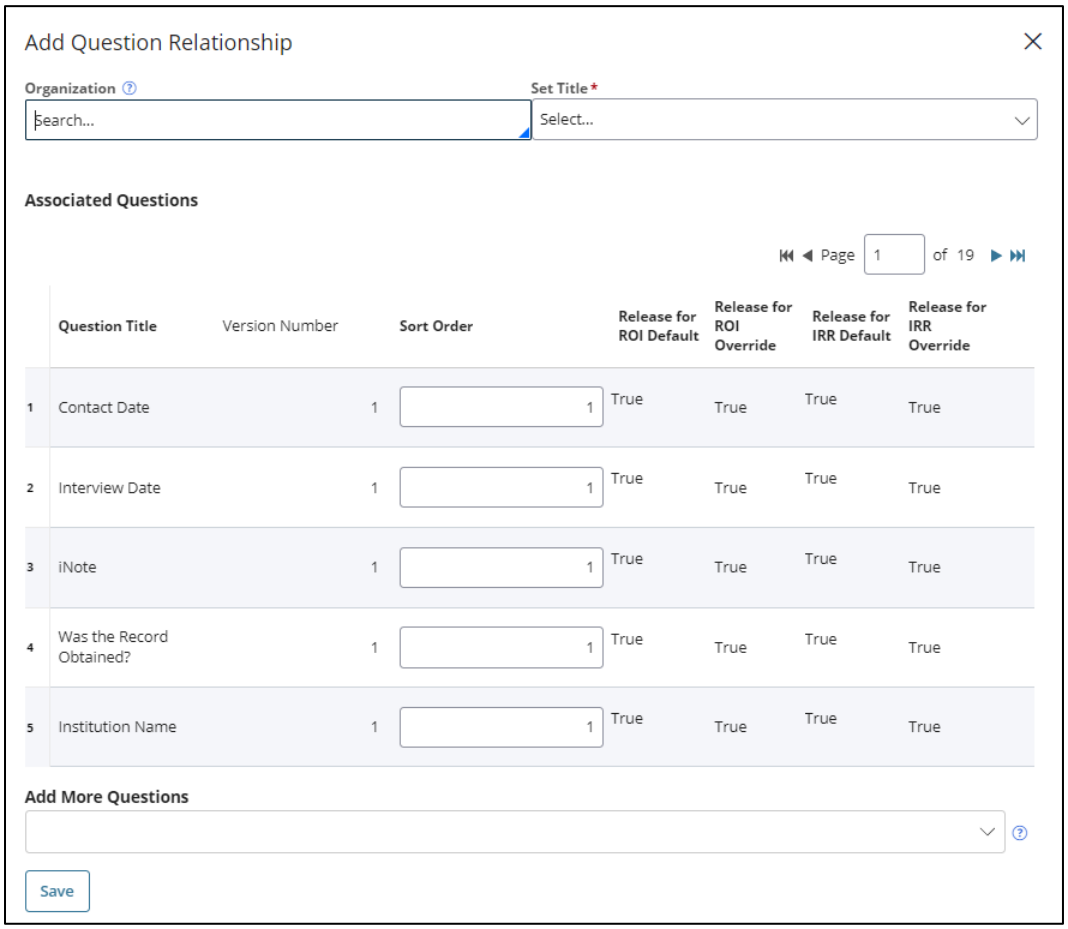
1. From within the **Question Sets** subtab table, double click the **row** of the question to be edited.
2. Make any necessary changes.
3. Select **Save**.

7.12.3 CREATING A QUESTION RELATIONSHIP

The Question Relationship allows the user to assign configured questions to configured sets. Question Managers can update configured Question Relationships as needed.

To Add a Question Relationship:

1. From within the **Question Configuration** page, select the **Question Relationships** subtab.
2. From the **Actions** drop-down, select **Add Question Relationship**.



3. Select an **Organization**.
4. Select a **Set Title** (Question Sets are preconfigured by the organization).

   Note: The options in the drop-down are the Question Set titles configured in the Question Sets subtab.
5. Select the **Questions** to affiliate with the **Relationship**.
6. Select the **Release for ROI Override** checkbox to override the initial Release for ROI designation.

Note: For example, if the default is set to **TRUE**, selecting this checkbox will make it so that this question is *not* released for ROI.

7. Select the **Release for IRR Override** checkbox to override the initial Release for ROI designation.

   Note: For example, if the default is set to **TRUE**, selecting this checkbox will make it so that this question is *not* released for IRR.

8. From the **Add More Questions** drop-down, select additional **Questions** to include in the relationship (from the question bank).
9. Select **Save**.

7.12.4 PREVIEW A QUESTION SET

The Preview tab can be found on the subtabs of the Question Configuration Menu. This tab is used to preview the Question Sets to see how they will appear on screen for a caseworker.

To Preview a Question Set:

1. From within the **Question Configuration** page, select the **Preview** subtab.

Figure 7-49: Preview Question Set

2. From the **Set ID** field, select a **Set-ID#** which corresponds to a question set.
3. The question set preview will appear below.

8 Progression Engine

The progression engine is used for Continuous Vetting (CV) and Investigation cases to systematically detect when a case is ready to move into the next status (for CV) or next phase (for investigation). In CV, the progression engine decides when to push the case forward to the next review-type status, based on completed alert cases. For Investigation, the progression engine decides if an Investigation case can move to Quality Review based on completed leads. An organization can configure exception rules so that a case will be pushed forward even when all alerts or leads are not closed. See the following section for how to configure these rules.

8.1 Case Progression Exception Rules

The **Case Progression Exception Rules** determine if a CV Cover Case can advance to the next status without all CV Alerts being closed. By adding an exception rule, the **Operations Manager** is indicating that alerts with certain attributes do not need to be closed for the case to move forward. If there are multiple exception rules for an organization, the progression engine will consider each one of them before moving the case forward. You must be an **Operations Manager** and the org must have the Continuous Vetting org Function to add, edit, or delete the exception rules.

> An organization only has one exception rule in the org's configurations. The rule says that 50% of low priority, criminal alerts for CV need to be closed. This means if the case has four low priority, criminal alerts and two of them are closed, then the case can progress forward *if* all other alerts are closed too.

Case Progression Exception Rules are also used to process Investigation Cover and Lead cases by allowing an Investigation cover case to move to the Quality Review phase without all leads being closed. The progression engine is triggered when a lead closes or when a cover case SLA expires. It will determine whether a case can move forward based on the exception rules configured by the **Operations Manager** for an org with the Investigation Control function.

To view the Case Progression Exception Rule List:

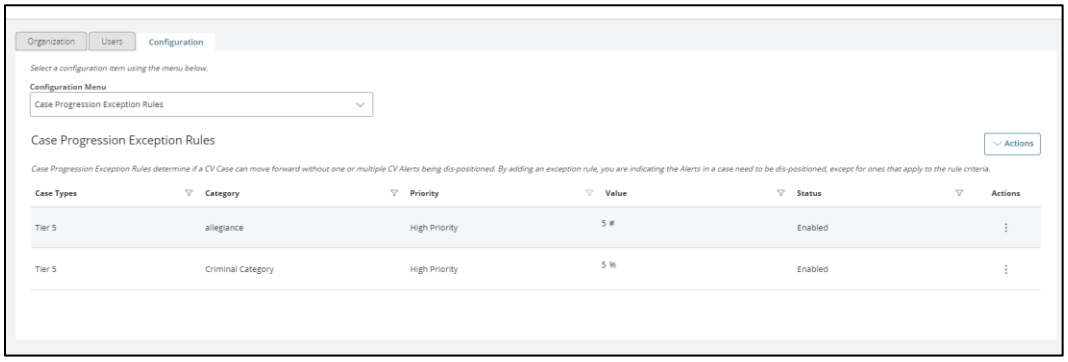


Figure 8-1: Org Management - Case Progression Exception Rules

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the Configuration Menu, select **Case Progression Exception Rules**.

8.1.1 CV ALERT PHASE

To add a Case Progression Exception Rule:

4. From the **Actions** drop-down, select **Add Rule.**

Figure 8-2: Add a Case Progression Exception Rule

5. From the **Phase** drop-down, select **CV Alert**.

a. Case Types – Type of case (this field captures both the Global Case Types and the Service Catalog Case Types).

b. Case Exception Category – Populated from the organization's case categories. This exception rule will only apply to cases with categories selected here.

c. Priority –Priority level of the case. This exception rule will only apply to cases with priority levels selected here. Populated from the Manage Priorities/Service Types System Settings table.

d. Value Type – select whether the number in the value amount should be interpreted by the system as a regular number or percentage to indicate the amount or number of alerts with the previously selected criteria that need to be closed in order for the case to progress forward.

e. Value Amount – enter a numeric value

f. Status – check enabled to apply this rule to the progression engine

6. Complete the required fields and select **Save and Add**.

To edit a Case Progression Exception Rule:

7. Select the **Ellipsis** of the exception rule you need to update.
8. Select **Edit Exception Rule**.
9. Update the exception rule and select **Save**.

To delete a Case Progression Exception Rule:

10. Select the **Ellipsis** of the exception rule you need to delete.
11. Select **Delete Exception Rule**.

8.1.2 INVESTIGATION PHASES

To add a Case Progression Exception Rule:

1. From the **Actions** drop-down, select **Add Rule.**

Figure 8-3: Add a Case Progression Exception Rule

2. From the **Phase** drop-down, select an **Investigation Phase**.
    a. Case Types – Type of case (this field captures both the Global Case Types and the Service Catalog Case Types).
    b. Case Exception Category – Populated from the organization's case categories. This exception rule will only apply to cases with categories selected here.
    c. Lead Status – Populated from the configured Workflow Builder statuses for the selected phase. This exception rule will apply to leads with statuses selected here, so they system can progress the case even if leads are in a particular status.
    d. SLA Expired – when checked, the rule will only apply once the SLA for the Investigation Phase has expired.
    e. Controlled Orgs – optionally select **Controlled Org(s)** to indicate which organizations within your hierarchy this exception rule will apply to.
    f. Status – check enabled to apply this rule to the progression engine.
3. Fill in required fields and select **Save and Add**.

To edit a Case Progression Exception Rule:

4. Select the **Ellipsis** of the exception rule you need to update.
5. Select **Edit Exception Rule**.
6. Update the exception rule and select **Save**.

To delete a Case Progression Exception Rule:

7. Select the **Ellipsis** of the exception rule you need to delete.
8. Select **Delete Exception Rule**.

9 Scoping Rules

The **Scoping Manager** can configure scoping rules that include subject details and tasks for the assigned investigator. The Scoping Manager configures scoping rules by creating rulesets which include adding leads, creating base rules and list rules, selecting contextual fields, and creating a series of checks. The following sections of the user guide explain how to create scoping rulesets.

The configured contextual fields will populate the Create Lead modal when a user is manually creating a lead. Methods of fulfillment will be configured for series of checks to indicate the parameters of a lead case for that Lead Category.

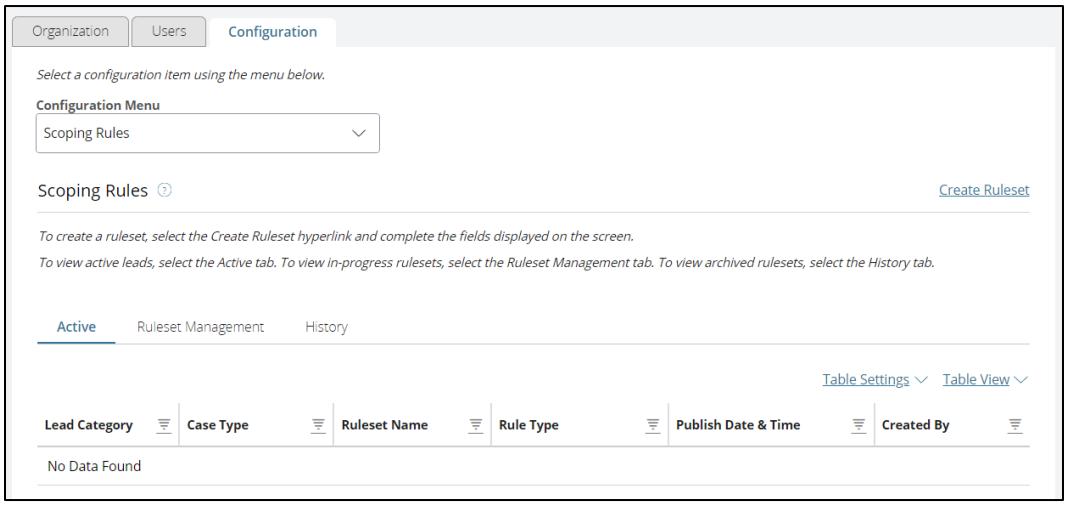


Figure 9-1: Org Management Configuration - Scoping Rules

Navigating to Scoping Rules

1. From the navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **Scoping Rules**.

On the **Scoping Rules** page there are the options to Create Ruleset, or view the **Active Tab**, the **Ruleset Management Tab**, or the **History Tab**.

9.1 Scoping Rules - Active Tab

The Scoping Rules – **Active** tab is where Active published rulesets can be viewed on a configurable table. Use the Table Settings and Table view links to configure the table. Select a Lead Category name to see details about that ruleset.

Figure 9-2: Scoping Rules - Active Tab

9.2 Scoping Rules - Ruleset Management Tab

The Scoping Rules - **Ruleset Management** tab is where created Rulesets can be viewed on a configurable table. Use the Table Settings and Table view links to configure the table. Select a Ruleset name to see details about that ruleset.

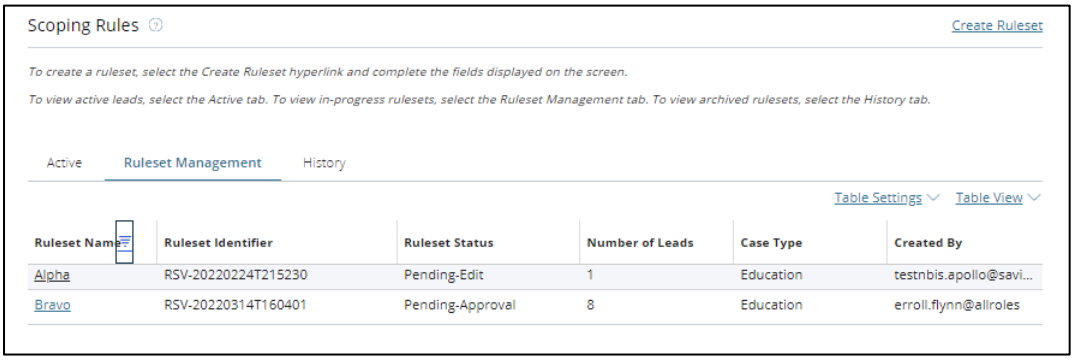


Figure 9-3: Scoping Rules - Ruleset Management Tab

9.3 Scoping Rules - History

The Scoping Rules - **History** tab is where previous Leads and Rulesets that have been completed or cancelled can be viewed on a configurable table. This History tab has buttons to view the **Leads** or **Rulesets**. Use the **Table Settings** and **Table View** links to configure the table.

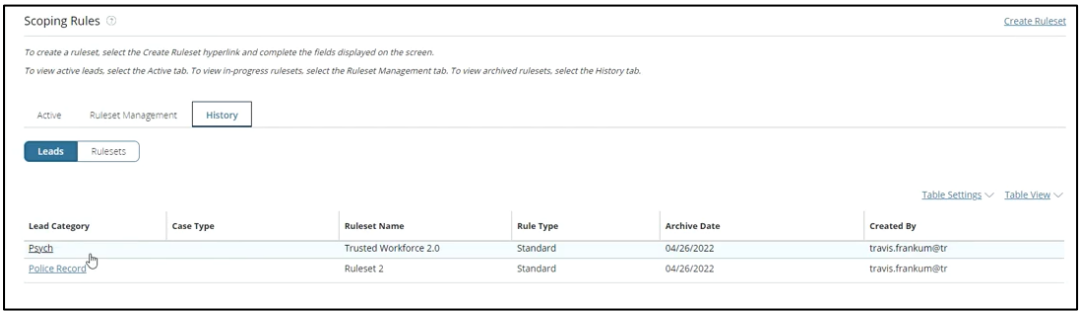


Figure 9-4: Scoping Rules - History Tab: Leads

4. Select the **History** tab and **Leads** to see archived leads.
5. From the **Lead Category** column, select a **Lead Category** to view more details.

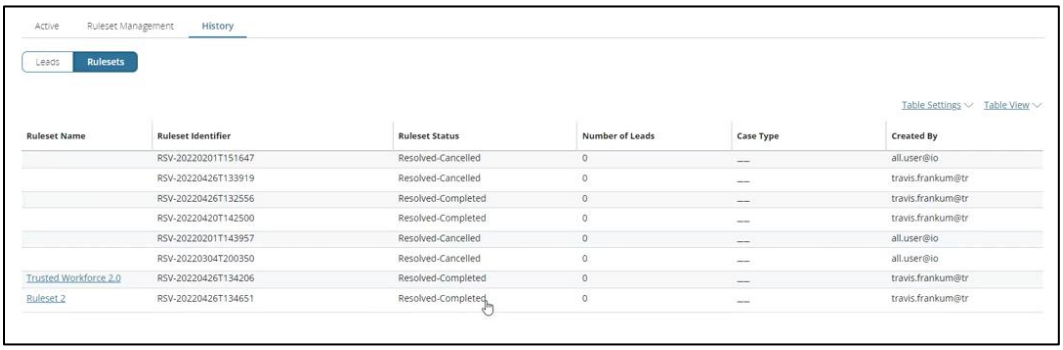


Figure 9-5: Scoping Rules - History Tab: Rulesets

6. Select the **History** tab and **Rulesets** to see rulesets that have been cancelled or completed.
7. From the **Ruleset Name** column, select a **Ruleset Name** to view more details.

9.4 Create a Ruleset

The first step in the process of configuring scoping rules is to create a Ruleset. The **Scoping Manager** can configure rulesets for their organization.

1. From the navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the Configuration Menu, select **Scoping Rules**.

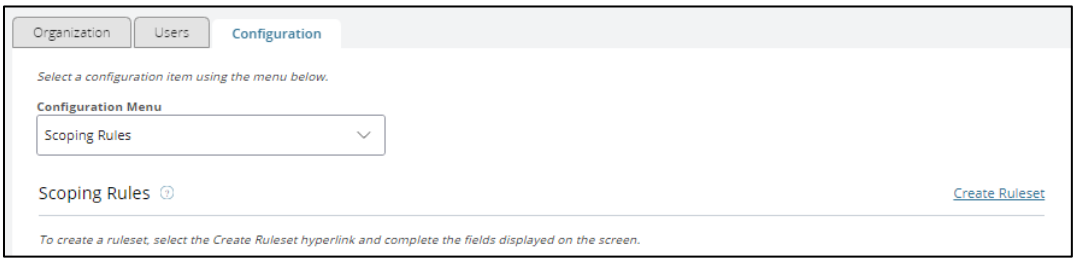


Figure 9-6: Org Management - Configuration - Scoping Rules - Create Ruleset

4. On the right side of the page, select **Create Ruleset**.

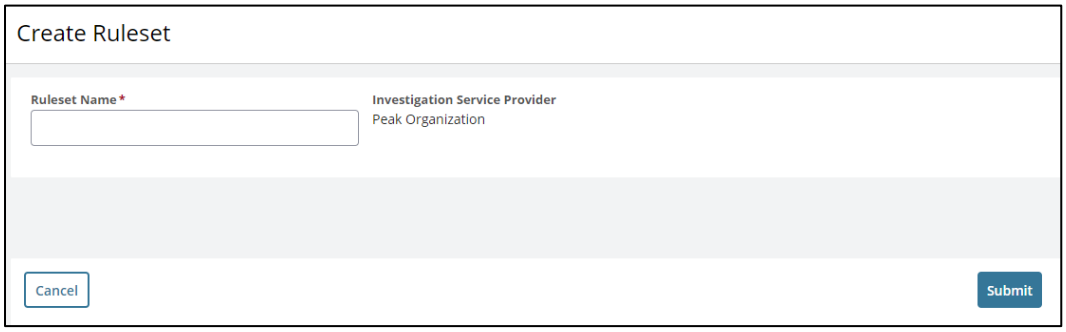


Figure 9-7: Create Ruleset

5. On the **Create Ruleset** screen, enter the **Ruleset Name** and select **Submit**.

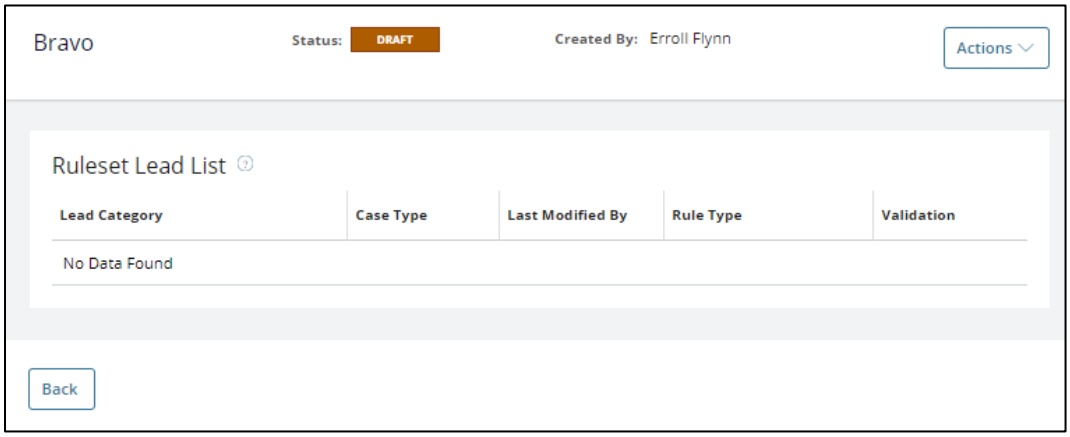


Figure 9-8: Example of a Created Scoping Rules Page

6. Select **Back** to return to the Scoping Rules page.

9.5 Lead Categories

Case Categories must be configured before a user can add a lead to a ruleset so that the Lead Category can be selected. The **Lead Category** options are configured under **Case Category** in the **Configuration Menu**. A Lead Category is a Case Category that applies to Background Investigation case types. The Lead Category drop-down populates under 2 conditions:

1. A specific category is not associated to a draft ruleset already

2. A specific category is not associated to a published category.

If a category has already been associated to a draft ruleset or a published category, then the user would need to create new case categories to be available for selection in the **Lead Category** drop-down menu when they add Lead to a ruleset. See Case Categories for more information on how to create a Lead Category.

9.6 Add a Lead

Once a ruleset is created, the **Scoping Manager** can add leads to be scoped (investigated). Rulesets will appear in the **Ruleset List** table under **Ruleset Management** on the **Scoping Rules** page.

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the Configuration Menu drop-down, select **Scoping Rules**.

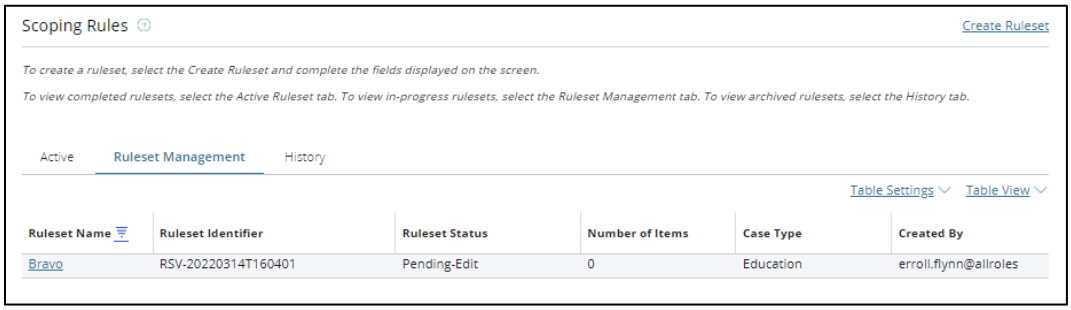


Figure 9-9: Ruleset List

4. Select the **Ruleset Name** link to open a specific ruleset.

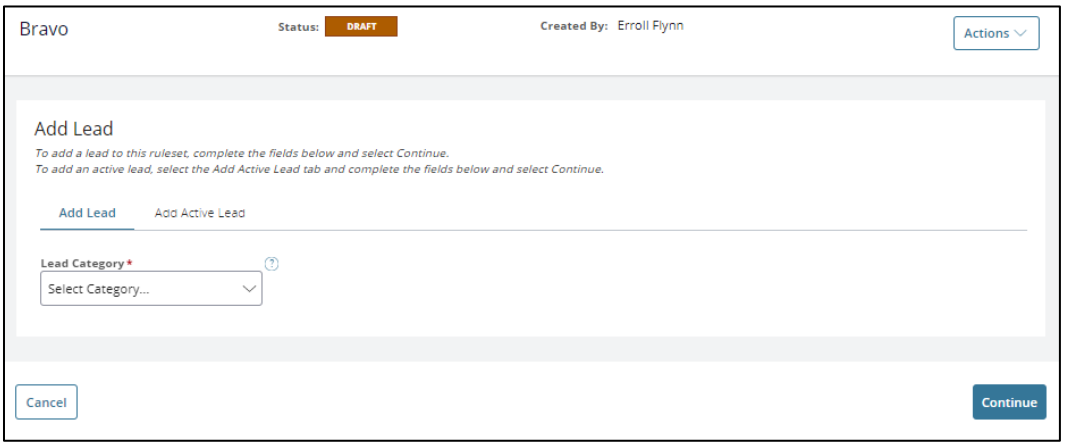


Figure 9-10: Select Lead Category

5. From the **Actions** drop-down on the Ruleset that was opened, select **Add Lead.**
6. On the Add Lead screen, from the **Lead Category** drop-down, select the **Lead Category** for the lead.

Note: The **Lead Category** options are configured under **Case Category** in the Configuration Menu. This will have to be completed separately and prior to adding a lead.

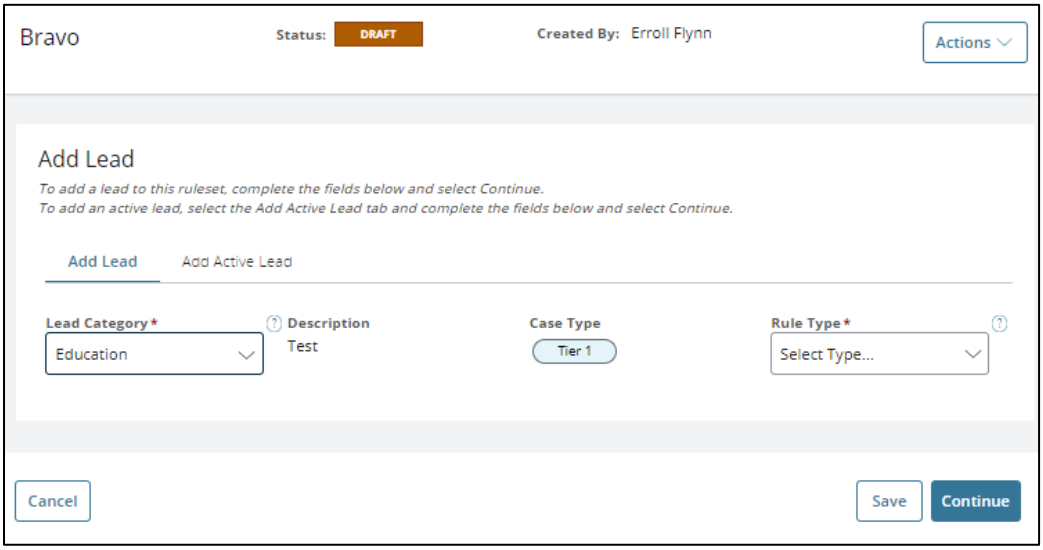


Figure 9-11: Select Rule Type

After selecting the **Lead Category**, the corresponding **Description** and **Case Type** will populate.

7. Select the **Rule Type: Base Rule** or **List Rule**. Select Base rule if the rule type is a standard rule type. Select List Rule if the rule type is one that has variations.

8. Select **Continue**. The **Lead Details Screen** will appear with options to view tabs for **Base Rules, Contextual Fields,** and **Series of Checks.**

9.7 Base Rules

A Base Rule is a standardized rule type which can be added to a lead so that the system can determine if a lead will be scoped as part of an investigation.

Once a user has added a lead and selected the **Base Rule** rule type, the **Lead Details** screen will appear.

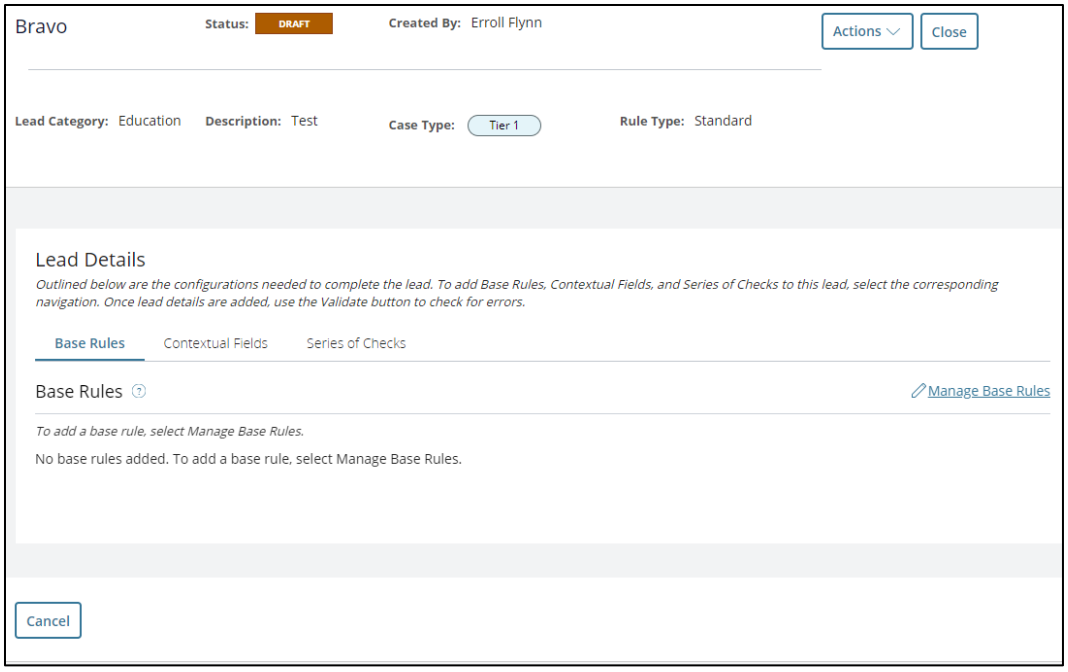


Figure 9-12: Base Rule Lead Details

9. Under **Lead Details**, on the **Base Rules** tab, select the **Manage Base Rules** link.

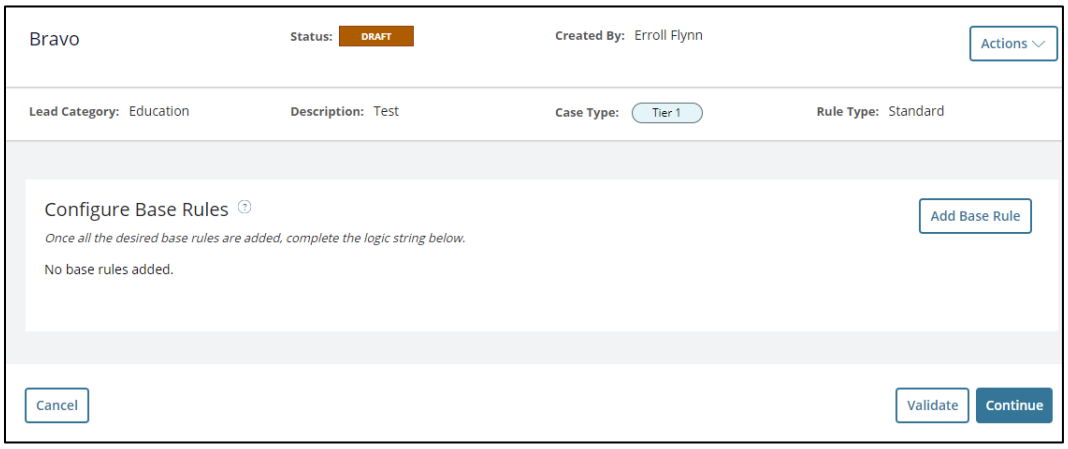


Figure 9-13: Configure Base Rules - Add Base Rule

10. On the **Configure Base Rules** screen, select **Add Base Rule**.

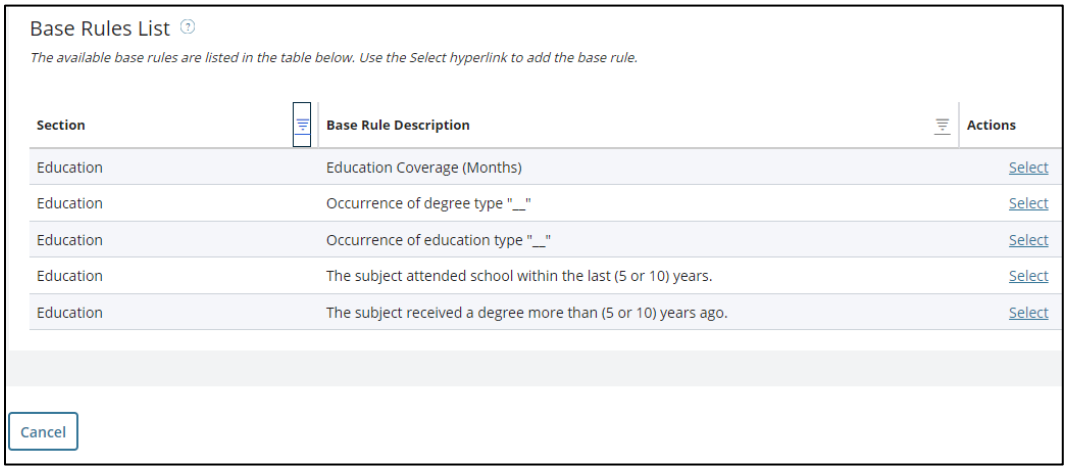


Figure 9-14: Base Rules List

Note: On the **Base Rules List** screen, use the filter on the table to filter for the desired **Section(s)**.

11. Under the **Actions** column, choose **Select** to select a specific **Base Rule**.

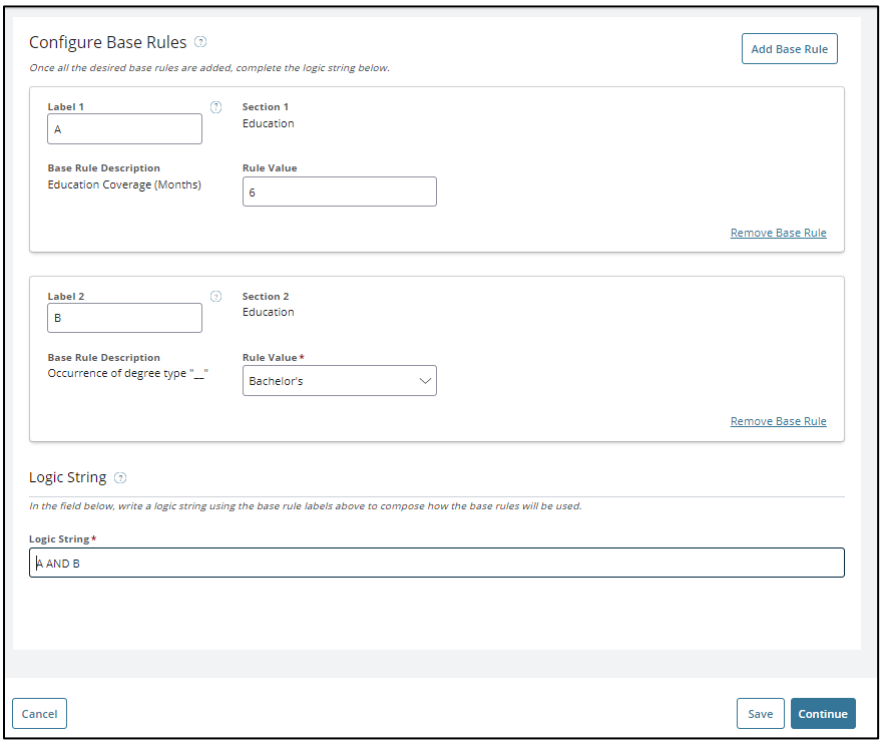


Figure 9-15: Example of Base Rules Configured

12. On the **Configure Base Rules** page, fill out **Label 1**, the **Rule Value** and **Logic String**, and then select **Save** and **Continue**.

    Note: Each Label can only be a single alpha character and must be unique from the other base rules listed on this page. Rule Value in the example shown refers to the number value of the time period referenced in the Base Rule Description. The Base Rule Description is Education Coverage (months). If the User wishes to consider 6 months of Education Coverage, the Value would be 6.

    Note: The logic string is composed of the base rules using the labels to tell the system how the rules should be used for scoping in a ruleset. It uses binary logic, parentheses to group the labels, and logical operators “AND” or “OR.” An example for the logic is: use both rule A and B for the scoping ruleset or use rule A or rule B in the scoping ruleset. To change the value or invert the logic string, “!” can also be used. (e.g., or (B and ! C)).

13. Select **Remove Base Rule** if a base rule is no longer needed. A confirmation modal will appear.

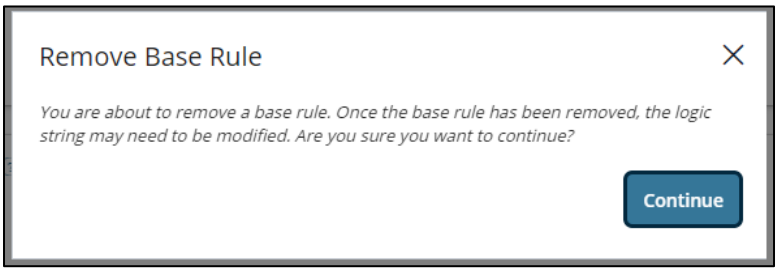


Figure 9-16: Remove Base Rule Confirmation

14. Select **Continue**.
15. When the user has finished configuring Base Rules, in the bottom right corner of the screen, select **Continue**.

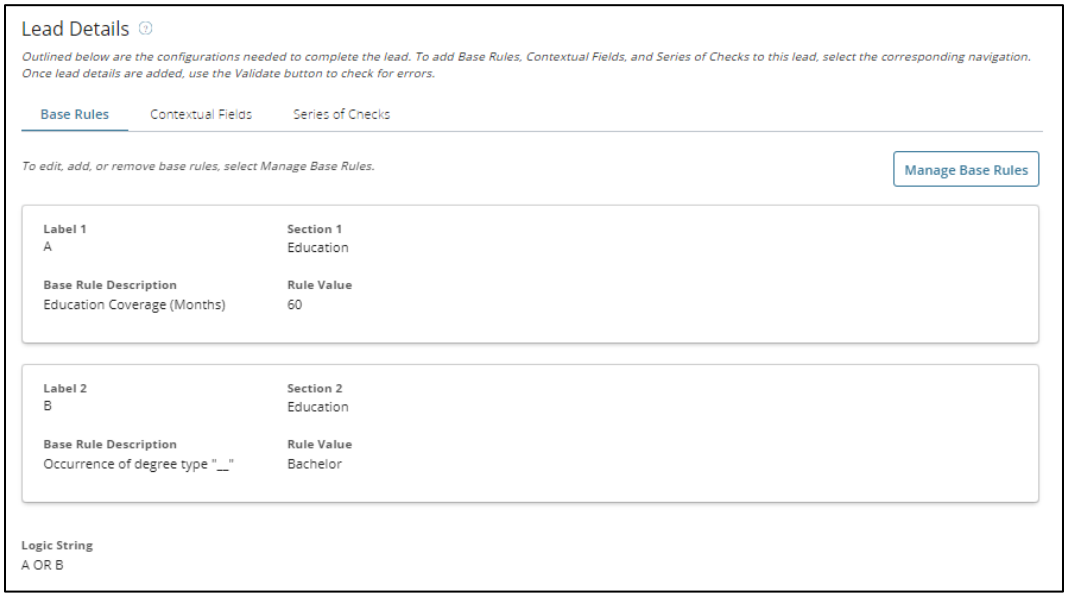


Figure 9-17: Review Base Rules

16. Select **Manage Base Rules** to make changes if needed.

Note: Now that Base Rules have been added, they populate to a page called **Lead Details**. On the **Lead Details** screen there are three tabs: **Base Rules**, **Contextual Fields**, and **Series of Checks**.

9.8 List Rules

A List Rule is a configurable rule type that is used to decide when a lead will be scoped as part of an investigation.

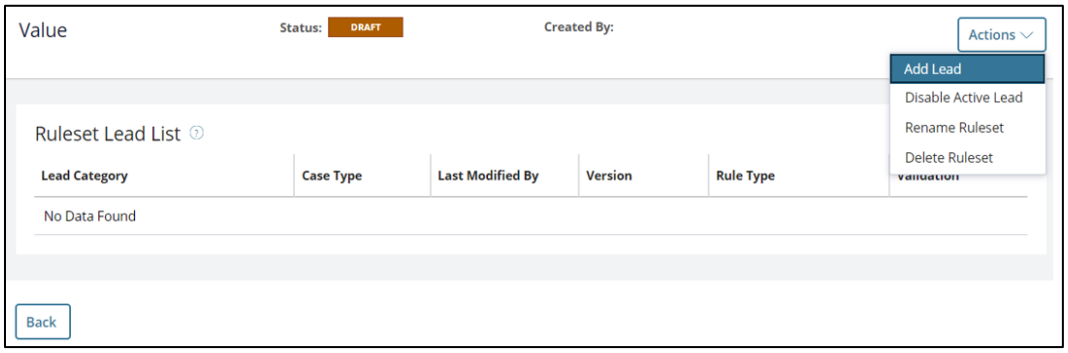


Figure 9-18: Actions - Add Lead

1. From within a ruleset, select **Add Lead**.

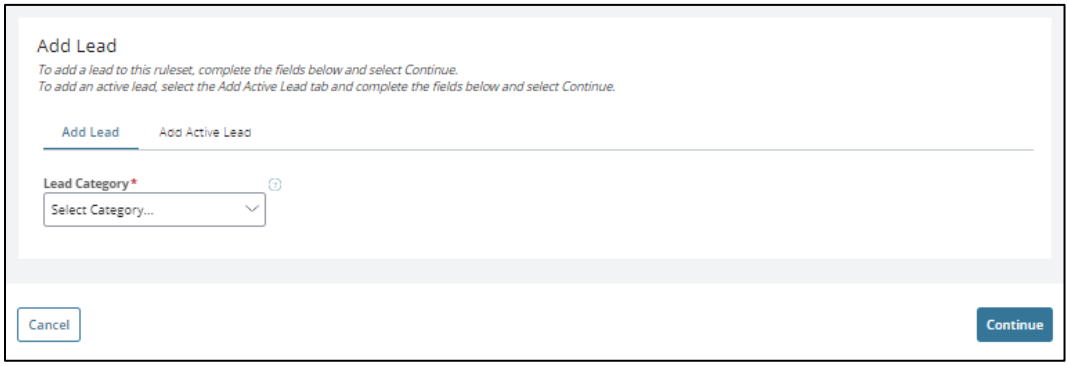


Figure 9-19: Select Lead Category

2. From the **Lead Category** drop-down, select a **Lead Category**.

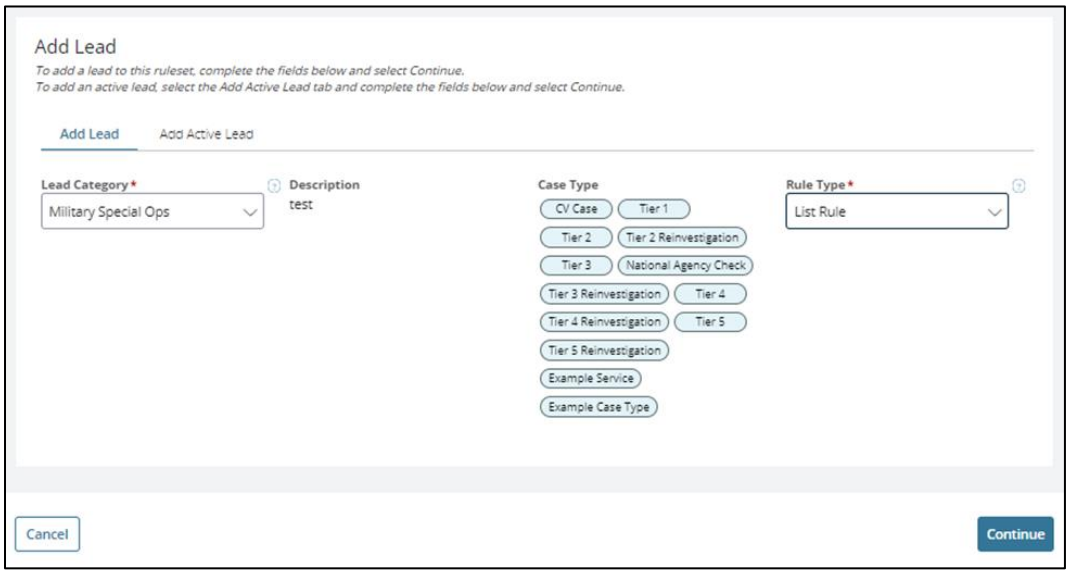


Figure 9-20: Select List Rule Rule Type

Note: Once a user has added a lead to a ruleset, the lead category **Description** and **Case Type** will populate.

3. From the **Rule Type** drop-down menu, select **List Rule**.
4. Select **Continue**.

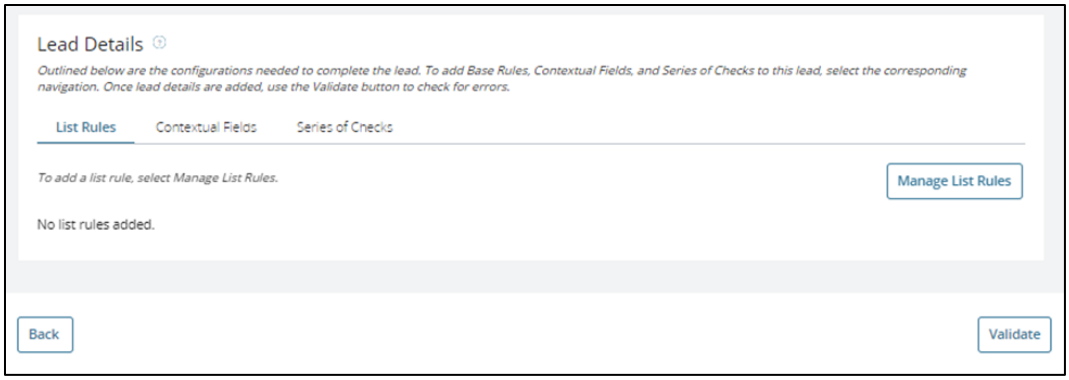


Figure 9-21: Lead Details - List Rule Tab

5. Under **Lead Details**, on the **List Rules** tab, select **Manage List Rules**.

Figure 9-22: Add List Rule

6. On the **Configure List Rules** screen, select a **Section** type from the drop-down list for the list rule to be configured. (Example: Military, Education, Address, Employment)
7. On the right side of the screen, select **Add List Rule**.

   Note: Each **Section** choice for **List Rules** will have a different set of choices on the Configure List Rules page.

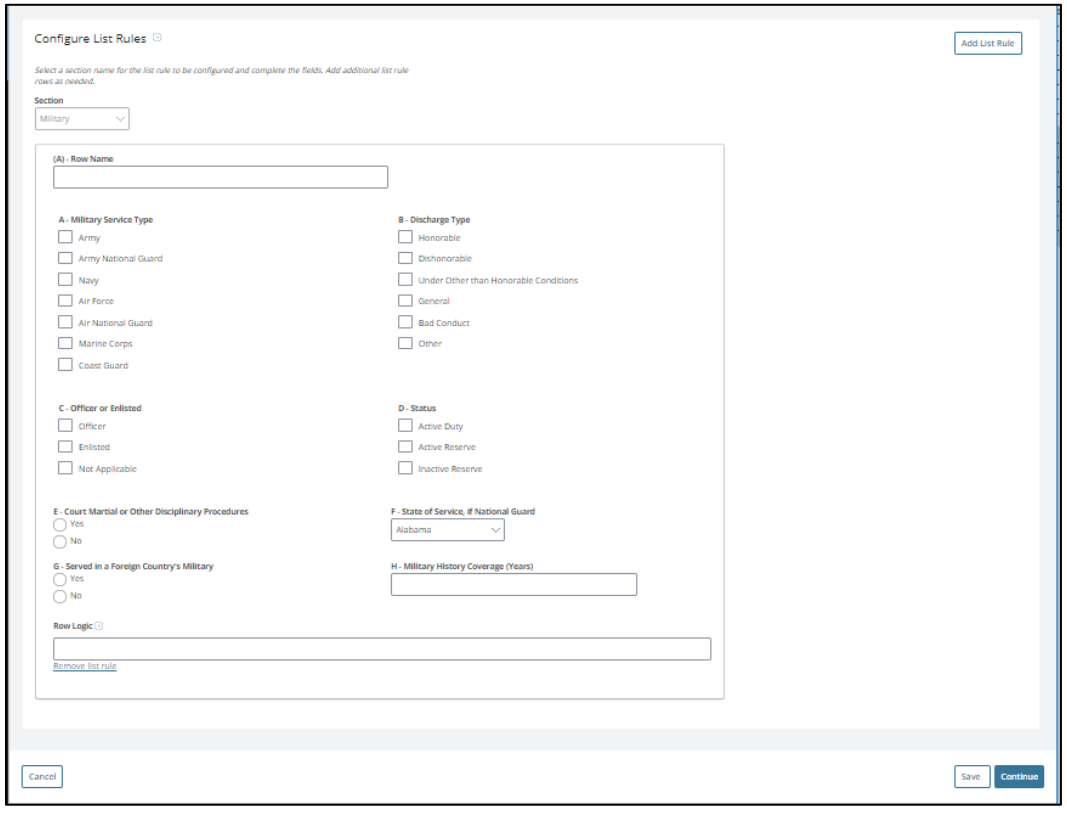


Figure 9-23: Configure List Rules - Military Example

8. On the **Configure List Rules** page, enter a **Row Name** for the **Section.**
9. Complete the section by making selections and filling in the desired fields.
10. Add **Row Logic**.

Row Logic tells the system how the rules should be used for scoping in a ruleset. It uses binary logic, parentheses to group the labels, and logical operators "AND" or "OR." An example for the logic is: use both rule A and B for the scoping ruleset or use rule A or rule B in the scoping ruleset. To change the value or invert the logic string, "!" can also be used. (e.g., or (B and ! C)). For example, enter 'A and B and C' if those are the only sections to be considered in system logic'.

11. Select **Continue**.

The **Row Name** and configuration for that row should display in a card on a new screen.

Figure 9-24: Review Read Only View of List Rule Configuration

12. Select **Continue**.

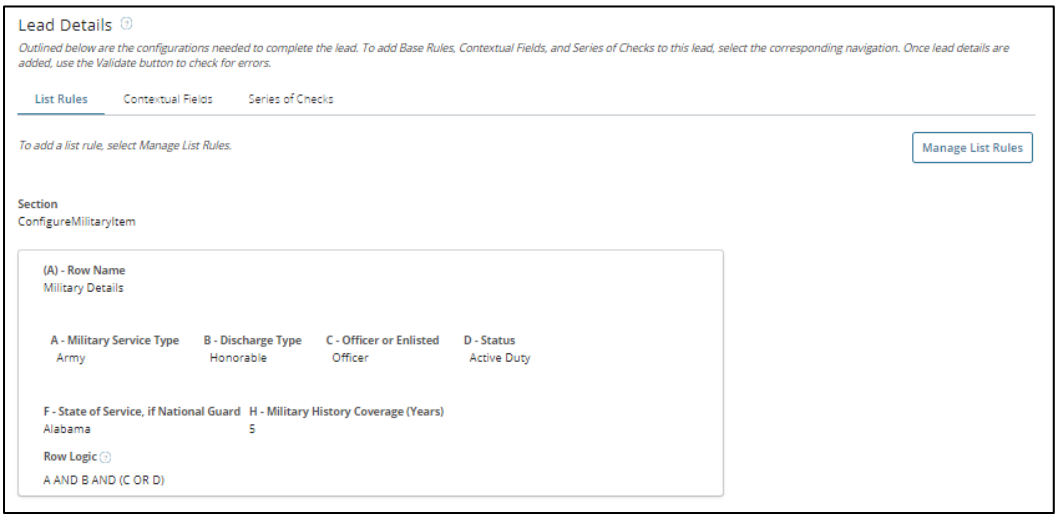


Figure 9-25: Lead Details - List Rule Tab with One List Rule Example

13. To add additional list rules or to make changes to a list rule, select **Manage List Rules.**

    Note: Select **Save** at any time to save your entries.

14. If you have more than one list rule, enter the **Scoping Logic String** and then select **Continue**.

    Note: Scoping logic is the overall logic for the lead referencing the results of the individual rows. This logic will use the true/false outcome of each individual row to determine if the lead as a whole should scope or not.

After configuring List Rules, complete **Contextual Fields** and **Series of Checks**, followed by **Validate** Ruleset. See Table of Contents for more information on those topics.

9.9 Contextual Fields

Within a Lead for a Ruleset, the Contextual Fields Tab is where contextual fields can be chosen to view specific data points from the subject's standard form. For example, the subject's SF-86.

1. Within the **Lead Details** screen, select the **Contextual Fields** tab and select **Manage Contextual Fields**.

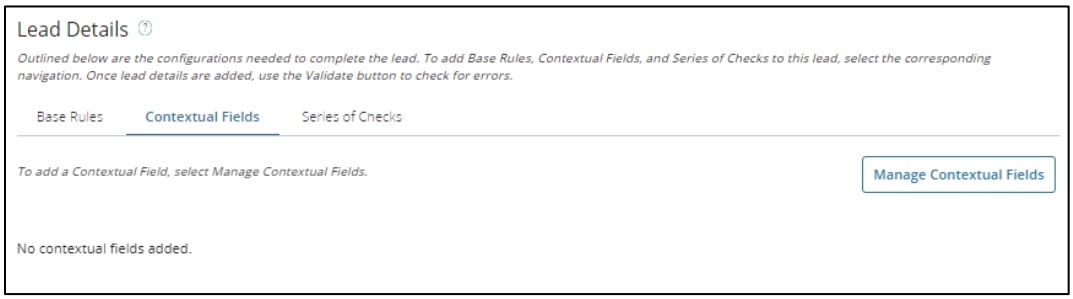


Figure 9-26: Contextual Fields Tab - Manage Contextual Fields

2. Within the **Configure Contextual Fields** screen, select **Add Section**.

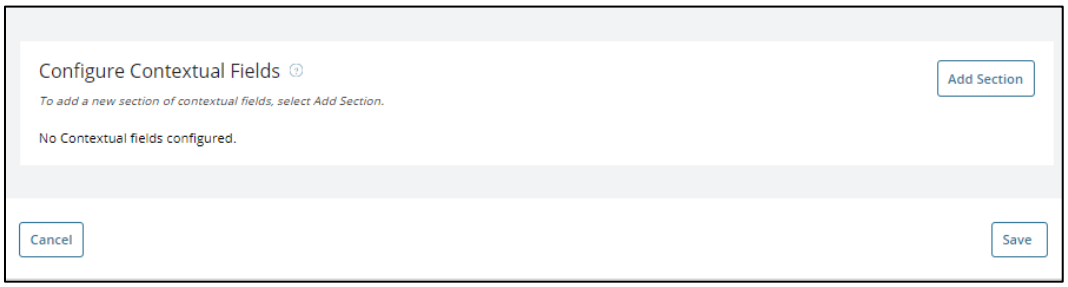


Figure 9-27: Configure Contextual Fields - Add Section

3. When the section appears, enter a name under **Section Name**. For example, Relatives-Mother.

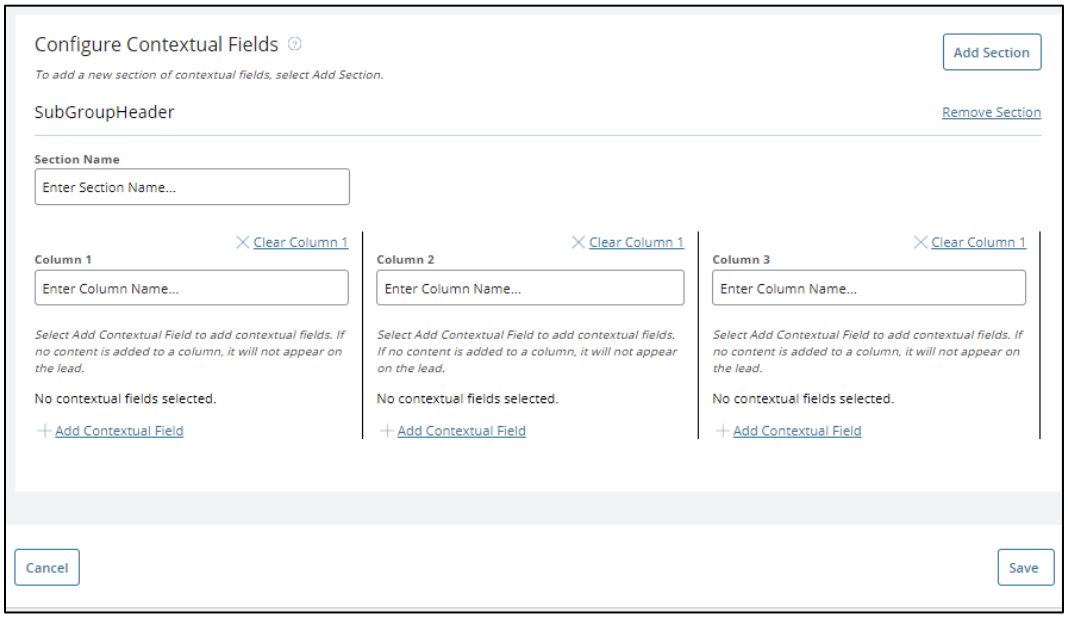


Figure 9-28: Configure Contextual Fields - Add Columns

4. Enter a name under **Column 1**, **Column 2**, and **Column 3** if needed. For example, 18.1 – Identification.
5. Under the column name, select **Add Contextual Field**.

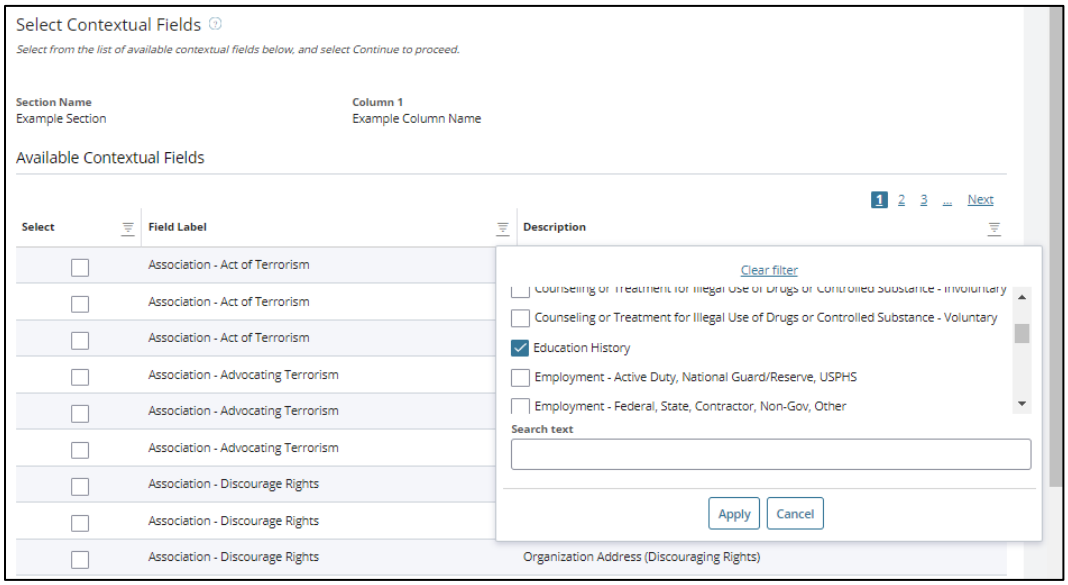


Figure 9-29: Apply Filter Options to Select Contextual Fields

6. In the **Select Contextual Fields** screen, use the filter option to locate and check the box for areas of interest and then select **Apply**. For example, Education History, List of Degrees.

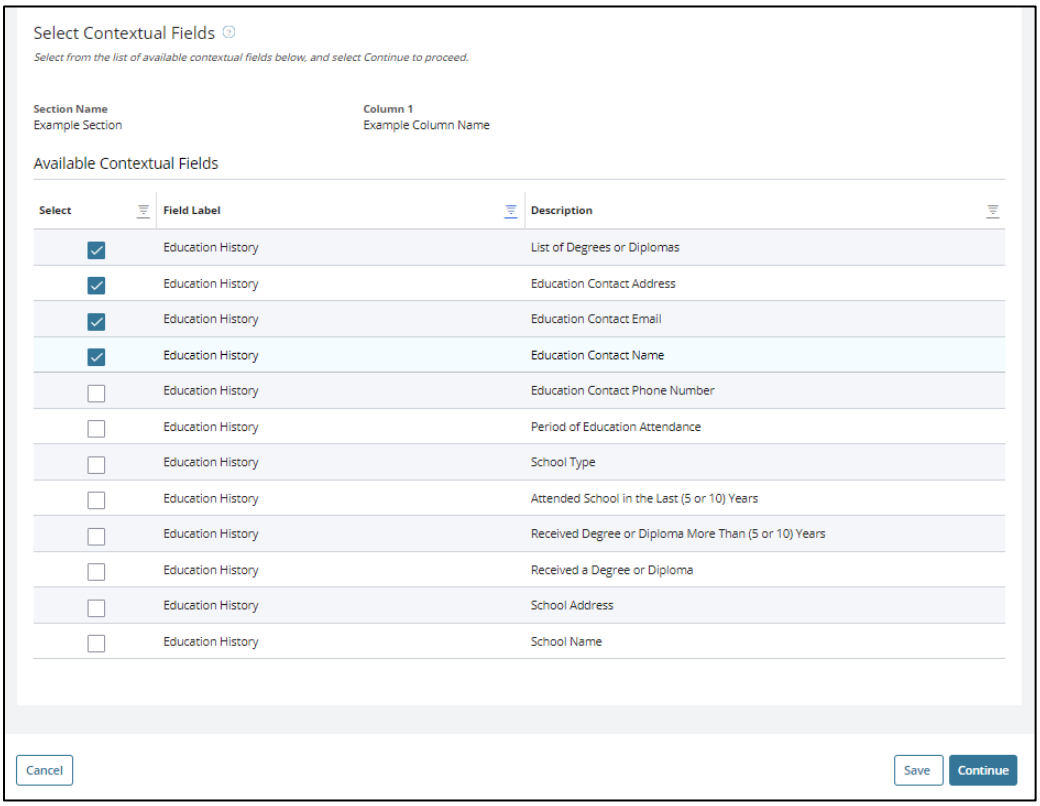


Figure 9-30: Select Available Contextual Fields

7. In the Select Contextual Fields screen, select the **checkboxes** corresponding to the applicable Field labels and Descriptions.
8. Select **Save** and **Continue**.

The Configured Contextual Fields screen will appear with the added contextual fields.

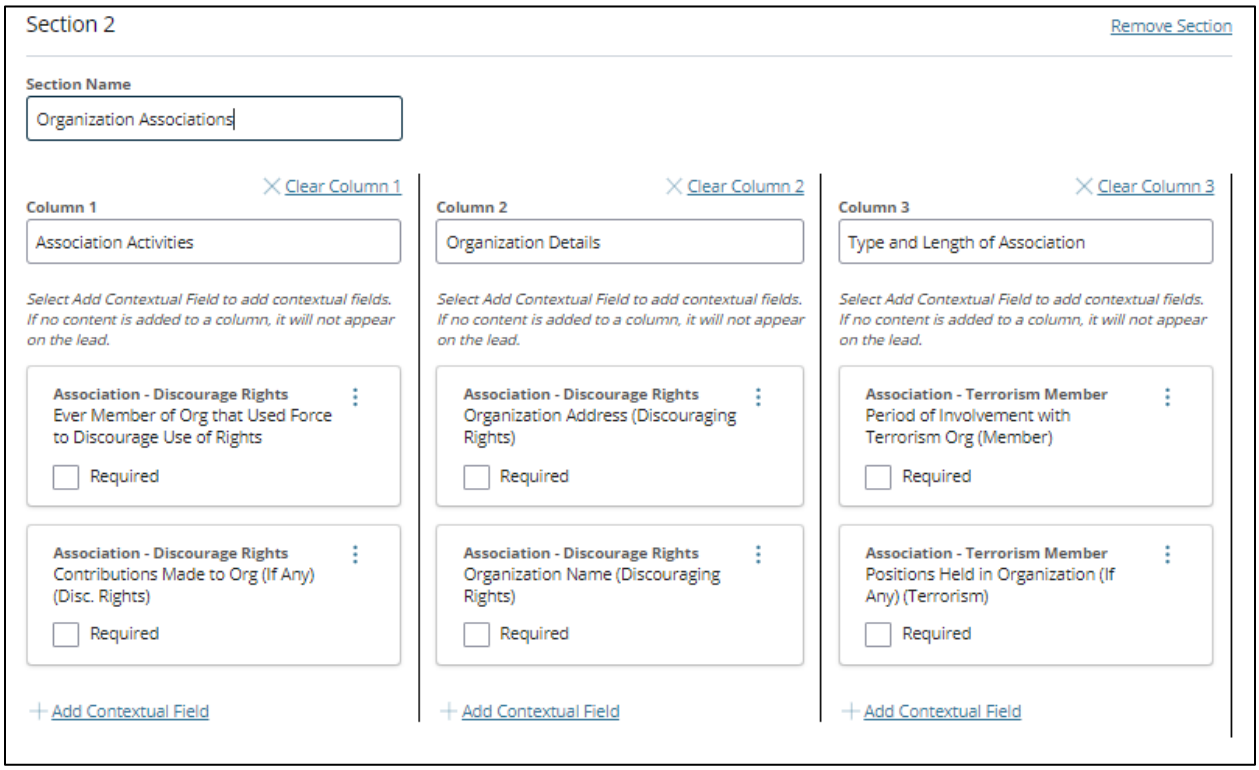


Figure 9-31: Example of Selected Contextual Fields

9. Select the **checkbox** on a Contextual Field to indicate that information for this field is required.
10. Select the **Ellipsis** on the Contextual Fields to access options to **Move Up, Move Down,** or **Remove.**
11. Select **Save** and **Continue** at the bottom of the screen when selections are complete.

Note: Other options on the Contextual Fields screen include **Add Section** to add another section of contextual fields, **Remove Section** to remove a section of contextual fields, and **Clear Column** to clear contextual fields that were selected in a particular column.

9.9.1 MANDATORY FIELDS TO ADD FROM A DATA SOURCE

A Scoping Manager with access to configure leads in Scoping Rules will need to add the mandatory contextual fields that are required if they have chosen a data source in the method of fulfillment in Series of Checks. Investigation Data Sources are configured by a System Manager in System Settings under Investigation Configurations – Manage Data Sources. See the **NBIS Admin Guide** for more information on configuring Investigation data sources.

When a Scoping Manager configures the series of checks on a lead in scoping rules, they are able to include both required and optional data source fields for a given data source to make them available to investigators.

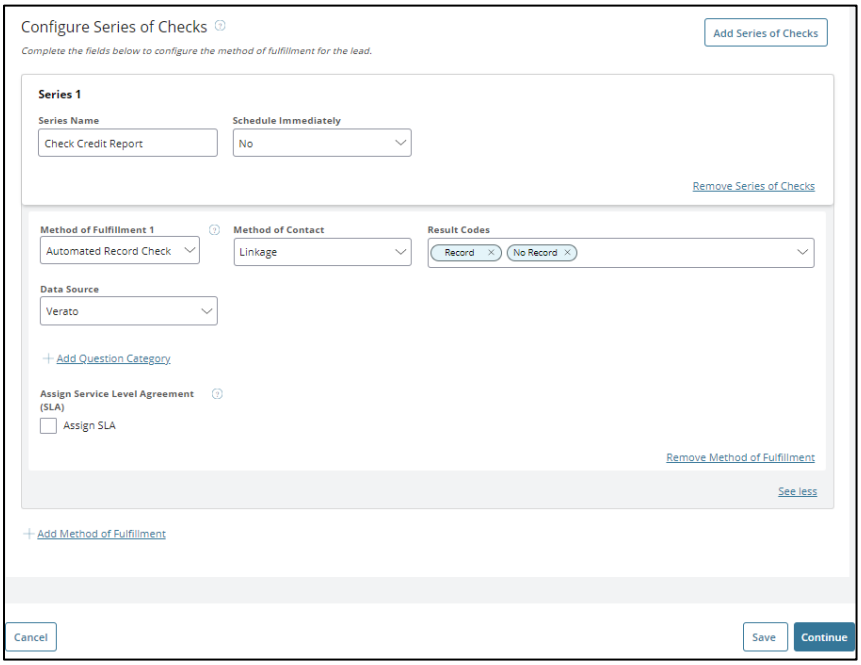


Figure 9-32: Data Source Selected under Method of Fulfillment in a Series of Checks

1. From within a Series of Checks, under Method of Fulfillment, select **Automated Record Check.**
2. Under **Data Source**, select a data source.

   Note: Data Sources for Investigations are configured by a System Manager in System Settings under Investigation Configurations – Manage Data Sources. See the **NBIS Admin Guide** for more information on configuring investigation data sources.
3. Under **Data Source**, select a data source.
4. When complete select **Save** and **Continue**.

For more instructions to configure a series of checks, see Series of Checks.

5. Select the **Contextual Fields** tab.

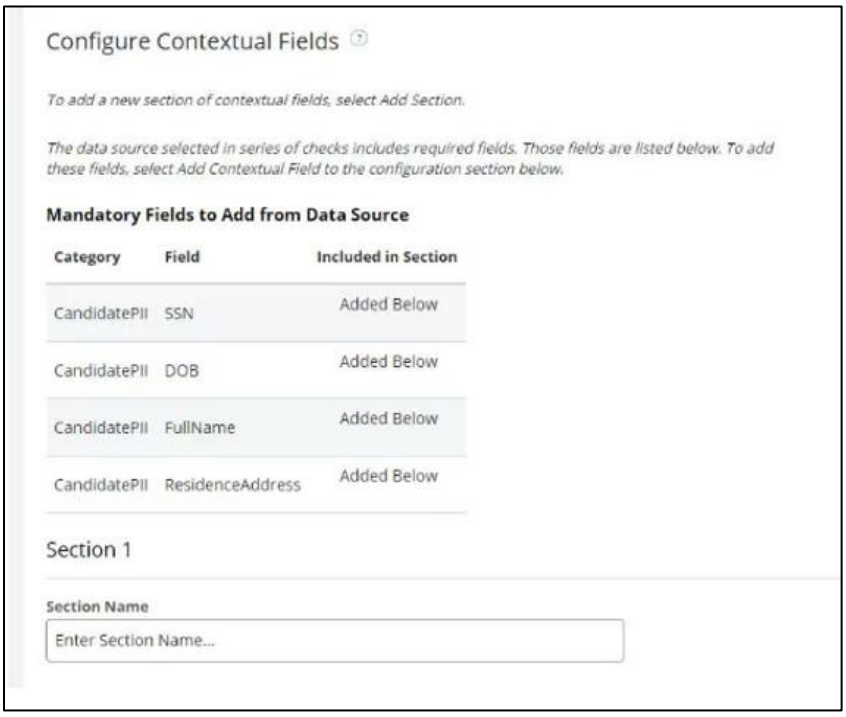


Figure 9-33: Contextual Fields Tab – Mandatory Fields to Add from Data Source

If the data source selected under Method of Fulfillment has mandatory fields, there will be a table showing the Category, Field, and whether the field has been included in the section. The fields in this table need to be configured as contextual fields in order for the ruleset to pass validation.

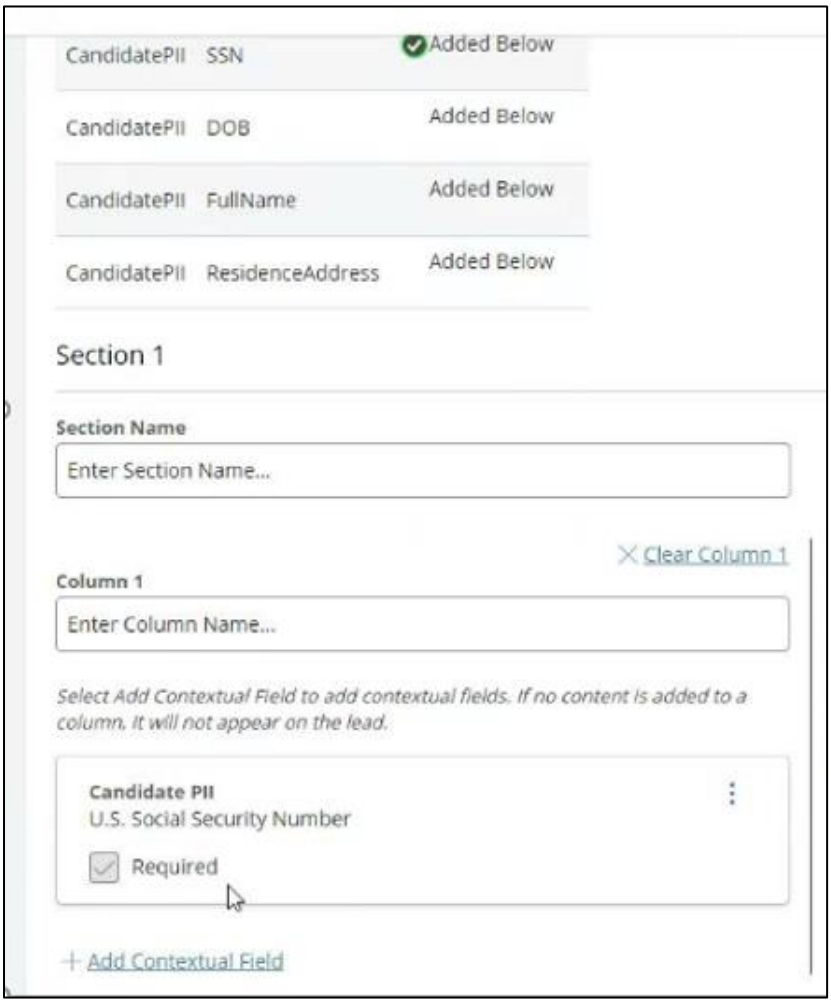


Figure 9-34: Contextual Fields Tab – Mandatory Fields to Add from Data Source

When the user has added a mandatory contextual field, there will be a check mark in a green circle to indicate that the field has been added in the section below. Under the section, the user then has the option to mark the mandatory field **Required**. The user can also add additional optional contextual fields as needed. The user is able to continue configurations without adding all of the mandatory fields, however, the lead would not pass validation until all mandatory fields for the data source have been added.

For more instructions to configure Contextual Fields, see Contextual Fields.

9.10 Series of Checks

The **Series of Checks** tab provides a way to configure a series of checks and schedule methods of fulfillment for the checks within a Lead for a Ruleset.

1. In the **Lead Details** screen, select the **Series of Checks** tab.

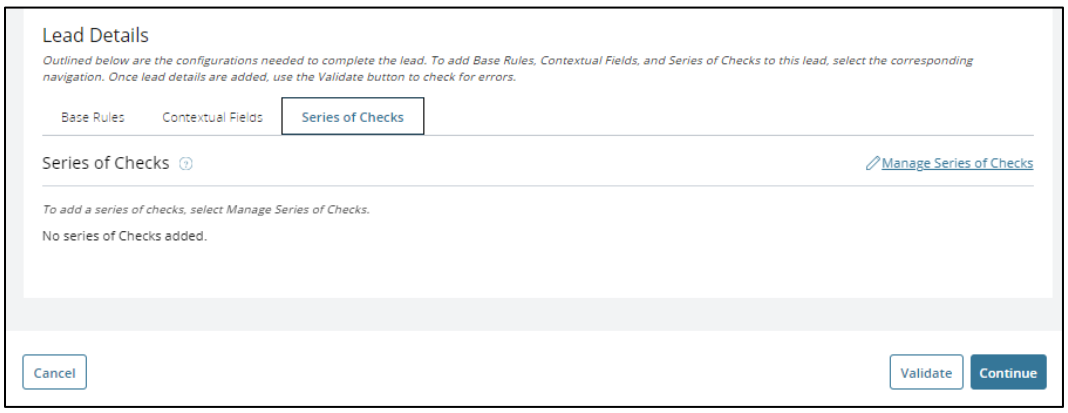


Figure 9-35: Series of Checks Tab – Manager Series of Checks

2. Select **Manage Series of Checks**.

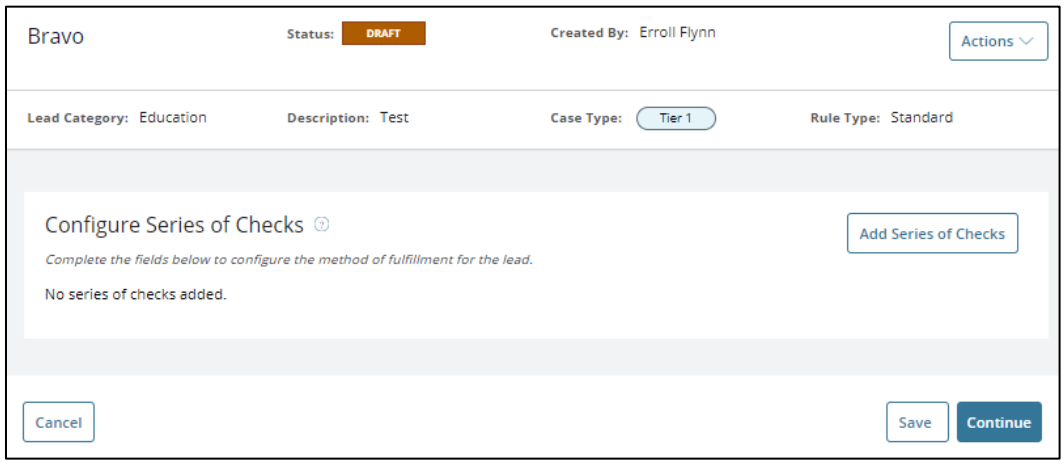


Figure 9-36: Add Series of Checks

3. In the **Configure Series of Checks** screen, select **Add Series of Checks**.

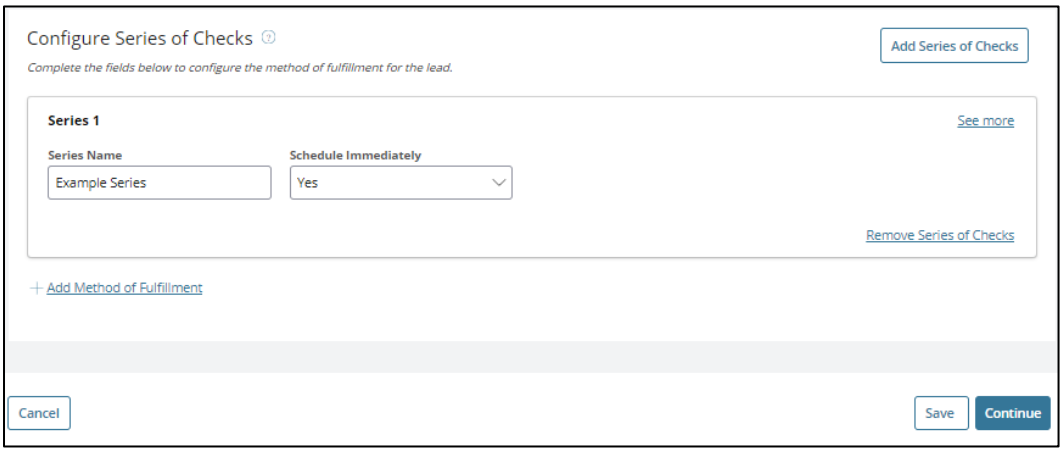


Figure 9-37: Configure Series of Checks - Series 1

4. Enter a name for the series under **Series Name**.
5. Under **Schedule Immediately**, select **Yes** or **No**.
6. Select **Add Method of Fulfillment**.

Note: Select **Remove Series of Checks** if this series is no longer needed, then the entry will disappear.

7. After selecting **Add Method of Fulfillment**, choose **See More** in the upper right corner of the series section to expand the section and see the **Method of Fulfillment** section.

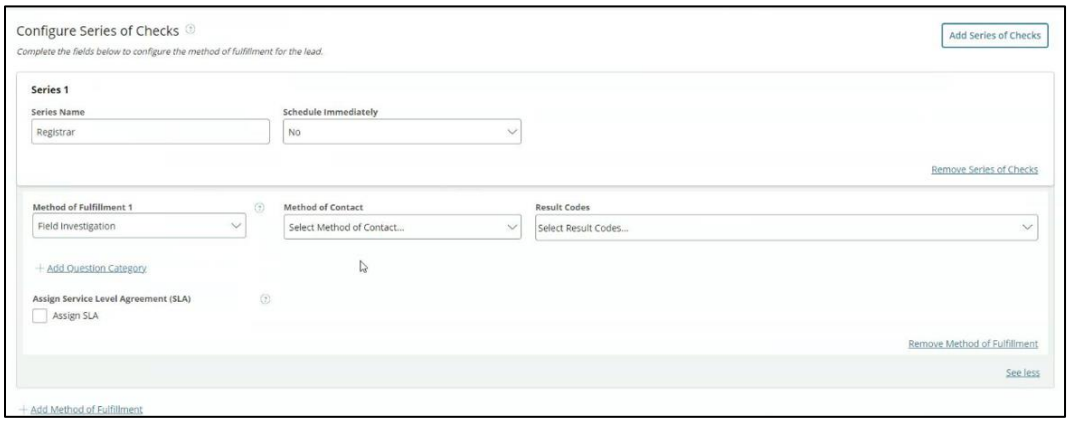


Figure 9-38: Method of Fulfillment Section

8. In the **Method of Fulfillment** section, from the drop-down, select a **method of fulfillment**.
9. Select **Method of Contact**.

   Note: Contact Method options are populated by the Manage Contact Method Options table in System Settings. See the **NBIS Admin Guide** for more information.

10. Select **Result Codes.**

    Note: If a at least one method of contact and at least one result code are not chosen, the lead will fail validation.

    Note: Result Code options are populated by the Manage Result Codes table in System Settings. See the **NBIS Admin Guide** for more information.

11. If needed, select **Add Question Category**.

Figure 9-39: Add Question Category

12. Select **Question Set Category 1** and **Question Set 1**.
13. Select **Add Question Set** again if additional question sets are needed.

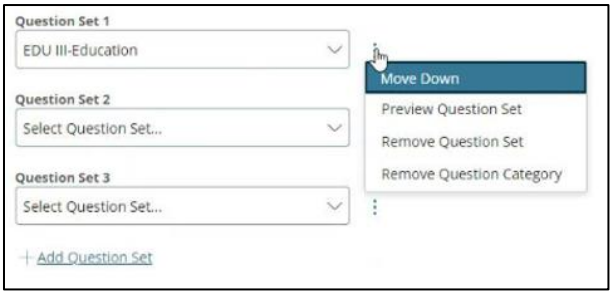


Figure 9-40: Question Set Ellipsis Menu Options

Note: If a Question Category is selected, then a question set must also be selected, or the lead will fail validation. If a Question Category is not selected, a question set does not need to be selected.

Note: The Question Categories and Question Sets that populate these drop-downs are preconfigured at this time.

14. Use the **ellipses menu to reorder** question sets, Preview Question Set or Remove Question Category.
15. Select the **Assign SLA checkbox** if needed.

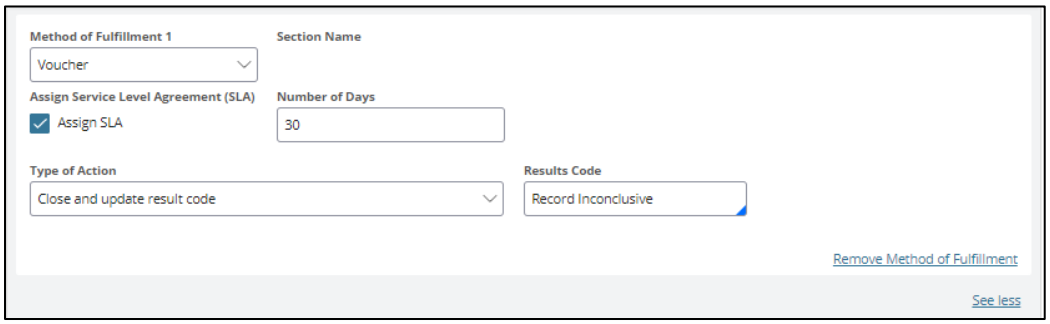


Figure 9-41: Method of Fulfillment – Assign SLA

16. If Assign SLA is checked, then, under **Number of Days**, enter the number of days at which the SLA should take effect.
17. Under **Type of Action**, select the **type of action** to occur when the SLA takes effect.
18. When finished, select **Save** and **Continue**.
19. To make changes, select **Manage Series of Checks** and repeat the process.

9.11 Add an Active Lead

A user can choose to **Add an Active Lead** if active leads have been created and are available. An active lead is a lead that has been published and is not currently being used in another ruleset.

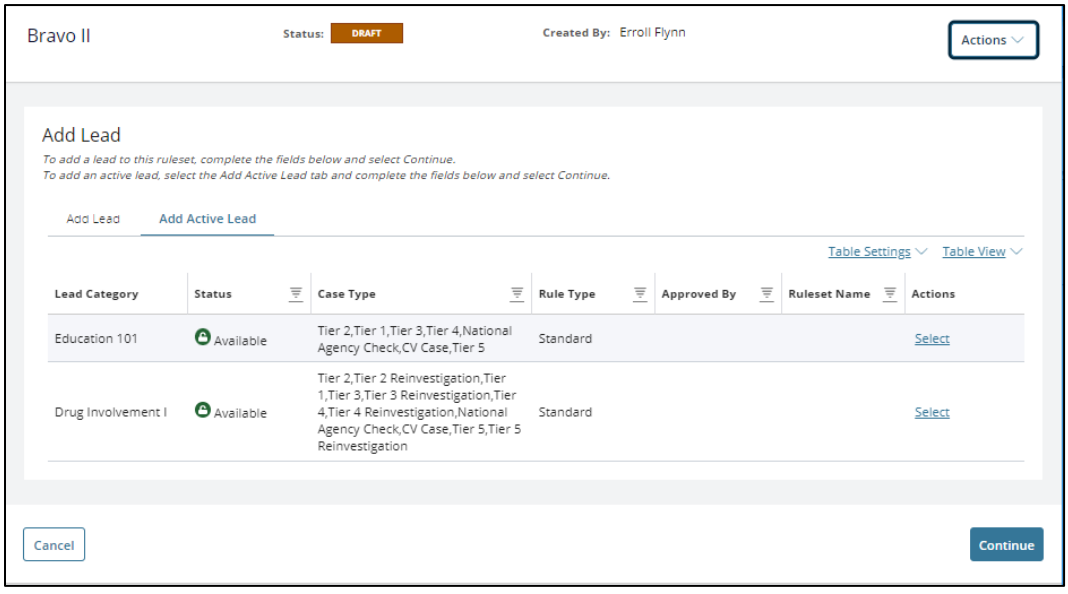


Figure 9-42: Add an Active Lead

1. Within a **Draft** ruleset, from the **Actions** drop-down menu, select **Add Lead**.
2. On the Add Lead screen, select the **Add Active Lead** tab.

3. On the Active Lead table, locate an Active Lead that has been created that can be used for your ruleset and choose **Select** under the **Actions** column to add the lead to your ruleset.
4. Select **Continue**.

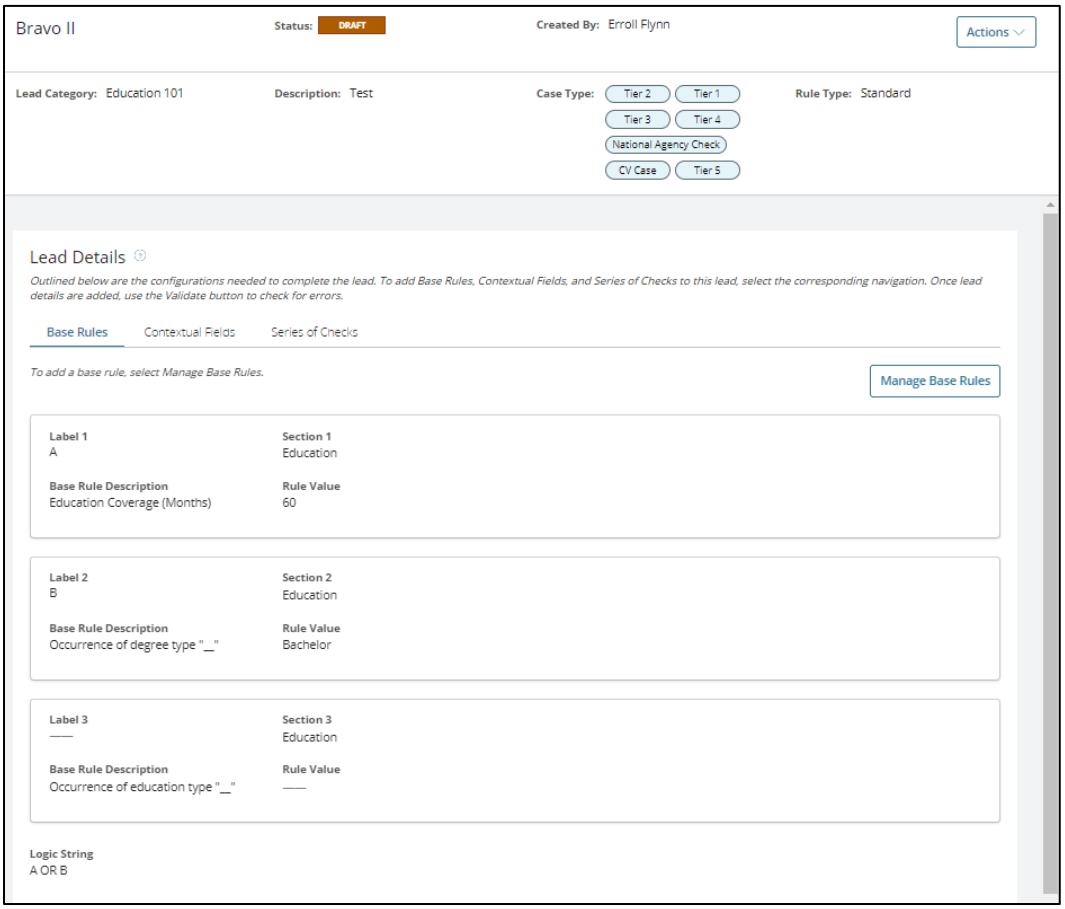


Figure 9-43: Active Lead Added to Draft Ruleset

Note: To edit the lead, select **Manage Base Rules** and follow the directions for managing base rules.

9.12 Edit Lead Details

1. To edit the details of an existing lead, select the **Ruleset Name** in **Ruleset Management**.
2. On the Ruleset Lead List, select the **Lead Category name**.

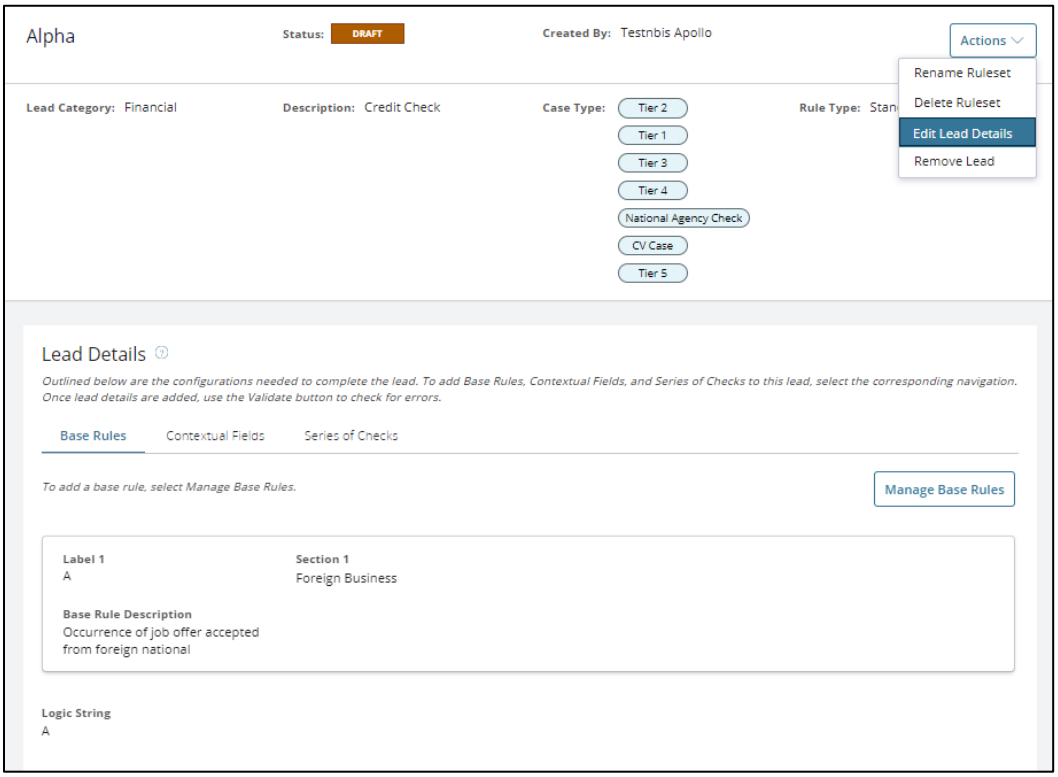


Figure 9-44: Edit Lead Details

3. Within the Lead, in the Actions drop-down menu, select **Edit Lead Details**.
4. After completing any changes, select **Cancel** or **Continue**.

9.13 Remove a Lead

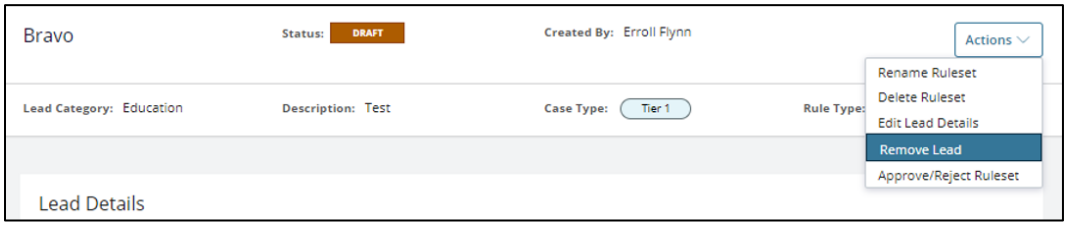


Figure 9-45: Actions Menu - Remove Lead

1. To remove an existing lead, from the **Actions** drop-down menu, select **Remove Lead**.

9.14 Validate a Lead

A Scoping Manager can validate a lead to determine if there are any errors that need to be corrected.

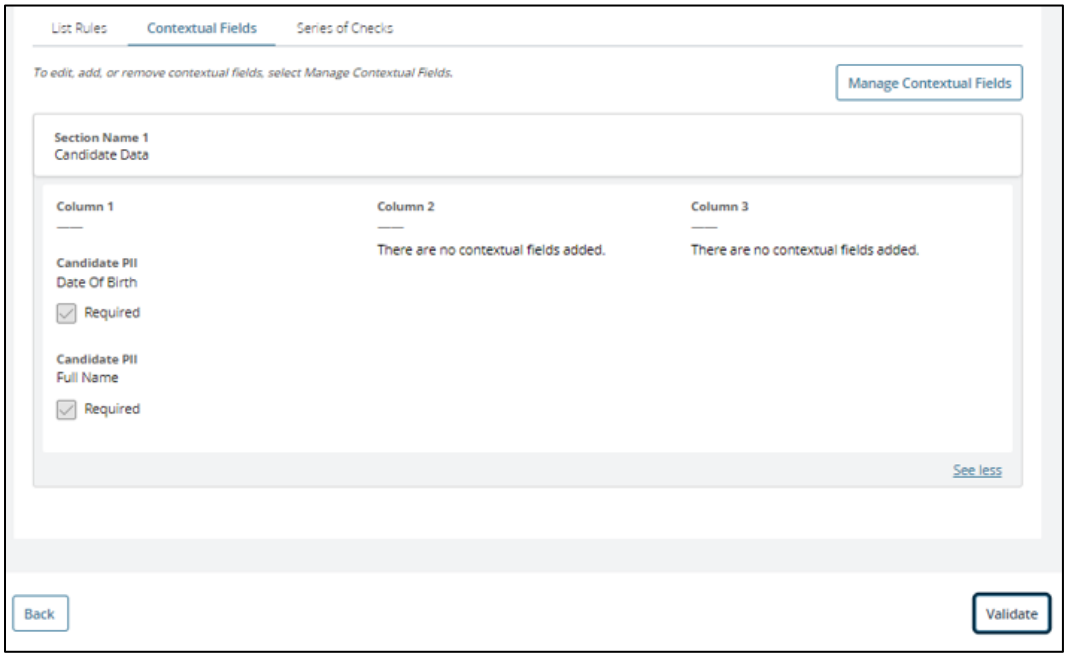


Figure 9-xx: Validate Lead

1. From within a lead, in lower right corner, select **Validate**.

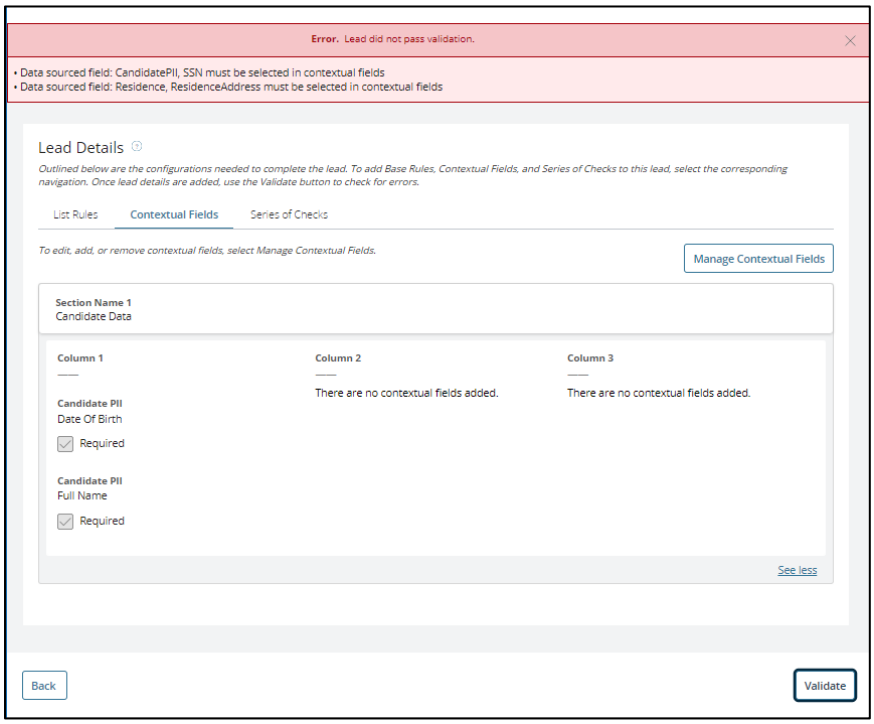


Figure 9-xx: Lead Validation Banner Error Message

If errors are found, details of the errors will be displayed in the error banner message.

2. Locate and correct the errors.
3. Select the **Validate** again.

9.15 Rename Ruleset

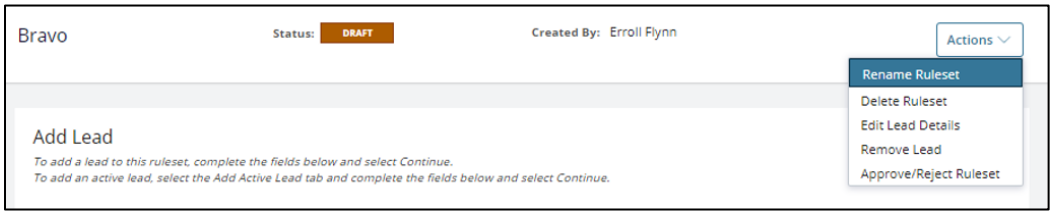


Figure 9-46: Actions Menu - Rename Ruleset

1. To rename an existing ruleset, from the **Actions** drop-down menu, select **Rename Ruleset**.

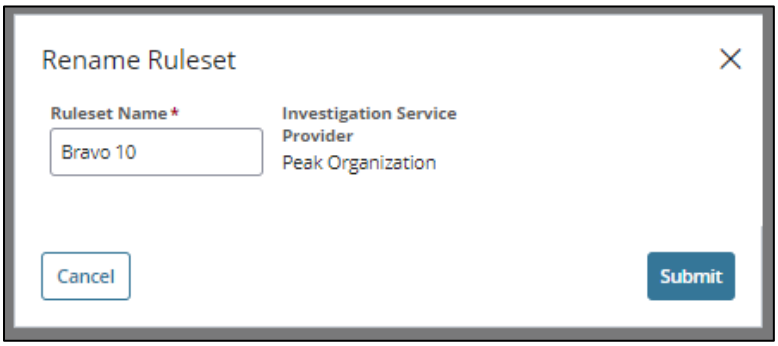


Figure 9-47: Rename Ruleset Screen

2. In the **Rename Ruleset** window, enter the new name and select **Submit**.

9.16 Delete Ruleset

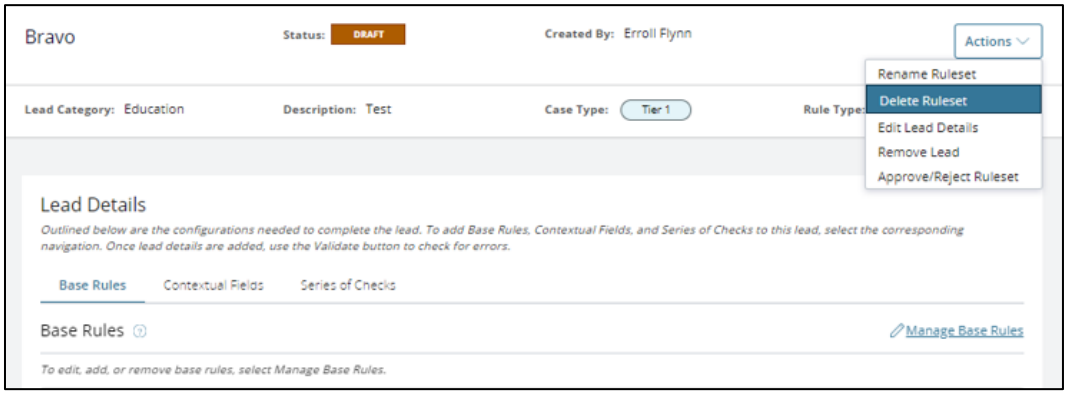


Figure 9-48: Actions Menu - Delete Ruleset

1. To delete a ruleset, from the **Actions** drop-down menu, select **Delete Ruleset**.
2. Verify that the ruleset no longer appears in the **Ruleset List**.

9.17 Submit Ruleset

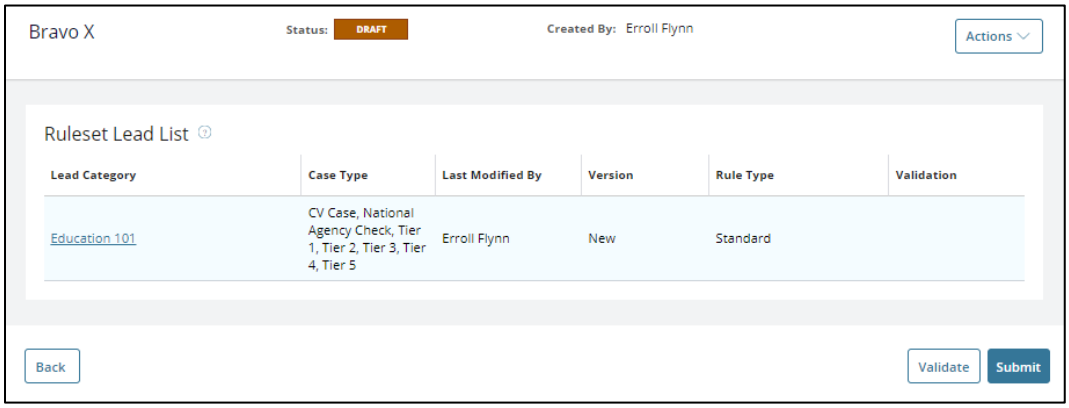


Figure 9-49: Review Ruleset Lead List and Submit

3. From the Ruleset Management tab, select a **Ruleset Name**.
4. Review the **Ruleset Lead List.**
5. When complete, select **Submit**.

Figure 9-50: Submit Ruleset Confirmation

6. On the confirmation screen, read the text and select **Continue** to confirm the Ruleset Submission.

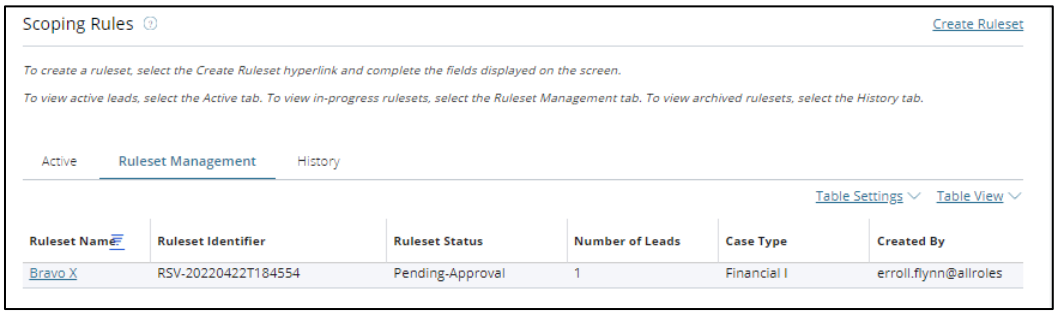


Figure 9-51: Ruleset Status - Pending Approval

7. On the Ruleset Management tab, see that the ruleset status has changed to Pending Approval.

9.18 Validate Ruleset

A Scoping Manager can validate a ruleset to determine if there are any errors that need to be corrected prior to publishing the ruleset.

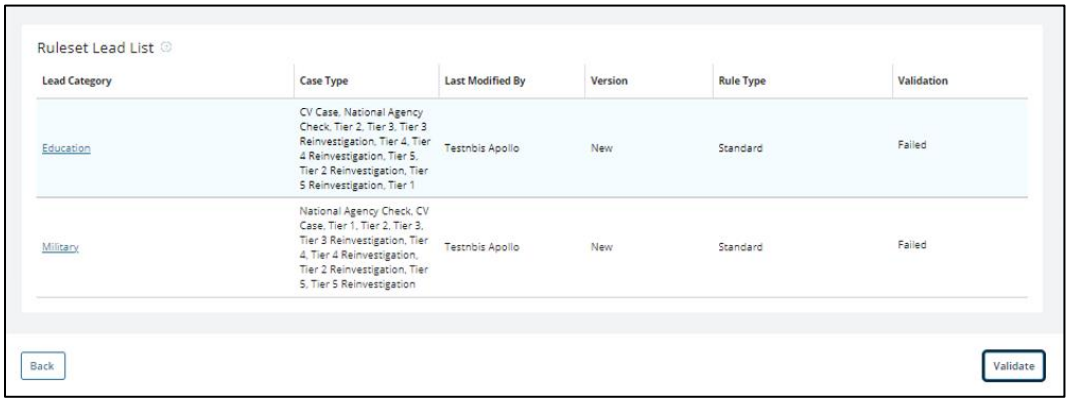


Figure 9-52: Validate Ruleset Lead List

1. From within a ruleset and after leads have been added, to the right under the ruleset lead list, select **Validate**.

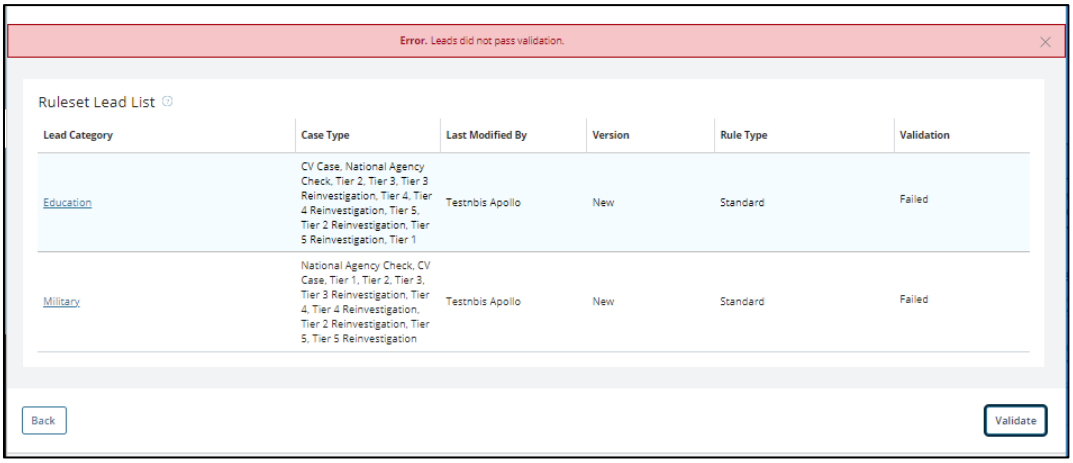


Figure 9-53: Ruleset Lead List with Validation Error Banner

If errors are detected, there will be a red error banner above the ruleset lead list, and in the Ruleset Lead List table, under the Validation column, the word 'Failed' will appear for Leads that did not pass validation.

2. From the **Lead Category** column, select a **Lead Category** that shows 'Failed' to view the specific errors for that lead.

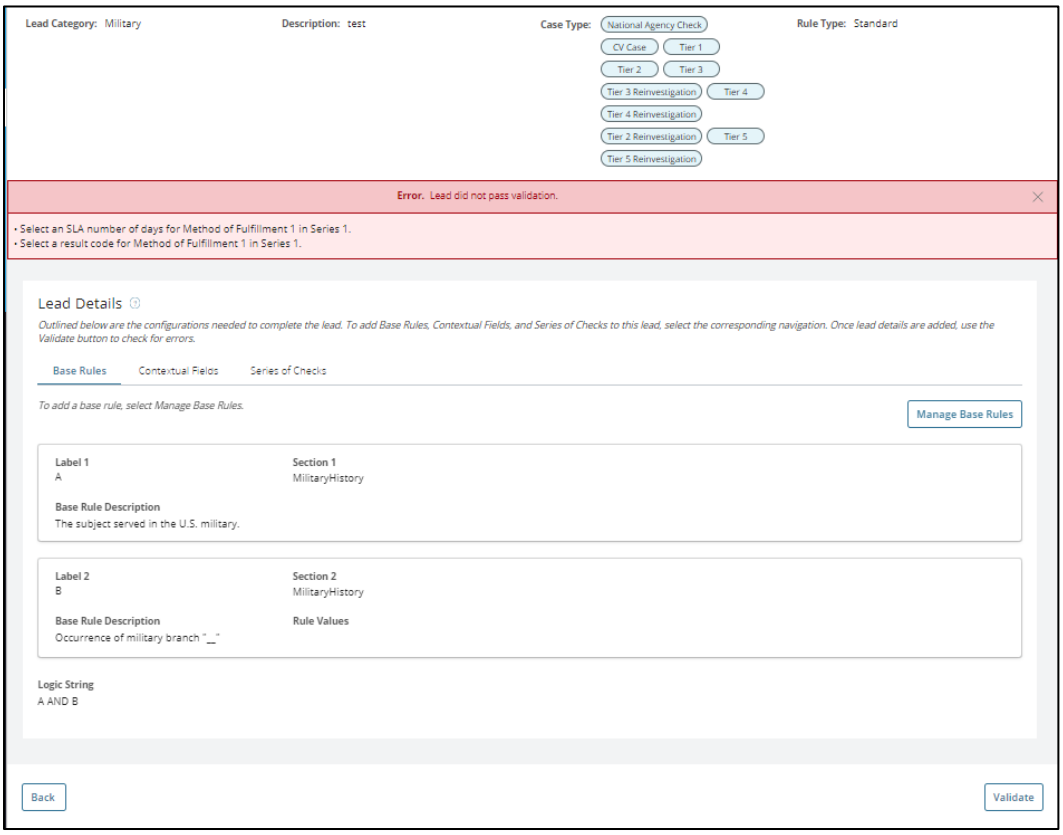


Figure 9-54: Lead Details Screen with Error Banner and Error List

Within the Lead Details screen, a red error banner will show that the lead did not pass validation and will list the specific errors.

3. Locate and correct the errors, and then select **Validate**.

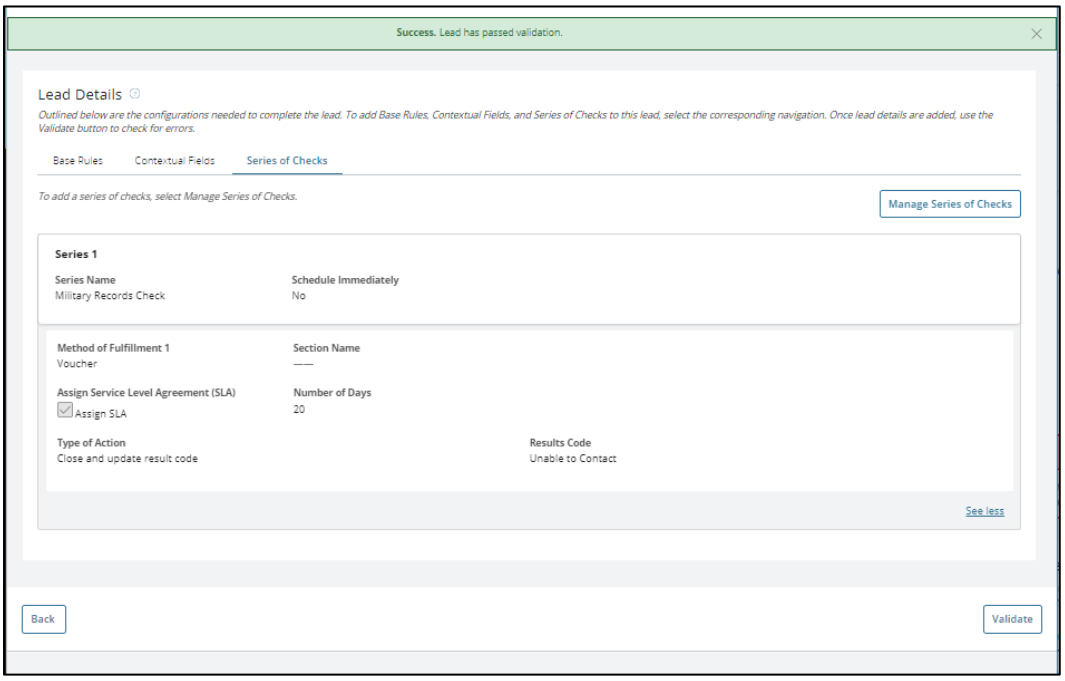


Figure 9-55: Lead Details Screen with Success Banner for Validation

If the lead passes validation, a green success banner will be shown above Lead Details.

4. Select the Back button, to return to the Ruleset Lead List.

When a lead has passed validation, the word 'Passed' will be shown in the Validation column for that lead.

9.19 Approve/Reject Ruleset

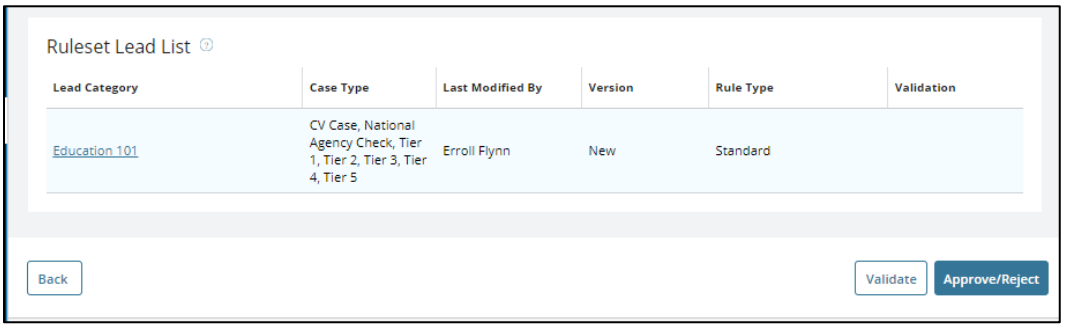


Figure 9-56: Ruleset Lead List - Approve/Reject Ruleset

1. To Approve or Reject a ruleset, open the ruleset from the **Ruleset Management** tab and then select **Approve/Reject Ruleset**.

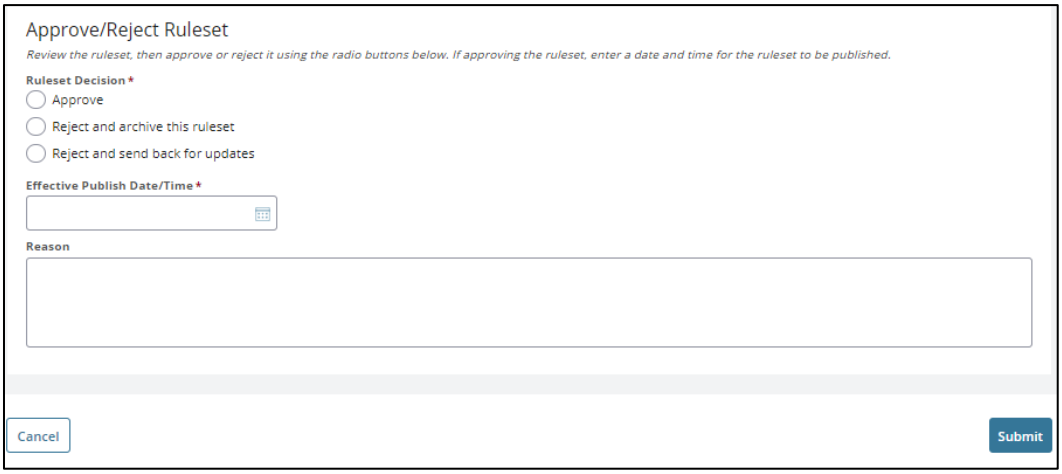


Figure 9-57: Approve/Reject Ruleset Screen

2. In the Approve/Reject Ruleset screen, choose one of the available options to approve or reject and enter details in the associated fields.
3. Select an **Effective Publish Date/Time**.
4. Optionally enter a **Reason**.
5. Select **Submit**.

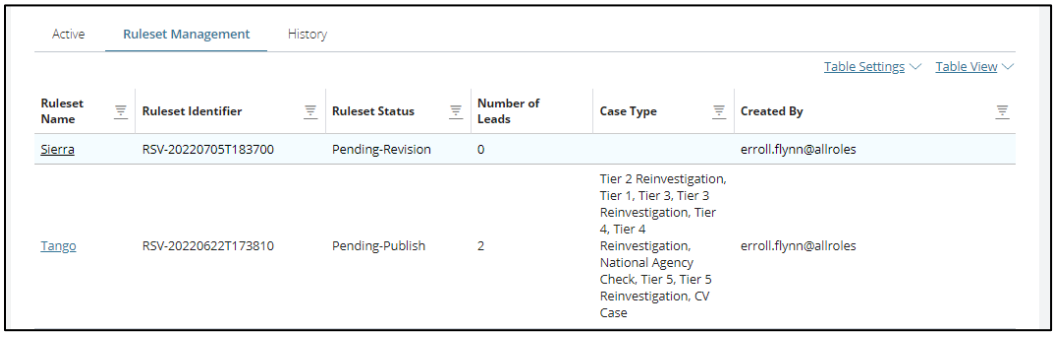


Figure 9-58: Rulesets - Pending Revision and Pending Publish

If **Approve** was selected, the Ruleset status will be in *Pending-Publish* on the Ruleset Management tab, and it will be published at the set date and time.

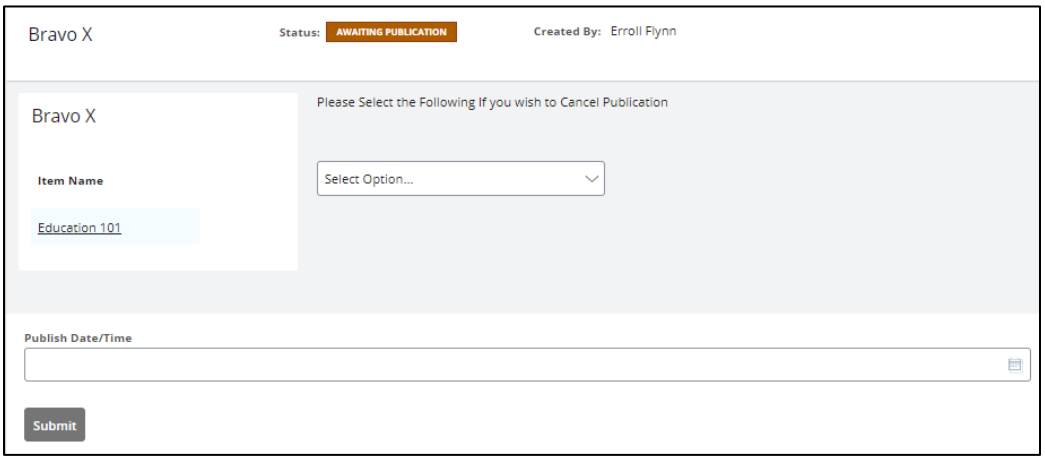


Figure 9-59: Awaiting Publication Screen

6. To see options available after submitting a ruleset for approval but before the publication date, select the **ruleset name** from the Ruleset Management tab and select the drop-down menu.
7. To change the Publication Date, select **Change Publication Date**.
8. Select the **calendar icon** to select a new date, and then select **Submit**.

The Ruleset will be published at the new set date and time and will appear on the **Scoping Rules – Active tab.**

If **Reject and send back for updates** was selected, the Ruleset status will be in *Pending-Revision* on the Ruleset Management tab, and it will be editable.

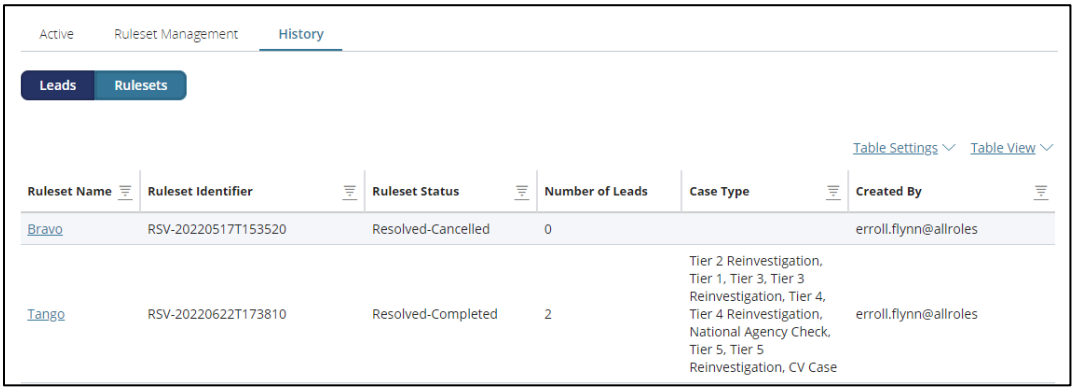


Figure 9-60: History – Cancelled and Completed Rulesets

If **Reject and archive** was selected, then the ruleset will be archived and viewable on the history tab under rulesets.

9.20 Disable Active Lead

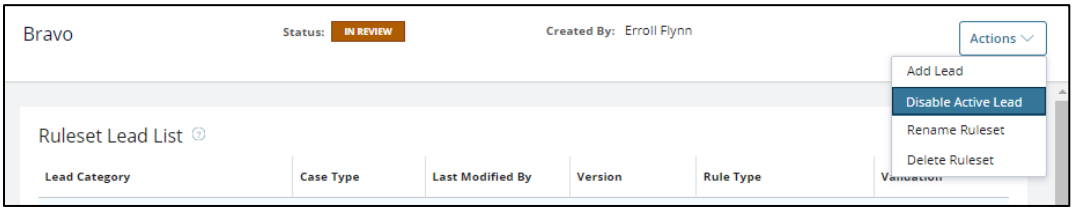


Figure 9-61: Scoping Rules - Disable Active Lead

1. To disable an active lead, from the **Actions** drop-down menu, select **Disable Active Lead**.

10 Workflow Builder & Module Configuration

Workflows are used in NBIS to control the steps and process for how cases are completed end to end, both within and across phases.

Note: Workflow Builder is used for all phases except Agency (Initiation, Review, and Authorization). To manage a workflow for Agency phases, utilize the Form Routing tab. See the Form Routing section for more information.

Note: To see an overview flow of the configuration, see Workflow Builder Configuration Diagram for more information.

10.1 Workflow Builder Overview

The Workflow Builder tab in Org Management allows the **Operations Manager** role to completely configure the workflow(s) for their organization, so they can cater to their specific needs. A **System Manager** can access Workflow Builder and configure/validate a workflow at the NBIS level for the Component and Interim Adjudication phases.

10.2 Managing a Workflow

10.2.1 NAVIGATE TO THE WORKFLOW BUILDER

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. Under the Configuration Menu, select **Workflow Builder**.

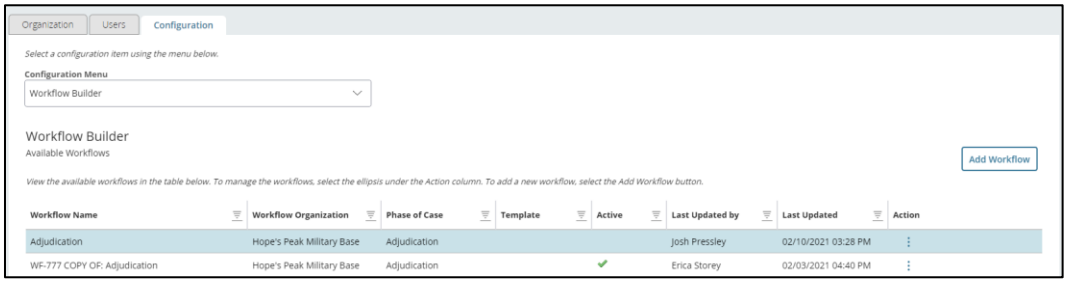


Figure 10-1: Workflow Builder - Add Workflow

Note: The Template field will always be blank.

10.2.2 ADD A NEW WORKFLOW

4. On the workflow builder screen, select the **Add Workflow** button.

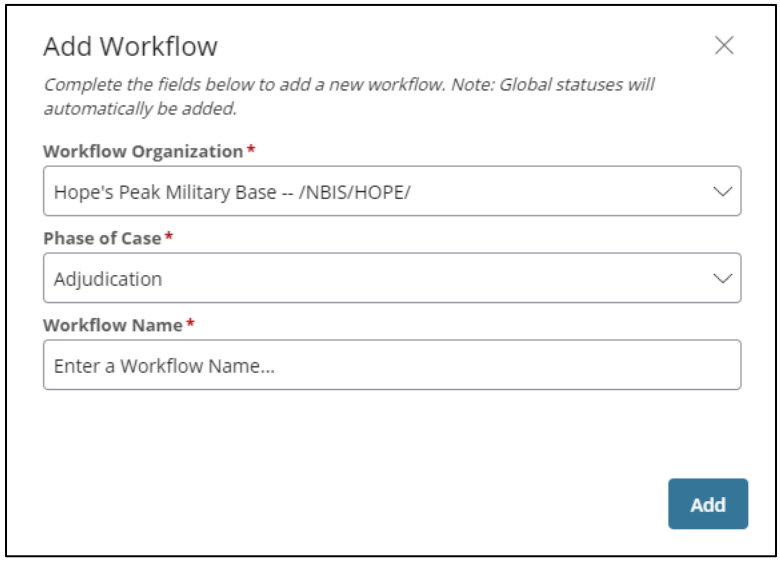


Figure 10-2: Add Workflow Modal

5. In the Add Workflow pop-up window, select the appropriate **Workflow Organization**, and **Phase of Case**, and enter a name in the **Workflow Name** field.

    a. Workflow Organization – must be configured with the correct Org Type for the Phase of Case of the workflow

    b. Phase of Case – select from the org types configured for the Workflow Organization

    Note: See Providing Specific Org Types, Functions, and Roles to ensure your Organization has the proper org type.

6. Select **Add** to create the new workflow. On the Workflow Builder screen, the new workflow now appears in the list of Available Workflows.

    Note: You can only have one active workflow per phase at a time for your organization.

10.2.3 EDIT A WORKFLOW NAME

7. Under the **Actions** column, select the **ellipses**, and select **Edit Workflow**.

    Note: In the Edit Workflow modal you can only change the **Name** of the Workflow.

8. Select **Update** to save.

    Note: To edit the actions, statuses, and modules that the workflow contains, you need to select the specific actions from the ellipses as listed in the sections below (not the Edit Workflow

action). However, these different edit options are not available for Active workflows, it must be inactive to edit.

10.2.4 DELETE A WORKFLOW

9. Under the **Actions** column, select the **ellipses**, and select **Delete Workflow**.

   Note: The **Operations Manager** may delete a workflow that is no longer needed. To delete a workflow, there must be no active cases using that workflow and the workflow must be inactive.

10. In the confirmation pop-up window, select **Delete** to delete the workflow.

10.2.5 CLONE AN EXISTING WORKFLOW

Operation Managers may decide to clone an existing workflow as an easy way to replicate and then modify it.

11. Under the **Actions** column, select the **ellipses**, and select **Clone Workflow**.
12. In the confirmation window, select **Clone**.

10.3 Manage Workflow Statuses

A **Status** is the stage within a workflow that an assignment can move to and from.

Statuses allow you to track case movements within a single workflow configured by your organization. Each Status represents a stage within the workflow that you can associate to many Actions that will be available to a user when the case is active. The internal status name is what will be seen by the Case Processors who are working on the cases within your organization. The external status name is what external organizations will see if they check the status of a case.

10.3.1 ADD A WORKFLOW STATUS

1. Locate the appropriate workflow, under the **Actions** column, select the **ellipses** and select **Configure Status.**

   Note: The Closed, Received, and Reopened global statuses are automatically populated for every workflow.

2. In the status screen, select **Add Status** to add a new status.

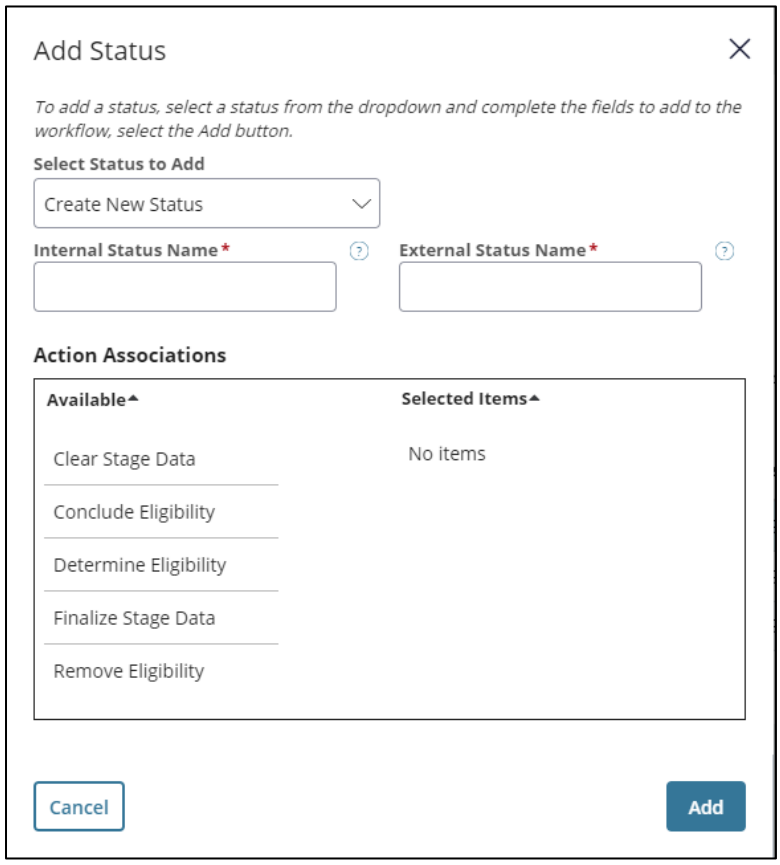


Figure 10-3: Add Status Modal

3. Select the drop-down arrow and choose **Create New Status**.
4. Fill in the required fields.

   Note: For Background Investigation cover phases, a checkbox with the option to suspend the case status will be available. When checked, the Progression Engine will not move cases forward if they are in this status.
5. Optionally select an **Action** from the Available column, and it will move to the Selected Items column, which means that this action will now be available when the case is in this status.

   Note: A new workflow might not have any actions available here because they have not yet been configured. Once an action is created, it will automatically be added to the starting status. Optionally, the action can be added or removed from additional statuses.
6. Select **Add** to add the new status.

10.3.2 EDIT A WORKFLOW STATUS

1. For the desired status, under the **Actions** column, select the **ellipses,** and select **Edit Status**.
2. In the Edit Status window enter the **Internal Status Name** and the **External Status Name**.

   Note: These fields for any global status cannot be edited.
3. Select the desired **Actions** associated with your Status from the **Available List**.

   Note: Actions associated with Global statuses may be edited. To remove an action from a status, select the Action from the Selected Items column, and it will move back to the Available actions column.
4. Select **Update**.

10.3.3 DELETE A WORKFLOW STATUS

An **Operations Manager** can delete an unused workflow status. Global statuses may not be deleted.

1. Under the **Actions** column, select the **ellipses**, and select **Delete Status**.
2. In the confirmation window, select **Delete**.

   Note: If there are any cases that are currently in a status, the status cannot be deleted. Once all cases are transitioned out of the status, it can then be deleted.

10.4 Manage Workflow Actions

Workflow actions are used to complete tasks on a case and transition it throughout the NBIS system. Actions are selected by **Case Processors** when working on cases. These actions are configured by the **Operations Manager** to use zero, one, or multiple modules. The same Actions can be available within multiple Statuses in the workflow and will always push the case to the ending status that has been configured for that Action. The instructions in this section will pick up after the **Operations Manager** is on the Configure Statuses screen.

10.4.1 ADD A WORKFLOW ACTION

1. From the **Switch To** drop-down menu, select **Configure Actions**.
2. Select **Add Action**.

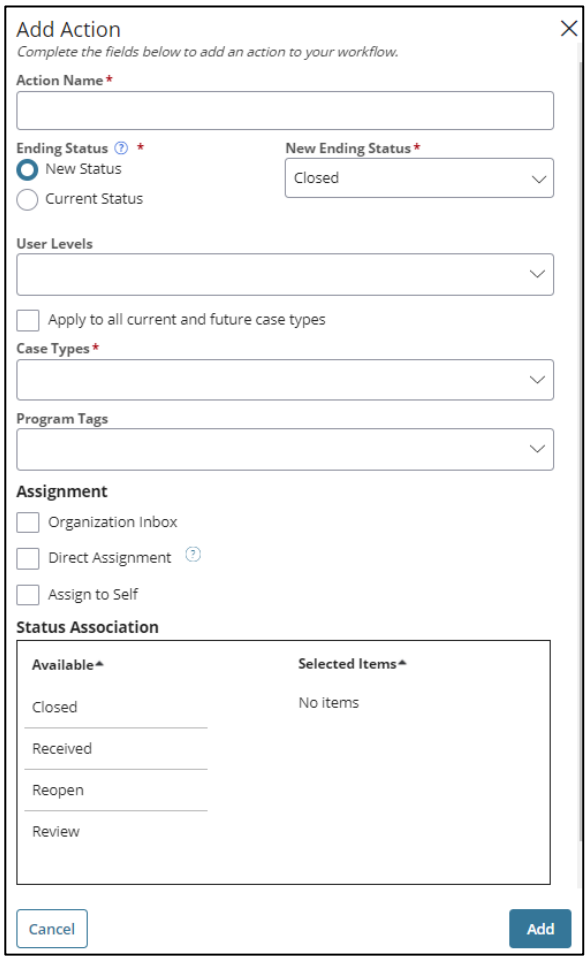


Figure 10-4: Add Action Modal

3. Fill in the action information (making sure to complete all required fields):
    a. **Action Name**
    b. **Ending Status** – The status the case will move to after an action is completed. If **New Status** is selected, you will be prompted to select the new ending status from the drop-down. If **Current Status** is selected, the action will end in the same status as it began and there will be no drop-down.
    c. **Hidden Action** – this is only available for Continuous Vetting and Background Investigation phases. Selecting the checkbox allows for the selection of a Backend Trigger Action and Available Status Associations. See Hidden Actions for more information.

        Note: Currently, the only trigger action available is Progression Engine. See Progression Engine for more information.

d. **User Levels –** Indicates which user levels this action will be available to.

e. **Case Types –** Indicates which case types this action will be available for. Select **Apply to all current and future case types** if the action is not dependent on a specific case type.

f. **Case Categories –** Indicates which categories of case types the action will be available for. This field only applies to Continuous Vetting and Background Investigation cases.

g. **Program Tags –** Indicates users with these program tags can take this action.

h. **Assignment –** Indicates if the case may be routed to an organization's workbasket, directly to a Case Processor's worklist, or to the user who took the action (or all three). The user level of the assignee will be required if Direct Assignment is chosen.

i. **Available Status Associations -** The status at which this action would be available. Select a status in the Available column and it will move to the Selected Items column, so the Case Processor will have this action to select from when they are assigned a case in that status. They can be removed by the same selection process.

Note: **System Managers** cannot utilize Program Tags, User Levels, and Case Categories in Workflow Builder.

4. Select **Add** to add the action.

10.4.2 EDIT A WORKFLOW ACTION

1. For the desired action, under the **Actions** column, select the **ellipses,** and select **Edit Action**.
2. Edit desired fields. You can edit all of the fields that were available when adding an action.
3. Select **Update** to save your changes.

10.4.3 DELETE A WORKFLOW ACTION

1. Under the **Actions** column, select the **ellipses**, and select **Delete Action.**
2. In the confirmation pop-up window, select **Delete**.

10.4.4 HIDDEN ACTIONS

Hidden Actions are only available for Continuous Vetting and Background Investigation cases and are not visible to case processors. They act as a way to automatically advance a cover case forward to another status when all alerts or leads under it are closed or a certain number that meet pre-specified criteria are closed. For example, Hidden Actions can be used to keep a cover case unassigned until all alerts under it are closed. See Case Progression Exception Rules for more information.

1. From the Workflow Builder screen, select the **ellipses** for an inactive **Continuous Vetting** or **Investigation** Workflow.

2. Select **Configure Actions**.
3. Select **Add Action**.
4. Select the **Hidden Action Checkbox**.

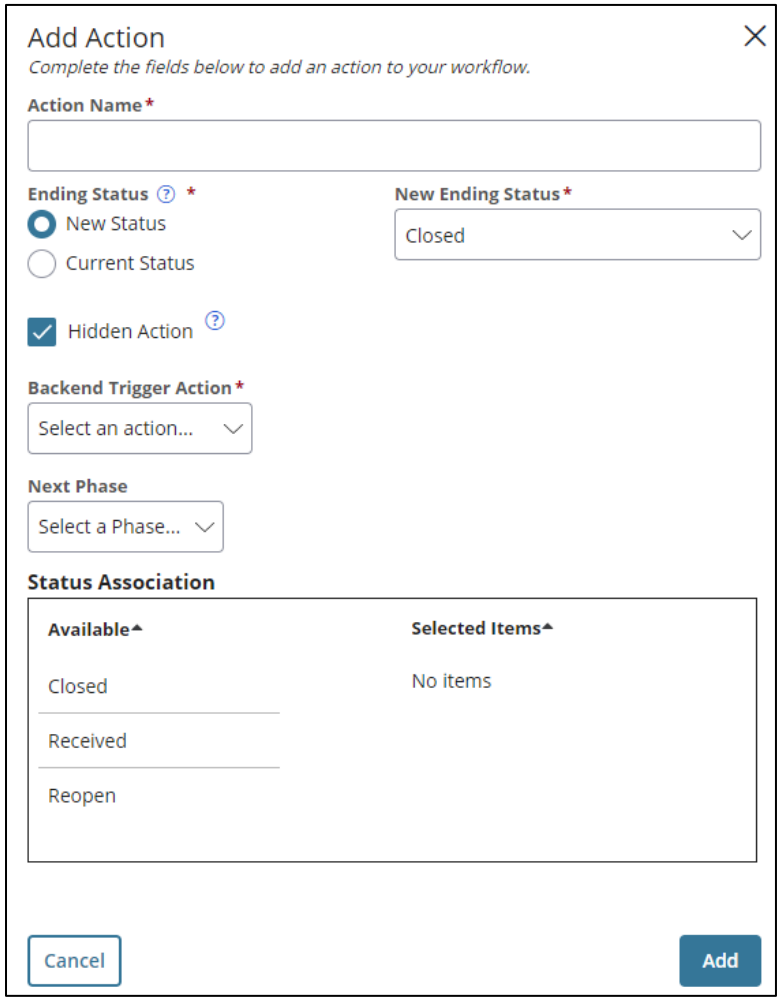


Figure 10-5: Add Hidden Action – Investigation Workflow Example

Once checked, all other data fields, except Status Association, will become hidden. A **Backend Trigger Action** drop-down will appear.

5. From the **Backend Trigger Action** drop-down, select a **Trigger Action**.

   Note: Currently, the only trigger action available is Progression Engine. See Progression Engine for more information.

   Note: For **Investigation** workflows, an additional **Next Phase** drop-down will appear to select which phase the case will move to when the Progression Engine triggers with this action.

6. Select a **Status** (or multiple) to associate to this hidden action.
7. Select **Add**.

10.5 Manage Workflow Modules

Modules are used when a user needs to complete an action on a case. Modules contain various fields in order to complete a specific action. In the workflow builder, the **Operations Manager** can select which module(s) they want to be available with an existing Action in the workflow. When the Case Processor is working a case and they select an Action, a pop-up screen will appear, containing the fields of the module(s) that were paired with that action.

Some modules can be configured, meaning the Operations Manager can control which fields are available to the Case Processor when they open the module in the case. Other modules do not have this functionality and can only be paired with Actions. The following table outlines all modules that are available and if they can be configured.

Incompatible modules and invalid orders can be configured. Be aware of the relationships between modules and their configurations.

Table 10-1: Workflow Modules Descriptions

Module	Description	Configuration Available?
Determination	Make a favorable or unfavorable eligibility determination.	Yes
Remove Determination	Remove a favorable eligibility.	Yes
Conclusion	Maintain a favorable eligibility.	Yes
Suspend Determination	Temporarily suspend a finalized favorable eligibility.	No
Reinstate Determination	Reinstate a suspended eligibility.	No
Pending Determination	Indicates a suspension of eligibility is pending.	No
Subtask	Send a subtask out to another org.	Yes
Clear Stage Data	Provides ability to remove or clear data that has been captured in one of the other modules, before it is finalized. Use if you are reviewing information and determine it is incorrect.	No

Module	Description	Configuration Available?
Finalize Data	Data captured in all the modules (except Clear Stage Data) must be finalized before the case can be closed and the data is saved to the subject's profile. The Subtask module must be finalized before it can be sent to the recipient.	No
Alert Prioritization	Allows the user to change the priority of an alert. This only applies to CV.	No
Notification	Send a note about the case to another organization.	Yes
Phase Transition	Transition the case from one phase to the next instead of closing the case.	Yes
Alert Disposition	After viewing an alert, use this module to indicate whether the alert is valid, invalid, or archived. This only applies to CV.	Yes
Distribution	Transition the case from one BI phase to the next instead of closing the case.	Yes
Org Redistribution	Transfer a case or lead from its current organization to another org across the org hierarchy with the same org functions and/or reschedule a lead based on zip code.	Yes
BI Close	Assign Case Seriousness, Case Closing Reason, and Justification to a Background Investigation cover case. Assign a Result Code to a lead case.	No

10.5.1 ADD A WORKFLOW MODULE

The instructions in this section will pick up after the **Operations Manager** is on the Configure Actions screen.

1. From the configure Actions screen, select the **ellipses** under the **Actions** column, in the row of the Action you want to add modules to.
2. Select **Configure Modules**.

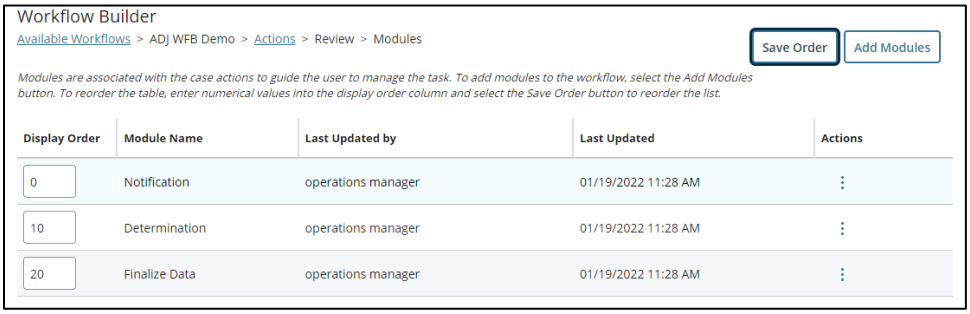


Figure 10-6: Workflow Builder - Modules

3. Select **Add Modules**.

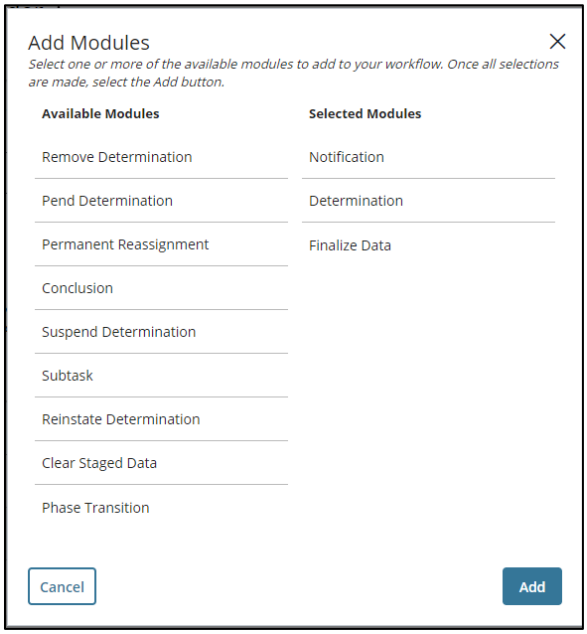


Figure 10-7: Add Module Modal

4. In the Add Modules pop-up window, under **Available Modules**, select the desired module(s) to move to the **Selected Modules** list.
5. Select **Add** to add the module(s).
6. After adding the modules, edit the **Display Order** field to control which set of fields appear first in the pop-up screen to the Case Processor when they are completing a case.
7. Select **Save Order** to save the order of appearance for the Modules. Modules will be arranged from lowest to highest number.

10.5.2 DELETE A WORKFLOW MODULE

8. In the row of the desired module, under the **Actions** column, select the **ellipses**.
9. From the drop-down, select **Delete Module**.
10. In the confirmation window, select **Delete.**

10.5.3 WHERE TO CONFIGURE MODULES

10.5.3.1 MODULE CONFIGURATION WITHIN WORKFLOW BUILDER

The **Operations Manager** can configure the fields available in a module within the Workflow Builder tab, from the configure Actions screen. Modules can also be configured from the Configuration tab in Org Management, see Configure a Workflow Module in Modules Configuration Tab for more information. The instructions in this section will pick up after the **Operations Manager** is on the Configure Actions screen.

1. From the row of the desired **Action**, select the **ellipses** and then **Configure Modules**.
2. From the row of the desired **Module**, select the **ellipses** and **Configure Module**.

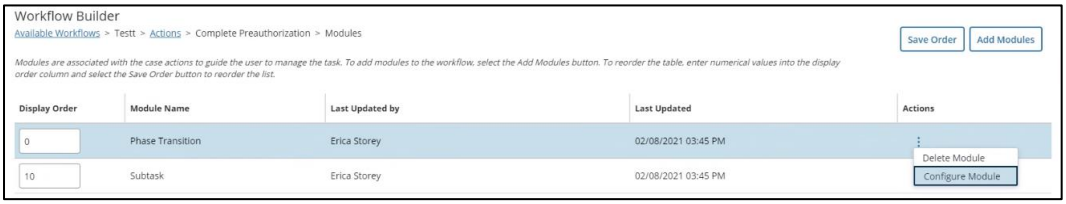


Figure 10-8: Workflow Builder - Configure Modules

Note: Make sure you have added modules to this action first. Not every module will have the Configure Module option available in the ellipses, because only some modules have pre-configurations accessible by users.

3. Complete the fields to control the data you want available to Case Processors when they are completing the module within the action.
4. Select **Submit** to save changes.

10.5.3.2 MODULE CONFIGURATION IN MODULES CONFIGURATION TAB

The **Operations Manager** can configure the fields available in a module from the Configuration tab in Org Management. In this tab you will see action and module pairings that were created from both active and inactive workflows in your organization's Workflow Builder tab. Only configurable modules that are already bound to an action will appear here. Modules can also be configured in the Workflow Builder tab, see Configure a Workflow Module in Workflow Builder for more information.

The **System Manager** is also able to configure modules this way for an NBIS level workflow for the Component and Interim Adjudication Phases. See NBIS Level Configurations for Workflow Builder for instructions on how to add an NBIS level workflow.

1. From the left navigation menu, select **Org Management**.
2. Select the **Configuration** tab.
3. From the **Configuration Menu** drop-down, select **Modules.**

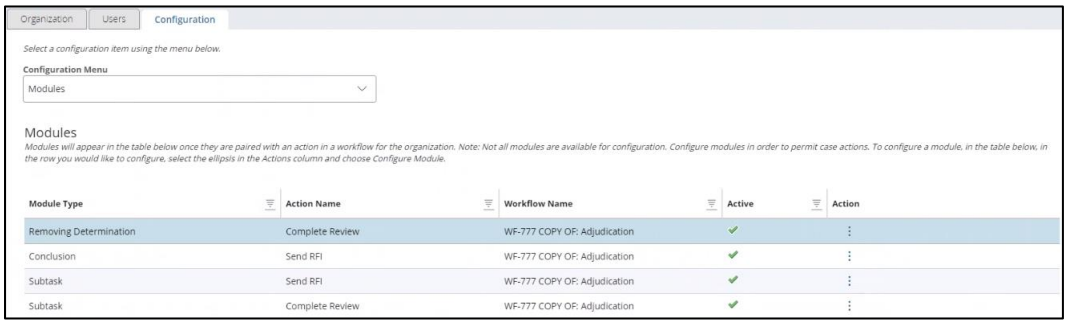


Figure 10-9: Org Management - Modules

4. From the row of the desired module, in the **Action** column, select the **ellipses**.
5. Select **Configure Module**.
6. Complete the fields to control the data you want available to Case Processors when they are completing the module within the action.
7. Select **Submit** to save your configurations.

10.5.4 CONFIGURATIONS FOR DETERMINATION MODULES

There are three modules that capture eligibility determinations for a subject that have org level configurations. The configuration steps below apply to all three modules. The specific configuration fields are dependent upon the **Module Type** which is displayed in the Modules list.

- **Determination Module** is used to initially grant eligibility or to make an unfavorable eligibility determination
- **Conclusion Module** is used to maintain a previously granted eligibility
- **Remove Determination** module is used to take away a previously granted eligibility.

The instructions in this section will pick up after the **Operations Manager** is on the Configure Actions screen.

1. From the row of the desired **Action**, select the **ellipses** and then **Configure Modules**.
2. From the row of the desired **Module**, select the **ellipses** and **Configure Module**.
3. Select the **Determination Type**.

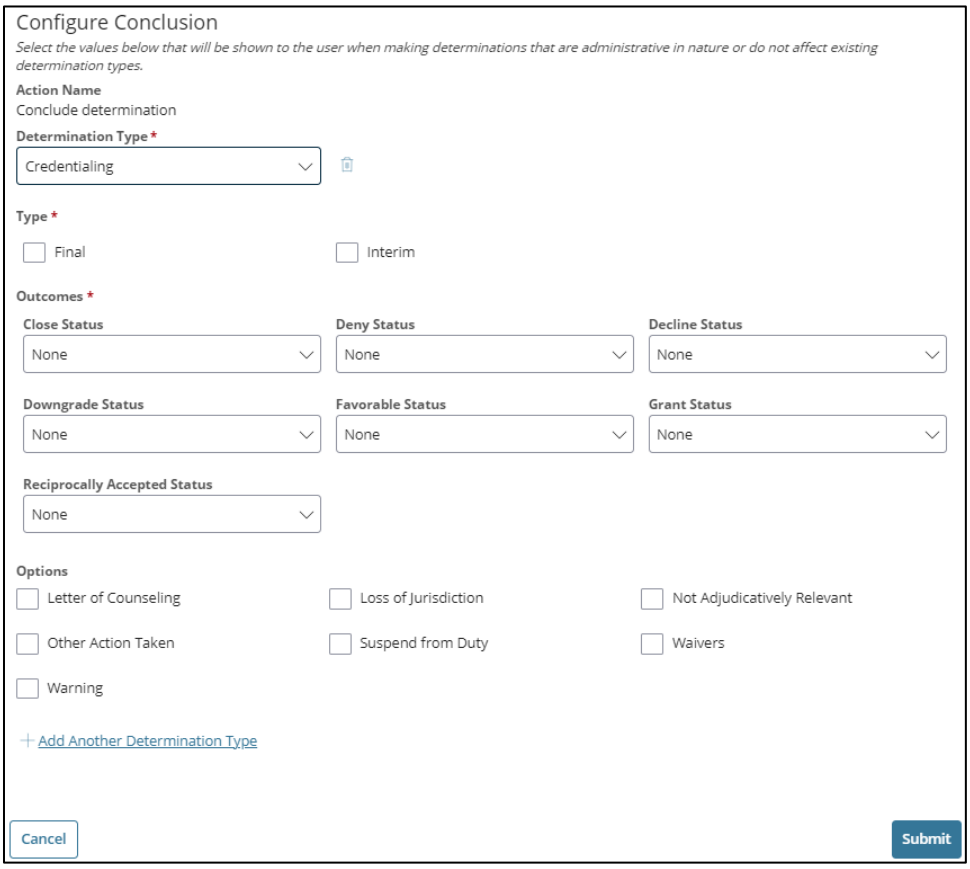


Figure 10-10: Configure Conclusion Module

4. A set of fields will appear below. For each field, select the data that you want to be available for the Case Processor to choose from when they are completing this module.

   Note: Different Determination Types will trigger different fields and data options to appear below.

> At the NBIS global Case Type Relationships table, the Outcomes, Options, Add-Ons and Types data is mapped to the Determination Type and Organization Type, which controls what is displayed to the Operations Manager when they are configuring these modules for their organization. The values that appear here are from the Case Type Relationship table in System Settings.
>
> The values that appear here are from the Case Type Relationship table in System Settings. If the Determination type that you selected has multiple case types associated with it, then all those Case Type Relationship values configured will appear on the modal for the Case Processor. The case type only filters the data in the case worksheet modal, so the Case Processor may see some options in this configuration window that will not appear in the popup to complete the determination action.
>
> Make sure you are configuring the necessary values to be available for the appropriate case type.

5. Once the first set of fields are complete, (optionally) select **Add a New Adjudication Type** to add an additional Determination Type to be completed with that module.
6. Select **Submit** to save configurations.

10.5.5 SUBTASK MODULE CONFIGURATION

The **Subtask Module** is used when a Case Processor wants to request more information about a subject from an external organization (a common example is a Request for Information (RFI)). The **Operations Manager** will configure the subtask module for the **Case Processor** for when they are working the case and the actions for the subtask recipient organization. The instructions in this section will pick up after the Operations Manager is on the Configure Actions screen.

1. From the row of the desired **Action**, select the **ellipses** and then **Configure Modules**.
2. From the row of the desired **Module**, select the **ellipses** and **Configure Module**.
3. Input the **Subtask Name, Subtasks Instructions,** and **Response Request Duration.** These fields will be visible to the Adjudicator when they select the action to send out a sub-task.

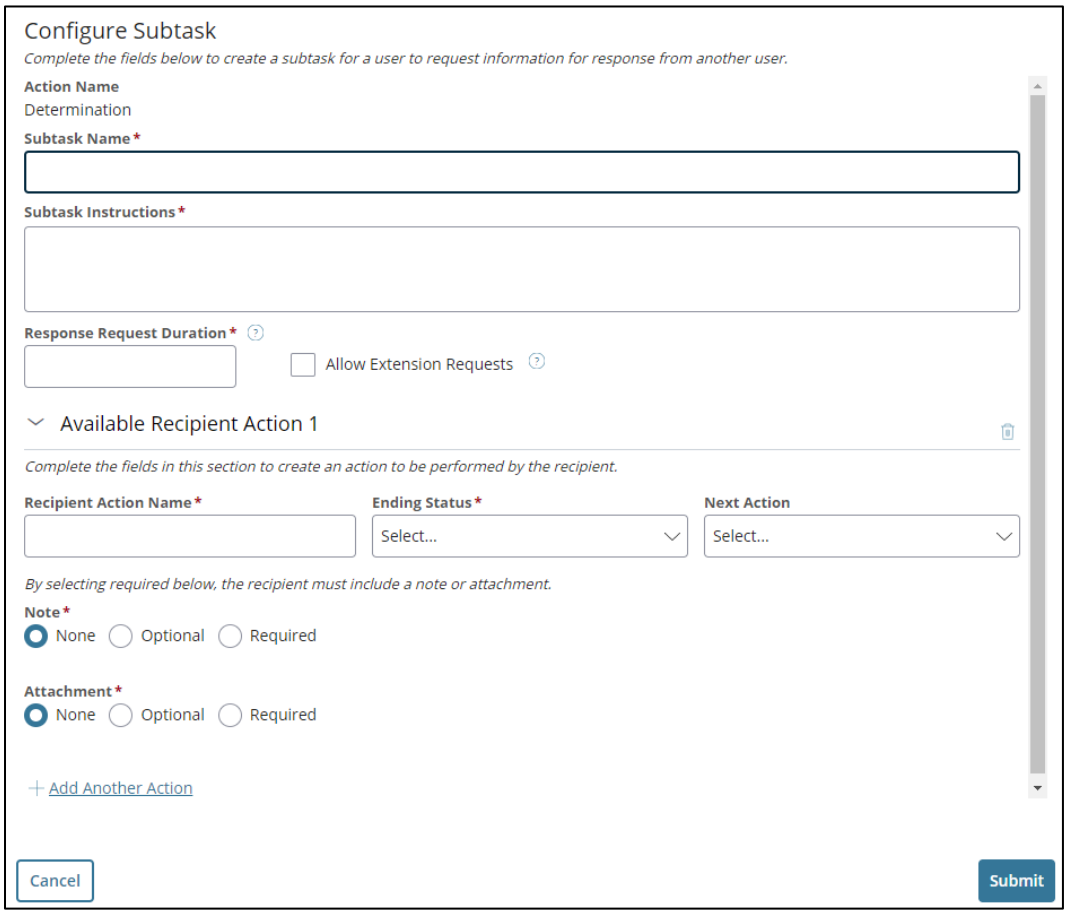


Figure 10-11: Configure Subtask Module

4. You can also check to **Allow Extension Requests** which will automatically create a default Available Recipient Action. An extension request will allow the organization more time to gather the information.

   Note: **Available Recipient Actions** are actions that the subtask recipient will have available to them when they receive the subtask case assignment.

3. Complete the required fields for at least one other **Available Recipient Action** and indicate what action the subtask recipient can take.

   Note: The **Ending Status** is the status the case will be routed to when they submit the subtask.

4. The **Next Action** field is used when you have configured another Action with a Subtask Module in your workflow, and you want the subtask recipient to complete that subtask after the one you are currently configuring.

5. Optionally select **Add Another Action** to give the subtask recipient an additional action to choose from.

6. Select **Submit** to save the configurations.

10.5.6 PHASE TRANSITION MODULE CONFIGURATION

Phase Transition module allows the **Case Processor** to transfer a case from one phase to another, such as from the Adjudication Phase to the Appeals Phase. Depending on what phase you are transferring to, there will be different logic used to determine the routing options.

Table 10-2: Phase Transition Logic Table

Transitioning To	How Available Organizations are Determined
Interim	The service will depend on the subject's owning organization.
Component Adjudication	The service will depend on the component adjudication organizations within the subject's owning organization's hierarchy.
Anything else	Follows service relationships defined within the Org Relationships tab.

The instructions in this section will pick up after the **Operations Manager** is on the Configure Actions screen.

1. From the row of the desired **Action**, select the **ellipses** and then **Configure Modules**.
2. From the row of the desired **Module**, select the **ellipses** and **Configure Module**.
3. Enter the **Phase Transition Name**.

Figure 10-12: Configure Phase Transition Module

4. From the **Next Phase** drop-down, select a **Phase**.

5. After selecting a **Phase**, the **Organization Selection** field will appear to choose the specific organization(s) the case will be routed to in the next phase. If multiple organizations are selected, the case processor will select which organization to route the case to when taking the action.

   Note: If organization relationships are not set up with an org in the phase selected, then the **Organization Selection** field will not appear. The **Case Processor** will need to select from any implementer available for the phase when taking the action.

   Note: If any of the organizations selected have service catalog configurations enabled, an additional field **Service Catalog Case Types** will appear. Case types selected here will be available to the **Case Processor** to select when taking the action on a service catalog case. This will determine the case type that the case will take in the organization it is phase transitioned to.

6. Select **Submit** to save the configurations.

10.5.7 NOTIFICATION MODULE CONFIGURATION

The **Notification Module** is used for notifying users within any organization and/or for sending files. The instructions in this section will pick up after the Operations Manager is on the Configure Actions screen.

1. From the row of the desired **Action**, select the **ellipses** and then **Configure Modules**.
2. From the row of the desired **Module**, select the **ellipses** and **Configure Module**.
3. Complete the **required fields**.

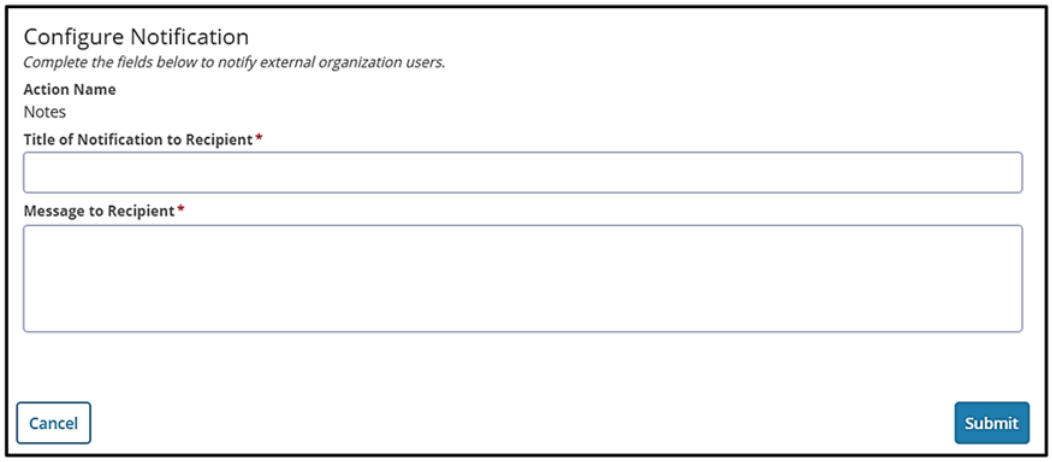


Figure 10-13: Configure Notification Module

4. Select **Submit** to save the configurations.

10.5.8 ALERT DISPOSITION MODULE CONFIGURATION

The **Alert Disposition Module** is used to configure which fields are available to the CV Analyst when using the module in an alert case. Reasons, Guideline Categories, justification, and alert comments can all be included and required for valid, invalid, and/or archived alerts.

The instructions in this section will pick up after the **Operations Manager** is on the Configure Actions screen.

1. From the row of the desired **Action**, select the **ellipses** and then **Configure Modules**.
2. From the row of the desired **Module**, select the **ellipses** and **Configure Module**.
3. Under **Disposition Types**, select the applicable **disposition(s)**.

   Note: You can select multiple dispositions to configure fields for in this module. Configurable fields will populate based on the disposition type selection.

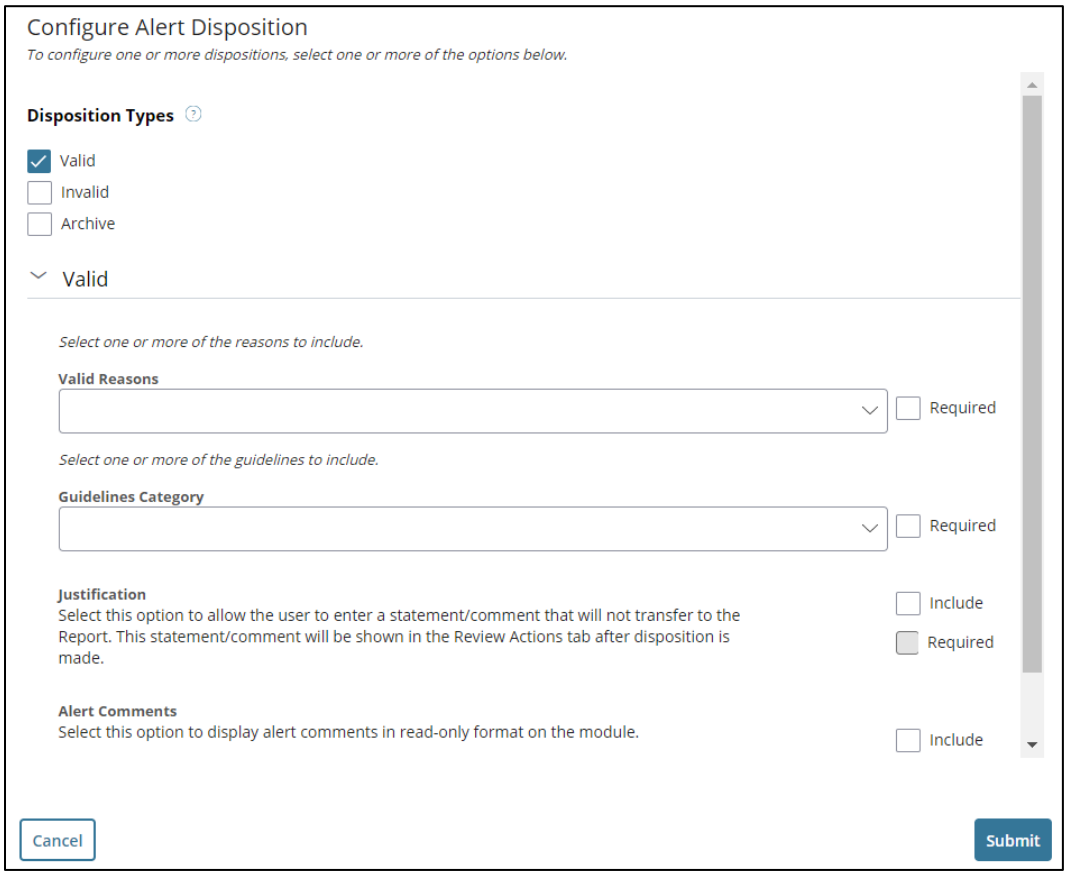


Figure 10-14: Configure Alert Disposition Module – Valid Checked as an Example

4. From the **Reasons** drop-down, select the applicable **reasons**.
5. From the **Guidelines Category** drop-down, select the applicable **guideline category**.

6. Optionally select the **Required** checkbox for Reasons, Guideline Category, and Justification.

   Note: The **Include** checkbox must be selected first for **Justification** before the **Required** checkbox is available.

7. Optionally select the **Include** checkbox next to **Alert Comments** to display the alert comments on the module.

8. Select **Submit** to save the configurations.

   Note: The reasons that can be selected for this module are managed in System Settings; see the **NBIS Admin Guide** for more information.

10.5.9 DISTRIBUTION MODULE CONFIGURATION

The **Distribution Module** allows the Case Processor to transition a case from one phase to another within the background investigation phases. The Distribution module uses an organization's configured distribution rules to route the case to the next phase and appropriate organization. The available "Next Phase" drop-down options in design-time configuration of this module are managed in System Settings. When transitioning from Preparation to Investigation, the Distribution module will create lead cases for any of the staged leads in the Preparation lead list so that they can be worked within the appropriate organizations.

The instructions in this section will pick up after the **Operations Manager** is on the Configure Actions screen.

1. From the row of the desired **Action**, select the **ellipses** and then **Configure Modules**.
2. From the row of the desired **Module**, select the **ellipses** and **Configure Module**.
3. Select the **Next Phase** to transition the case.

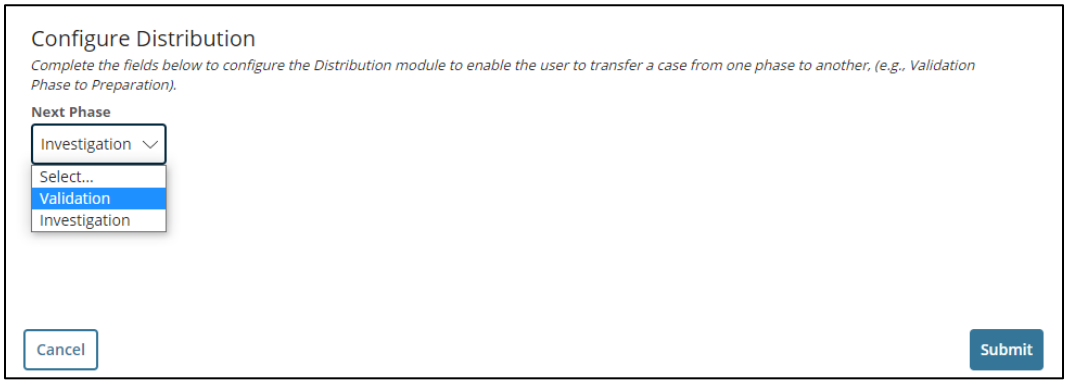


Figure 10-15: Configure Distribution Module

4. Select **Submit**.

10.5.10 ORG REDISTRIBUTION MODULE CONFIGURATION

The Org Redistribution Module allows the Case Processor to transition a case from one organization to another within the same background investigation phase. When the **Route using Zip Code** checkbox is selected, the Org Redistribution module will use an organization's zip code to route the case to the appropriate organization. If the checkbox is not selected, the module will route the case to another organization in the org hierarchy and the function of the org. To have the module appear in design-time configuration is managed in System Settings.

The instructions in this section will pick up after the **Operations Manager** is on the Configure Actions screen.

1. From the row of the desired **Action**, select the **ellipses** and then **Configure Modules**.
2. From the row of the desired **Module**, select the **ellipses** and **Configure Module**.
3. Select the **Route using Zip Code** checkbox route the case to another org based on zip code.

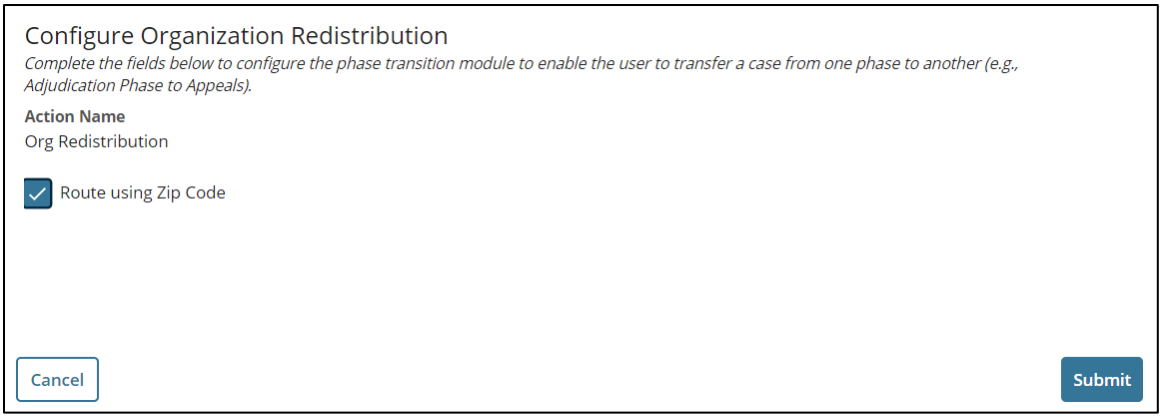


Figure 10-16 Configure Org Redistribution Module

4. Select **Submit**.

10.6 Workflow 360

Workflow 360 is a section of workflow builder where an Operations Manager can validate and activate an individual workflow along with the ability to evaluate the workflow. The test harness allows you to use different filters to determine if the workflow was configured correctly. This includes filtering by User Level, Program Tags, and Case Types, Status, and Actions associated.

The instructions in this section will pick up after the **Operations Manager** is on the main Workflow Builder configuration screen.

1. In the row of the desired workflow, under the **Actions** column, select the **ellipses**.
2. Select **View Workflow 360**.

10.6.1 USER TEST HARNESS FILTERS

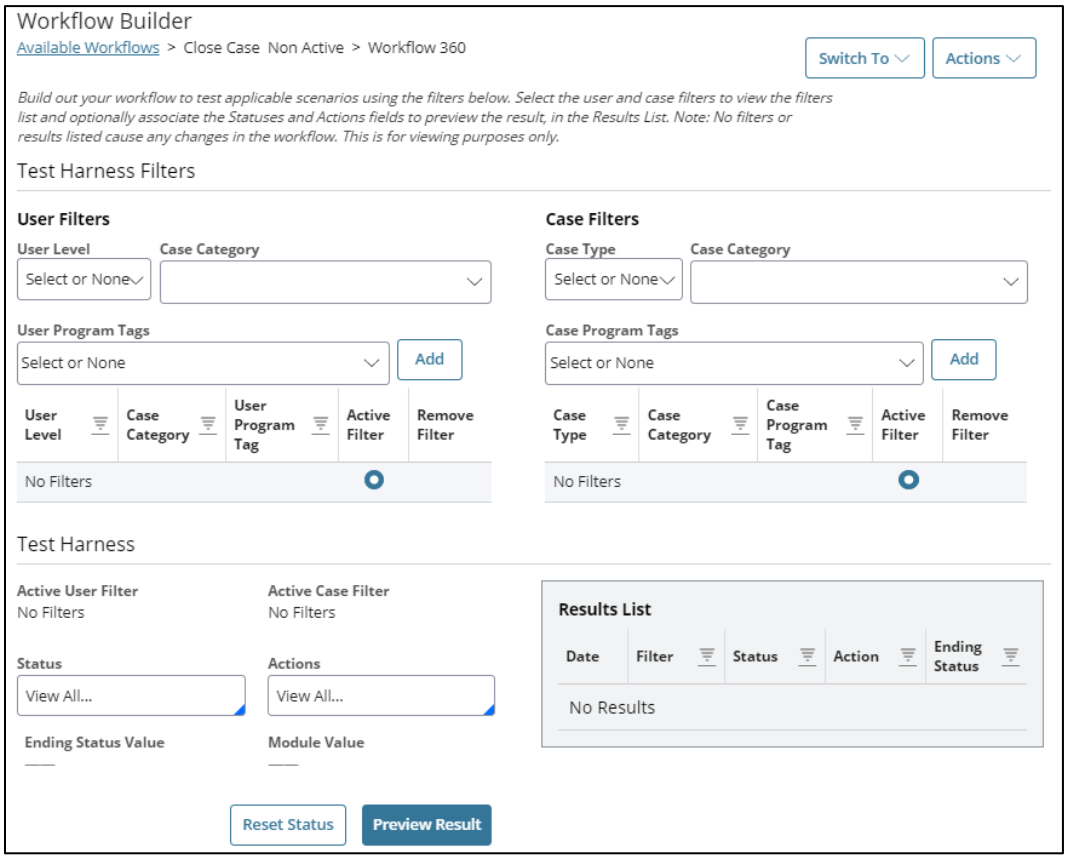


Figure 10-17: Test Harness in Workflow 360

1. From the **User Level** drop-down, select the **User Levels** that are in the workflow to be tested.
2. From the **User Program Tags** drop-down, select the **User Program Tags** that are in the workflow to be tested.

3. Select **Add**.
4. Under **Active Filter**, select the **radio buttons** to activate the filter. Selections will load below the filtered User section.
5. From the **Case Type** drop-down, select the **Case Types** that are in the workflow.
6. From the **Case Category** drop-down, select the **Case Categories** that are in the workflow.

   Note: System Managers cannot utilize Case Categories in Workflow Builder.
7. From the **Case Program Tag** drop-down, select the **Case Program Tags** that are in the workflow.

   Note: User levels, Case Categories, Case Types, and User/Case Program tags may be added individually or in combination with each other.
8. Select **Add**.
9. Select the **radio buttons** to activate the filter for the selection to test.
10. Select the **trashcan icon** to remove an item from your list.

10.6.2 USING THE TEST HARNESS TO TEST WORKFLOW SCENARIOS

The Test Harness allows a user to select filters for user capabilities and case specifications, you can use the test harness to preview potential actions/statuses/modules that would occur if those criteria were to occur. Once a result is previewed, the ending status is placed in the first field automatically. This allows a manager to ensure that all possible cases that are sent through the workflow builder are configured correctly.

1. In the **Test Harness**, from the Status drop-down, select a **Status** to Test the workflow you have configured.
2. From the Actions drop-down, select an **Action** associated with the Status to Test the workflow you have configured. The only Actions available are those built into the workflow for the Status you are testing. The Ending Status value and associated Module will display below the drop-down.
3. Select **Preview Result** to populate your selections to the results list. The ending status for each action will automatically populate to the Status box as a shortcut so the next associated action can be chosen.

10.6.3 USING THE FULL VIEW OF THE WORKFLOW

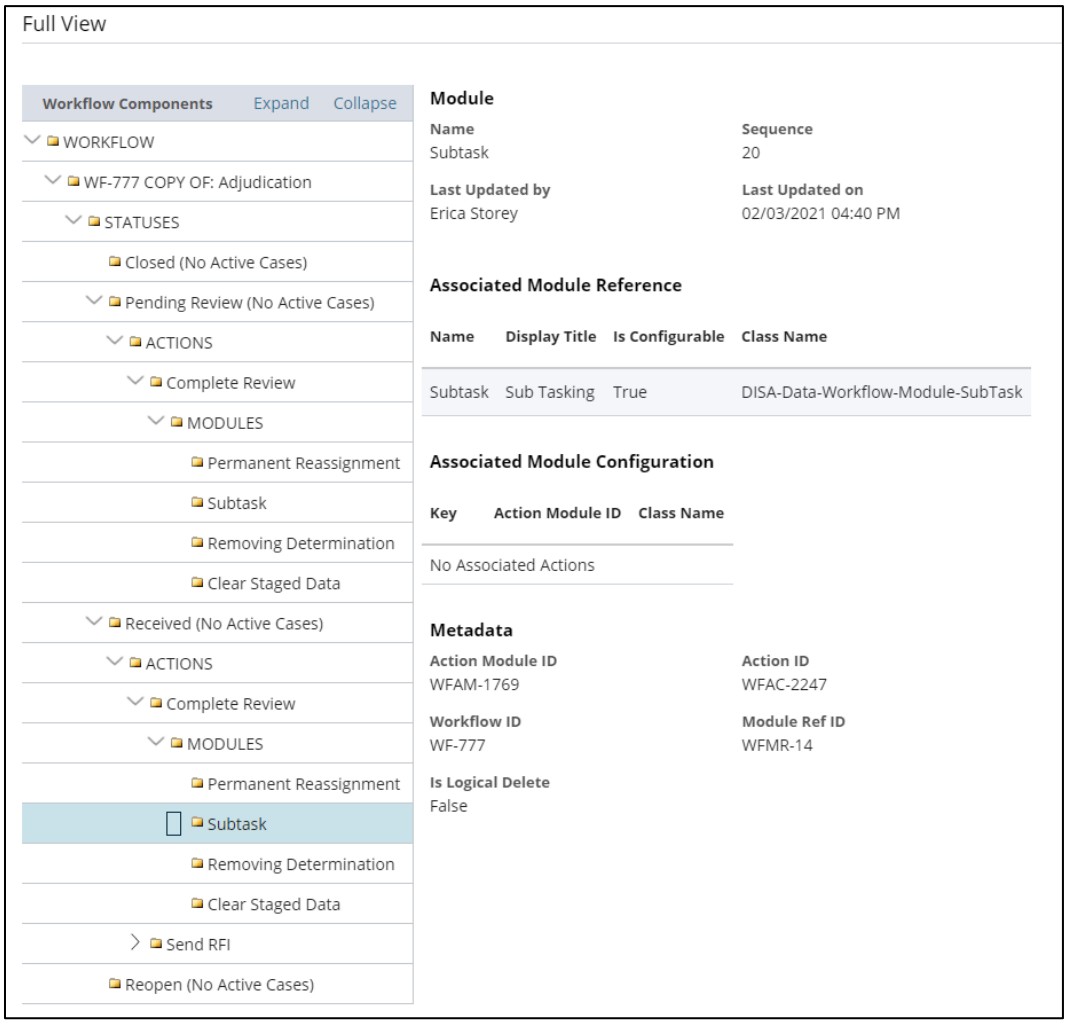


Figure 10-18: Full View of Workflow

The view of the workflow allows the user to view the workflow in a hierarchical format. Additional Meta data about each configuration will also be displayed for advanced troubleshooting needs.

1. In the **Full View** section, select the **arrow next to the Workflow** to view the entire workflow.

   Note: All components of the Workflow appear in the hierarchical view: all Statuses, Actions, and associated Modules appear in the list.

2. Select a **Status** to view metadata associated with that status. Details for that Status appear to the right of the status.

10.6.4 VALIDATE AND ACTIVATE WORKFLOW

Validation of a workflow occurs during and after testing of a workflow in Workflow 360. The **Operations Manager** triggers the system validation. After validation, a list of errors and warnings will display identifying missing or unused configurations.

Validate a workflow:

1. In the row of the desired workflow, under the **Actions** column, select the **ellipses**.
2. Select **View Workflow 360**.
3. From the **Actions** drop-down, select **Validate Workflow**.
4. Select **Validate Workflow**.

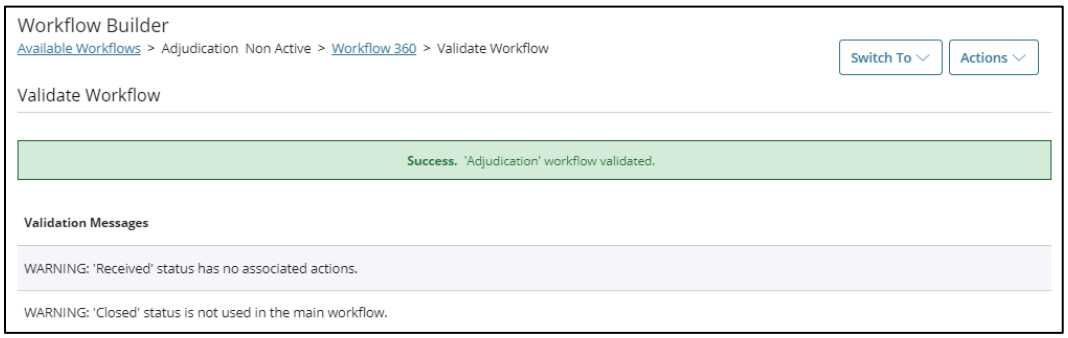


Figure 10-19: Workflow Builder - Validate Workflow

If the workflow is successfully validated, then a **success message** will appear. If there are issues, they will appear as errors or warnings, with specifics to assist in resolution. **Errors** are issues that will prevent the workflow from being activated, and you will need to re-configure the specific parts of your workflow to correct them before it can be used by your organization. **Warnings** do not stop the workflow from being activated, however the system is recommending that you resolve them before doing so.

Activate a workflow:

The Activate Workflow action will be available for inactive workflows that have been successfully validated. If you had a different workflow for the same phase that was previously active, it will become inactive upon activation of a new one.

5. From the Actions drop-down, select **Activate Workflow**.
6. Select **Activate Workflow**. This workflow will now be used by cases in your organization and will be reflected as active in the Workflow Builder landing page.

10.7 NBIS Level Configurations for Workflow Builder

A **System Manager** can access the Workflow Builder and configure/validate a workflow at the NBIS level for the Component Adjudication or Interim Determination phases. Currently the only phases that exist at the NBIS Level are Component Adjudication and Interim.

NBIS Level workflows are pushed from top level organization down to local organizations. Local organizations do not control these workflows.

1. Login as a **System Manager**.
2. From the left navigation menu, select **Org Management**.
3. Select the **Configuration** tab.
4. Under the Configuration Menu, select **Workflow Builder**.
5. On the workflow builder screen, select the **Add Workflow** button.

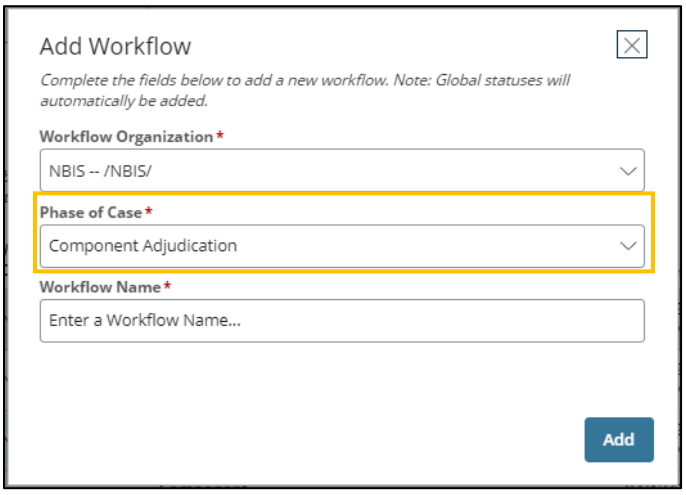


Figure 10-20: Add NBIS Level Workflow

6. In the **Add Workflow window**, under **Workflow Organization**, select **NBIS**.
7. Under **Phase of Case**, select **Component Adjudication** or **Interim**.
8. Select **Add** to add the workflow.

Note: See above sections for how to configure the workflow.

10.8 Workflow Builder Configuration Diagram

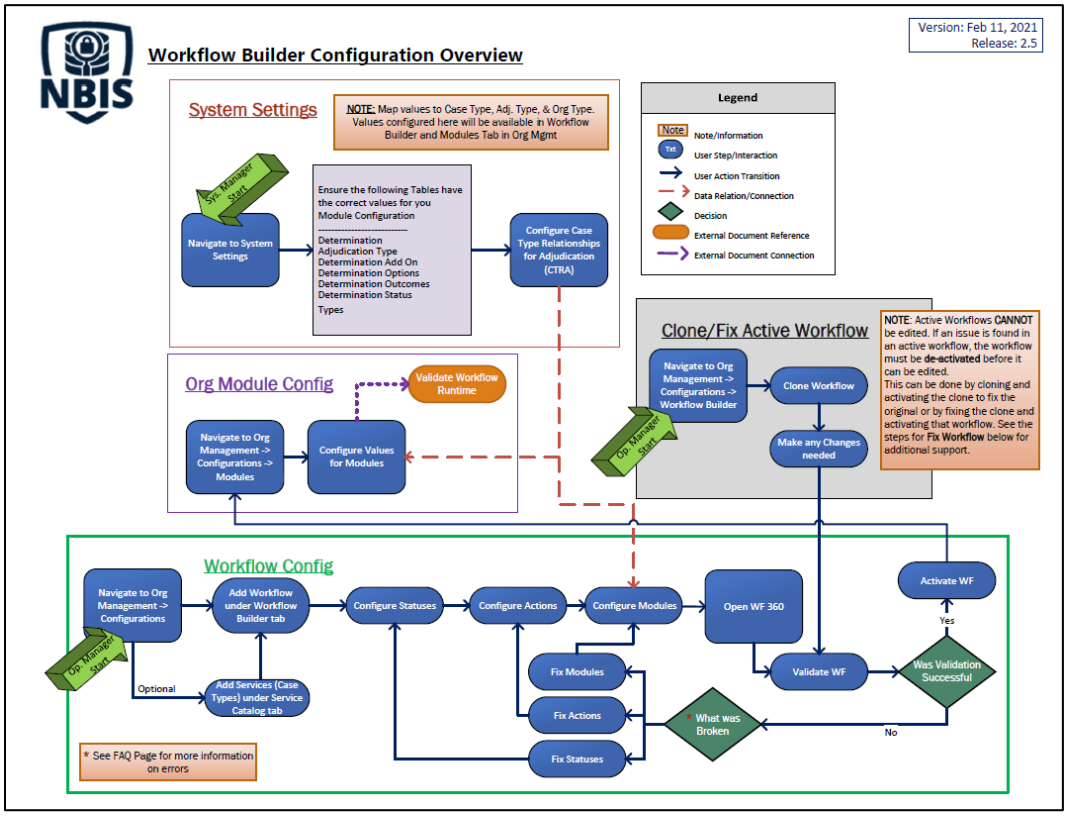


Figure 10-21: Workflow Builder Configuration Diagram

11 Reporting

The Reporting system is used to create reports using various types of data within the NBIS system. These reports can be adjusted and filtered by the user and exported to PDF or Excel. All roles will have access to the Reports tab on the left navigation menu. In order to have reports populated on the tab, the Reports Manager for their organization will need to grant the appropriate roles access.

11.1 Manage Report Access

Users with the role of **Reports Manager** are able to configure access for Reports. The **Reports Manager** for an organization can manage individual report access for their organization. Report access includes the ability to run reports and/or export reports.

11.1.1 MANAGE INDIVIDUAL REPORT ACCESS

A user with the role of **Reports Manager** is able to configure the roles that will have permissions to run individual reports, and from that list, the roles that will be able to export the report data.

The **Reports Manager** is able to select the roles for their organization that are able to run and export individual reports.

1. From the left navigation menu, select **Report Builder**.

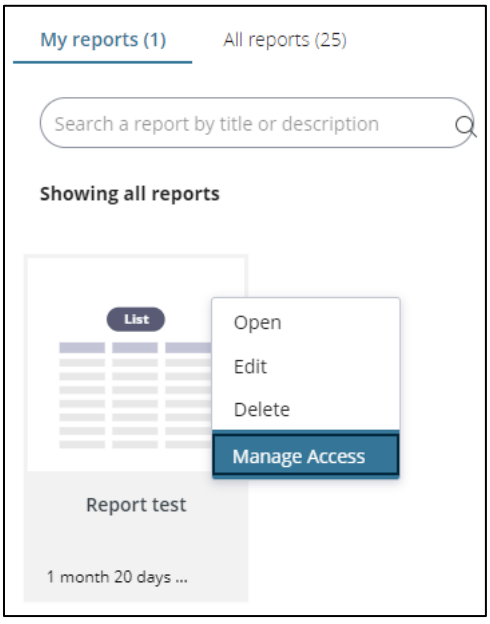


Figure 11-12: Manage Access for a Report

2. Select the **gear icon** on the top right of the report that access needs to be configured for.
3. From the drop-down, select **Manage Access**.

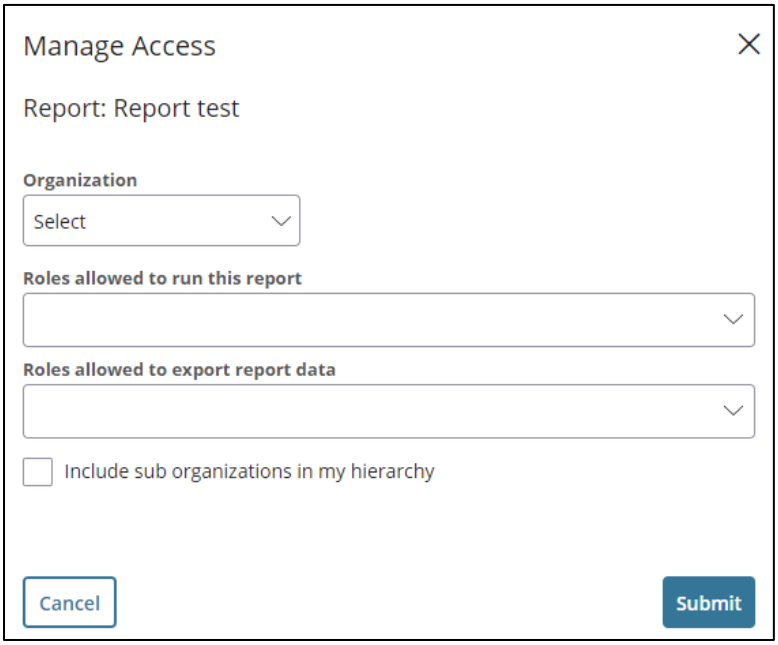


Figure 11-13: Select Roles to Run and Export Individual Reports

1. From the **Organization** drop-down, select the **Organization** that will have access to the individual report.
2. From the **Roles allowed to run this report** drop-down, select the **roles** to be given permission to run the chosen report.

   Note: Only the roles that were given **System Report Access** will be available in the drop-down.
3. From the **Roles allowed to export report data** drop-down, select the **roles** to be given permission to export the chosen report.

   Note: Only the roles that were added to **Roles allowed to run this report** will be available in the drop-down.
4. Checking the box to **include sub organizations in my hierarchy** will grant the configured report access to the users in the Report Manager's sub organizations.

11.2 Types of Reports

Table 11-1: Types of Reports

Report Name	Report Category	Report Description
Active Case Report	Subject Management	List of Active Cases which a user created within an organization. This report has a link which takes the user to the case in the Subject Profile.
Case Ingest Report 2.0	Inventory	Display the date and time that cases were received by a user's organization.
Inventory Report 2.0	Case Management	Display the cases based on the filters and headers aggregated within the report. Tracks if a case has been assigned to a User and the Date/Time of any status updates.
Adjudication Status Count By Org	Inventory	Display number and status of Adjudication cases in Adjudication Orgs
User Activity Report 2.0	Case Management	Display user activity based on the filters and headers aggregated within the report. Tracks the date/time of any action taken or any status updates made by a User.
Alert Ingest	Continuous Vetting	Display Alert Ingest records and the related errors
Case Ingest	Inventory	Display Case Ingest records and the related errors
CV Enrollment	Continuous Vetting	This report displays all subjects that are enrolled in Continuous Vetting for an organization during a specified timeframe.
CV Enrollment Failure	Continuous Vetting	This report captures subjects that are eligible to be enrolled into Continuous Vetting but the enrollment fails due to a failed data source enrollment.
EAdjudicated Case Count	Inventory	Display Adjudication cases by Date and SOI
Ingest Rules Report	Inventory	Displays the date and time that files were ingested, the Organization, Status, Ingest Type, Investigation Type, and the SOI if available.
Inventory Template Report	Inventory	Track the number of cases based on the filters and headers aggregated within the report

Report Name	Report Category	Report Description
LSR to PEGA Sync Report	Subject Management	Track the number of data batches from LSR to PEGA that have succeeded or failed so that support personnel can pull the report and troubleshoot.
PEGA to LSR Sync Report	Subject Management	Track the number of data batches passing PEGA to LSR that have succeeded or failed so that support personnel can pull the report and troubleshoot.
Subject Based Active Case Report	Subject Management	List of subject-based active cases which includes Submission and All Generic Case Types regardless of affiliation.
Submission Cases by Date Range	NBIS Report	Display all submission cases for your organization.
Sub Org Level Case Statistics	NBIS Report	Returns a count of all users in a sub-org(s) and the total amount of cases (by case type and SF form) for a specific date.
Top level Org Case Statistics	NBIS Report	Returns a count of all users in that organization and its sub-orgs and the total amount of cases (by case type and SF form) for the week and year that the report is pulled.
User Activity	NBIS Report	Display Activity by Org, User, and Program Tag
User List	NBIS Report	List of users, roles, and recent sign-on for an organization
User List Including All Sub Organizations	NBIS Report	List of users, roles, and recent sign-on for an organization hierarchy

11.3 Viewing a Report

1. From the left navigation menu, select **Reports.**

   Note: The reports available can be filtered by description or category.

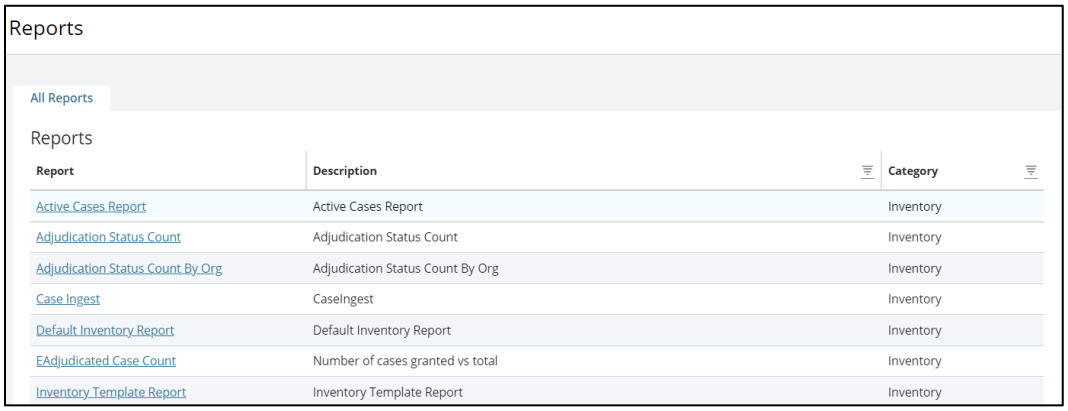


Figure 11-1: Reports

2. Select a **Report**.

Each report will vary based on its type and content. There are several general report structures that can be interacted with in similar ways.

11.3.1 DRILLING DOWN INTO A REPORT

Selecting interactive text within a table can be used to drill down for more targeted information. If the field value you selected was a possible value for the report filter, the table will be reloaded with that value added to the filter and a new list of results to match the query. This is not applicable to all values/reports.

Note: if a case ID is shown on a report, you can select the ID to open the Subject profile.

Note: A breadcrumb is present on the top left which can be used to take the user back to the Report once you have drilled down.

11.3.2 FILTER OPTIONS WITHIN A REPORT

Reports with a large number of records can be adjusted by filtering the report to more granular attributes. There are two types of report filtering based on the report type.

Reports with Selectable Filter Hyperlinks

Certain reports will contain a "Filtered by" banner at the top that displays selectable hyperlinks for each filter type for that report. To edit the filters, these links can be selected which will bring you to an edit filter modal to modify the current filtering on the report. The values in the filter modal will vary based on the data field selected. For any filter selected, the user will be able to select the values included for the filter and edit the filter caption. For example, if the user only wanted one case type to be present in the report, they select the "Case Type" hyperlink in the blue section at the top of the page and select the desired case type.

1. On the main page of the report, select a **bolded hyperlink** (filter) in the blue box above the cases listed.

   The Edit Filter modal will appear.

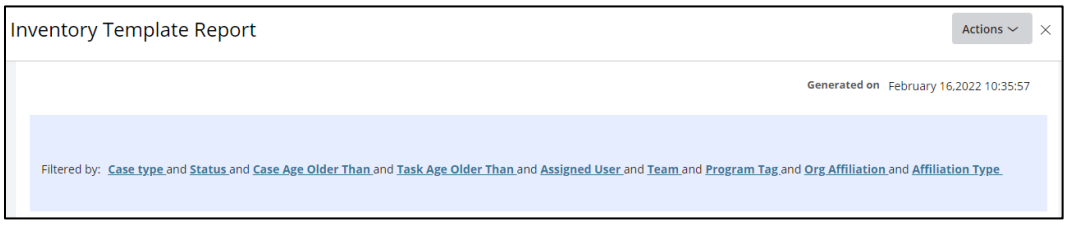


Figure 11-2: Report View - Selectable Filter Bar

2. Choose **Select Values** to bring up a modal to select filters for the field in the Report.

   Note: This option appears when **Case Type** is the selected filter. For other filters, you may input or select multiple values.

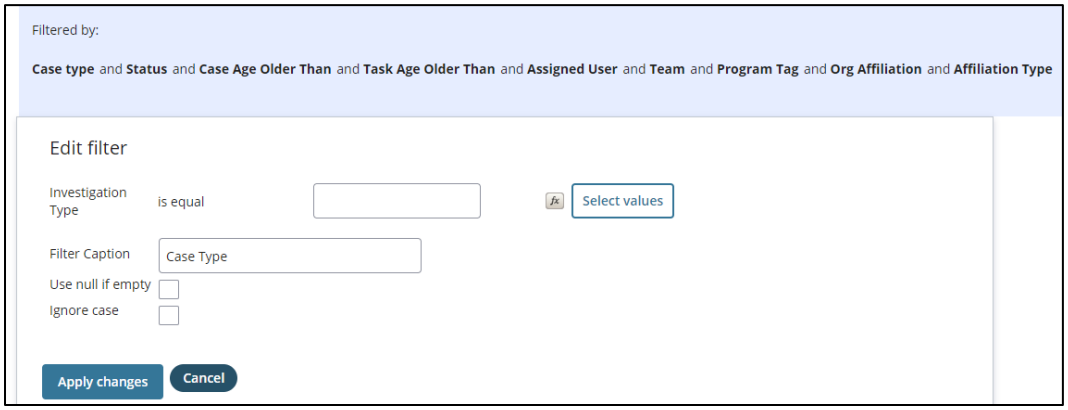


Figure 11-3: Report View - Edit Filter

3. Optionally check the boxes **Use null if empty** and **Ignore case** as needed.
   - **Use null if empty** – this only applies when a field value is blank or missing. If checked, the blank field will still be included in the report.
   - **Ignore case** – if checked, the field will not be case sensitive.
4. Select **Apply Changes** to update the filter. This will take the user back to the updated report.

Reports with Editable Filter Display

Certain reports will contain editable filter selections in a banner at the top of the report. The filter fields will vary based on the report type. Depending on the report, you can either enter in values for the filter field or select from a drop-down.

1. On the main page of the report, locate the field you need to filter by. From the filter drop-down, select a **value**.
2. Once all desired filters are selected, select **Apply Filters**.

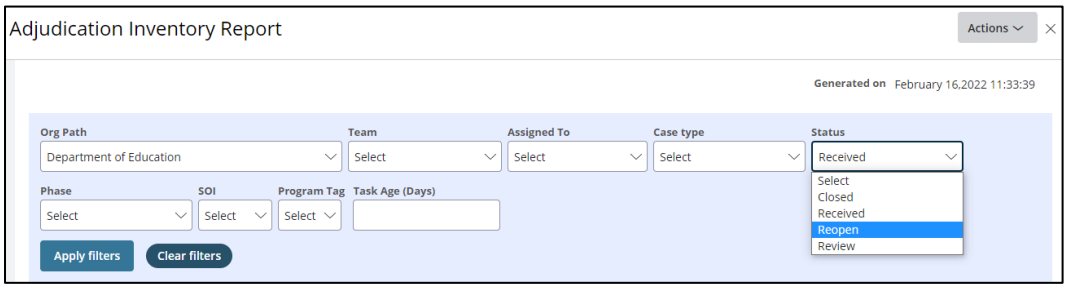


Figure 11-4: Report View - Editable Filter Bar

The filtered report will display below.

11.4 Report Actions

Every report has a set of standard actions that can be accessed from the actions drop-down within each report:

- **Refresh** – Refresh the current page.
- **Save as** – This will save allow you to save the current report view and filters as a new custom report only for your user. You will be prompted to enter a Report Name and Description and select a Report Category.
- **Report details** – A pop-up will appear with the details of the selected report: report description, report category, and report key.
- **Summarize** – This will allow you to summarize and/or sort the report based on the values for each field. This action is only available on certain reports. If both Summarize and List are available in a report's actions, they can be used to switch between the summarize and list views.
- **List** – Restructure the table and data appearance to assist in navigation and filtering. This action is only available on certain reports. If both Summarize and List are available in a report's actions, they can be used to switch between the summarize and list views.
- **Export to PDF** –Download a PDF version of the report. Once selected, the file will download automatically.

  Note: This action will not be available without the **Operations Manager** role.
- **Export to Excel** –Download an excel spreadsheet version of the report. Once selected, the file will download automatically.

  Note: This action will not be available without the **Operations Manager** role.

11.5 Report Builder

Users with the **Reports Manager** role are able to create a configurable report using the Report Builder on the left navigation menu. For users with the Reports Manager role, the Report Builder tab will house all functionality related to reporting. Users without the Reports Manager role but with other roles that have reports capabilities will instead have access to a **Reports** tab on the left navigation menu. See the previous reporting sections for more information on the **Reports** tab.

When navigating to Report Builder, you will first see the **My reports** tab which displays all reports you have configured. Selecting the **All reports** tab will display all reports you have access to. For more information on actions available for existing reports, see Report Actions.

11.5.1 CREATING A REPORT

Reports Managers can currently create reports for subject-related data.

1. From the left navigation menu, select **Report Builder**.
2. On the top right, select **New Report**.

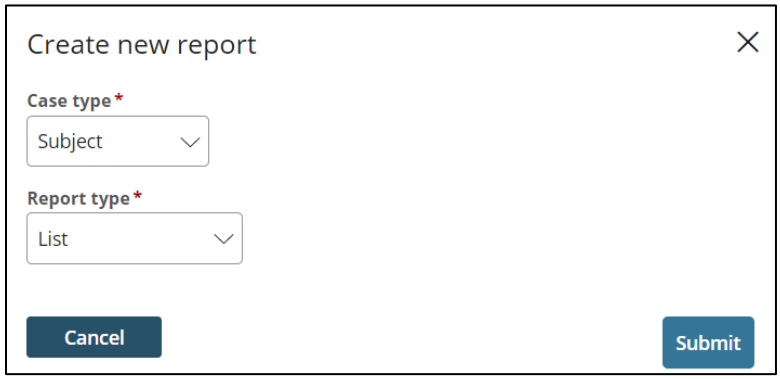


Figure 11-5: Create New Report Pop-up

3. From the **Case type** drop-down, select a **Case type**.

   Note: Currently the system supports **Subject** or **Subject Search** as the case type options.
4. From the **Report type** drop-down, select a **Report type**.

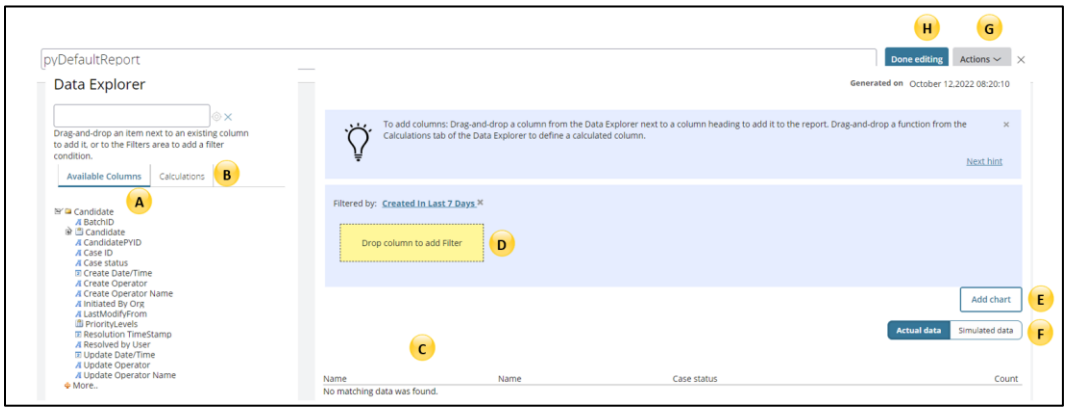


Figure 11-6: Report Configuration Screen

A. Available Columns – list of columns that can be added to the report or to the report filter conditions

B. Calculations – does not apply to subject-related data reports.

C. Columns – displays the columns that will be included in the report. Reports Managers can drag and drop columns here to add them to the report. Certain columns will be prepopulated in this area, but they can be removed.

D. Filters – Reports Managers can drop columns or calculations to this location to act as filters for the report

E. Add chart – this will open a model that allows you to configure a chart for your report using the configured columns

F. Actual data/Simulated data – toggle display between actual report data and simulated report data, if applicable

G. Actions – available actions for the report: Save as, Report details, Sort, Summarize

H. Done Editing – to save report and close out of editing an existing report.

5. Items that can be added to the report will be displayed in the **Data Explorer** section. You are able to drag items to add as a **Column** (C in Diagram) or **Filter** (D in Diagram).

   Note: For adding filters, see the following section Report Filter Configuration for steps on filter configuration.

6. Select **Done editing**.

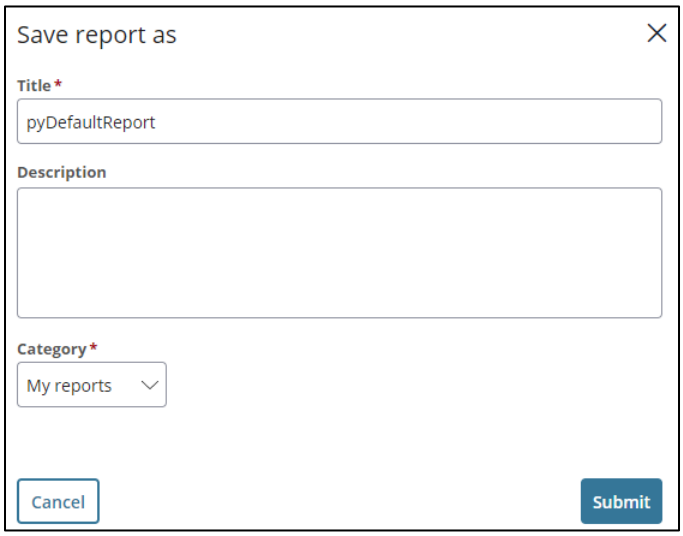


Figure 11-7: Save Report Pop-up

7. Enter a **Title**.
8. Optionally enter a **Description**.
9. From the **Category** drop-down, select a **Category**.

Note: Currently, **My Reports** is the single default category option.

10. Select **Submit**.

The report will appear on the **My reports** tab of the **Report Builder** page.

11.5.2 REPORT FILTER CONFIGURATION

The Reports Manager is able to further modify filters as they are added to the report.

1. After selecting **New report**, from the **Available Columns** list, select a **Column Field**.
2. Drag the column fields name to the **Add Filter** box.

Figure 11-8: Drag and Drop Filter Area

You will be brought to an **Edit Filter** modal. Only certain column field options are able to be modified. If no further modification is necessary, continue to step 8 to add the filter to the report.

3. From the drop-down, select the desired value comparison.
4. Choose **Select Values** to select a value to compare the field against.
5. Optionally enter a **Filter caption**.
6. Select the **use null if empty** checkbox to apply the filter even when report entries are missing a value for this field.
7. Select the **Ignore case** checkbox to ignore capitalization for application of this filter on report entries.

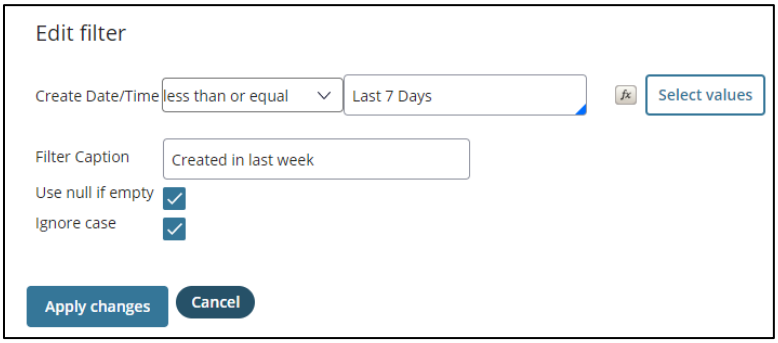


Figure 11-9: Edit Filter Screen

Note: The screenshot above is only an example of a report filter configuration. Depending on the column field used as a filter, some or all of these fields may not be necessary.

8. Select **Apply changes**.

11.5.3 REPORT COLUMN ACTIONS

When creating or editing a report, the Reports Manager has available actions for further modify the column display.

1. On the desired report column, select the **down arrow** next to the column name.

   A list of actions will appear.

2. Select an **Action**.

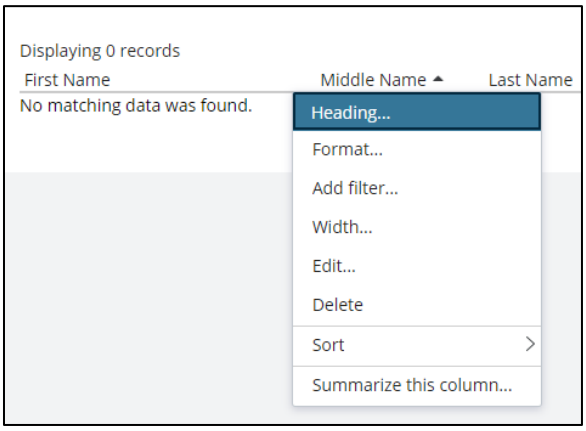


Figure 11-10: Report Column Actions

12 Team Management

A **Team** is a group of users within a main or sub org, that is created for internal organizational workflow management.

Teams are not applicable to SSC, Review, Authorize, and FSO Organization types.

12.1 Team Structure

This view of the **Teams** tab includes the list of Teams that have been created. The **Team Structure Manager** role can create Teams and add users to the team. For example, the Team Structure Manager for an Org can create "Junior Adjudicators" and "Senior Adjudicators" within an Organization, then add individuals from their org to each team.

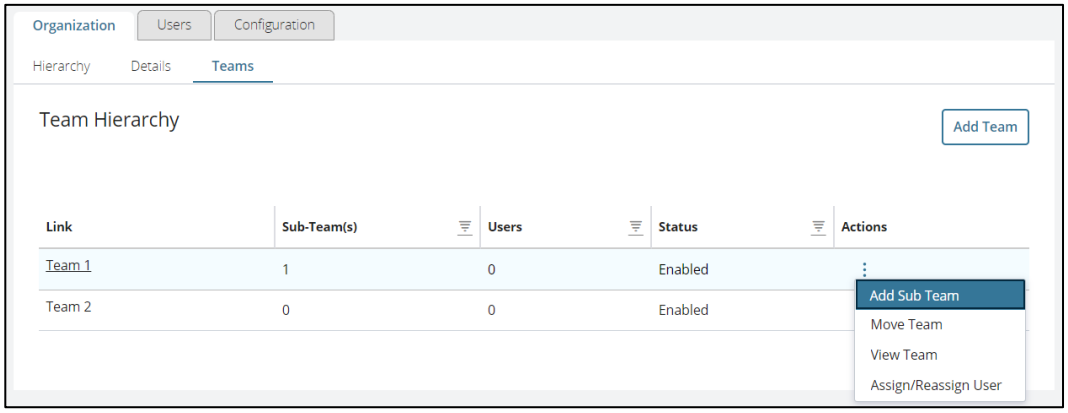


Figure 12-1: Team Hierarchy

1. From the left navigation menu, select **Org Management**.
2. Under the **Organization** tab, select the **Teams** tab.
3. Teams are visible under the **Teams Hierarchy** section. Select the **Team Name Hyperlink** to view a desired team's sub-teams.
4. To take further actions, under the **Actions** column, select the **ellipses**. See the following sections for add, view, or edit teams.

   Note: As an Organization Manager or Team Structure Manager, you can move the teams within the hierarchy as needed by selecting **Move Team**. Please refer to Team Migration section for further details.

12.2 Managing a Team

To add a Team:

1. From the left navigation menu, select **Org Management**.
2. Under the **Organization** tab, select the **Teams** subtab.

There are two ways to add a new team:

- Select the **Add Team** button. This will automatically add the team directly to the organization.
- Select the **ellipses** for the desired team and select **Add Sub Team**.

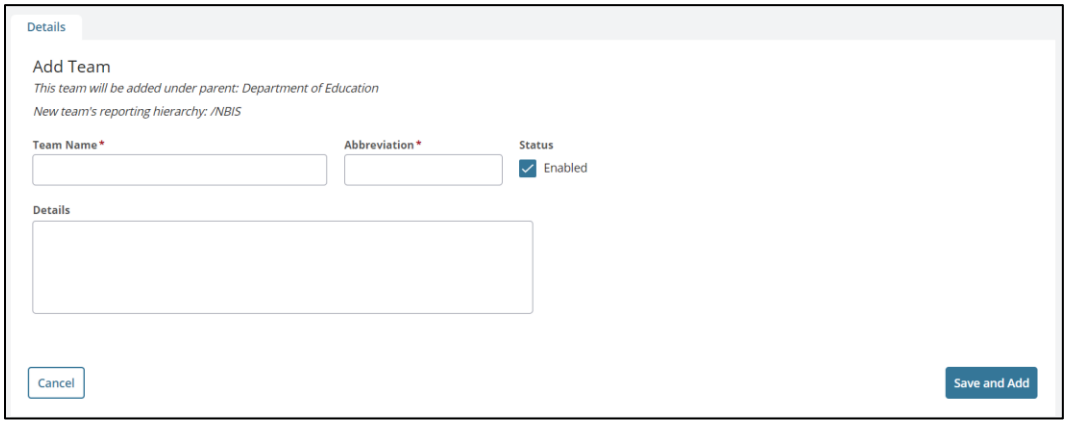


Figure 12-2: Add a Team

3. Complete the required fields and select **Save & Add** to create the new team.

To view a Team's Details:

4. Under the **Actions** column, select the **ellipses** for the desired team.

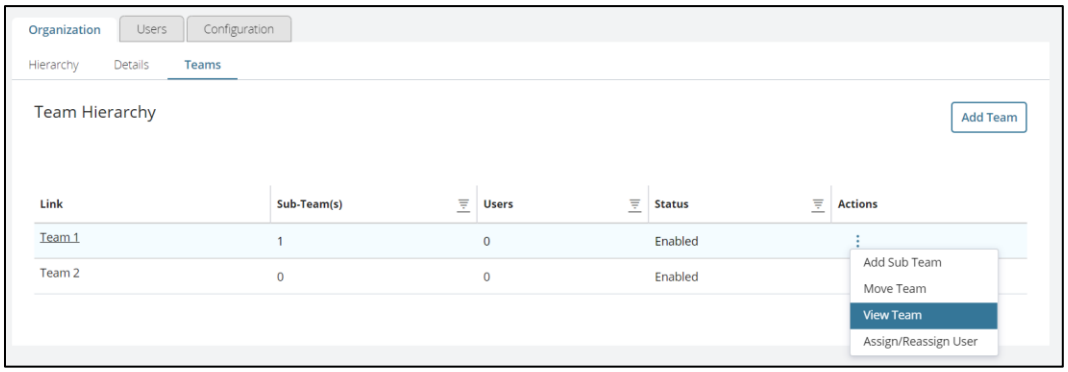


Figure 12-3: View Team Action

5. Select **View Team.**

To edit a Team's Details:

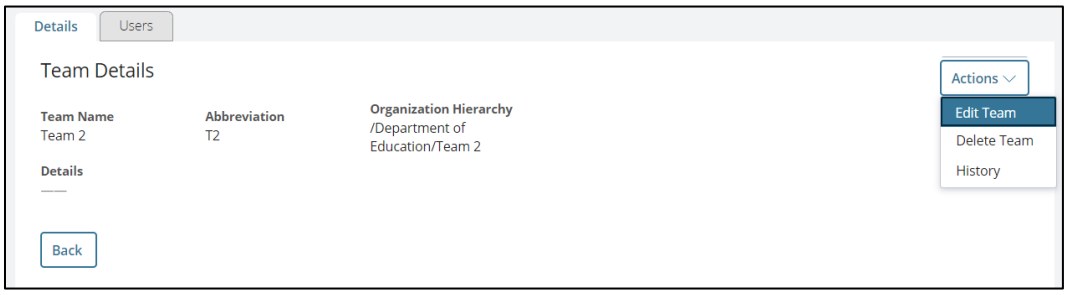


Figure 12-4: Edit Team Action

6. From the **Actions** drop-down, select **Edit Team** to modify the team's information.

   Note: You can also see the team's history of changes by selecting **History.**

7. Select **Save**.

   Note: Select the **Back** button if at any point you would like to return to the list of teams**.**

To delete a Team:

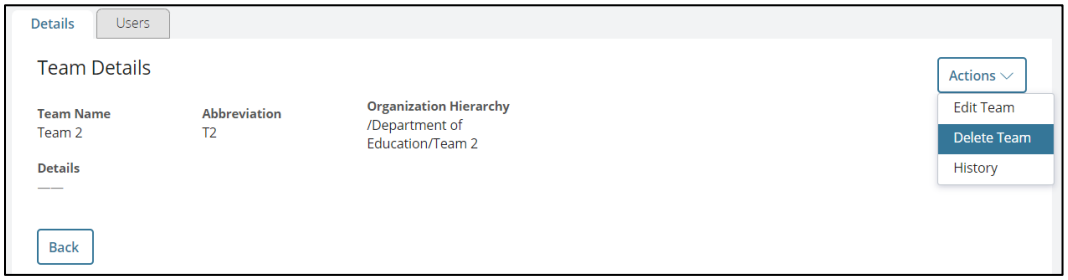


Figure 12-5: Delete Team Action

8. From the **Actions** drop-down, select **Delete Team**.

   Note: As the Team Structure Manager, in the team detail context, the Delete Team button can delete a Team. You can only delete a Team once all users are removed from the Team, and all sub-teams under the Team are removed. The Delete Team button should only appear once all the conditions to delete a Team have been met. You will be prompted to confirm the team deletion.

12.3 Managing a Team's Users

The **Team Structure Manager** can assign/reassign users to an existing team. The **Team Manager** can only see a read-only view of the team hierarchy and the organization details.

Note: Team Managers can only modify a user's capabilities, see User Management for more information.

To add an Existing User to a Team:

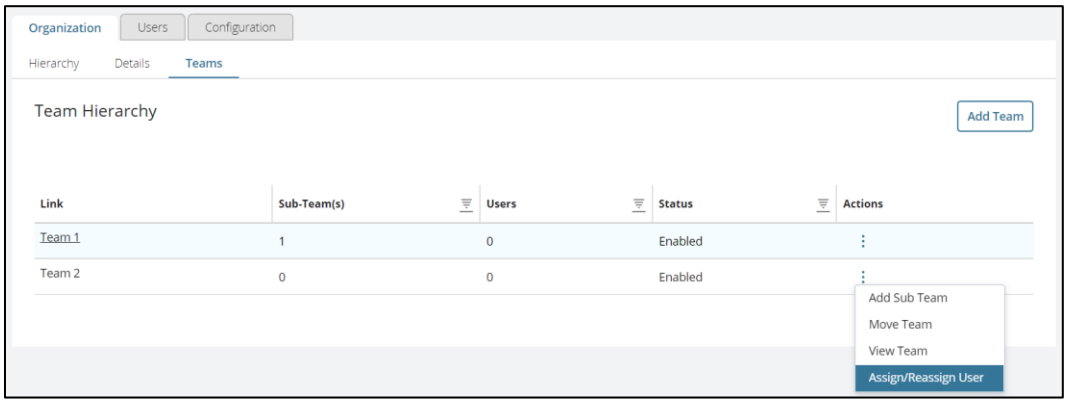


Figure 12-6: Assign/Reassign User Action

1. From the left navigation menu, select **Org Management**.
2. Under the **Organization** tab, select the **Teams** subtab.

There are two ways to add a new team:

- Under the **Actions** column, select the **ellipses** for the desired team and select **Assign/Reassign User**.
- Under the **Actions** column, select the **ellipses** for the desired team and select **View Team**. Select the **Users** tab and select **Assign/Reassign User**.

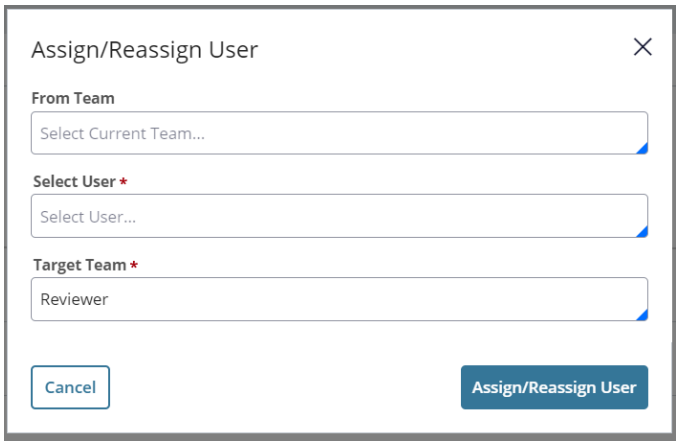


Figure 12-7: Assign/Reassign User

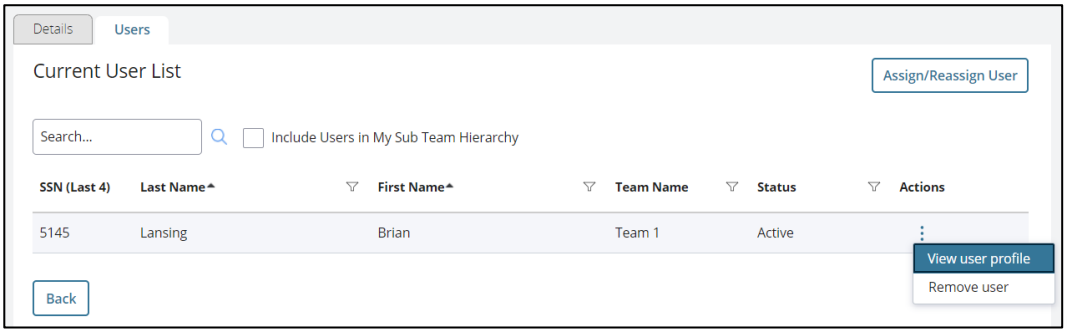
1. Select a **User** and a **Target Team**.

   You can select a different team in your org to select users from. Users in the selected team will be populated in the **Select User** field. If you do not select a team, the list of users will be the ones not assigned to a team in your org. You should see the number of users in the **Users** column increase by one.

2. Select **Assign/Reassign User** to add a user to the team.

To edit a Team's Users:

5. In the team's detail page, select the **Users** tab.



u

Figure 12-8: User List

6. Under the **Actions** column, select the **ellipses** for the specific user and select **View User Profile**.
7. The Team Manager can only update the capabilities for users at the Team level.
8. Make all necessary changes and select **Save**.

12.4 Team Migration

Team Structure Managers can move teams throughout the team's hierarchy, but teams cannot be moved outside of their organization.

1. From the left navigation menu, select **Org Management**.
2. Under the **Organization** tab, select the **Teams** subtab.
3. Under the **Actions** column, select the **ellipses**. Select **Move Team** for the team you want to move.

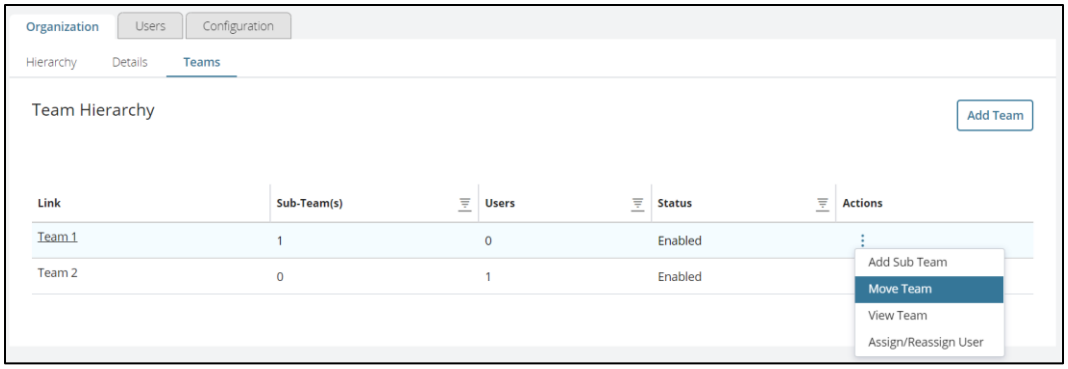


Figure 12-9: Move Team Action

4. Choose the receiving team and select **Move Here**.

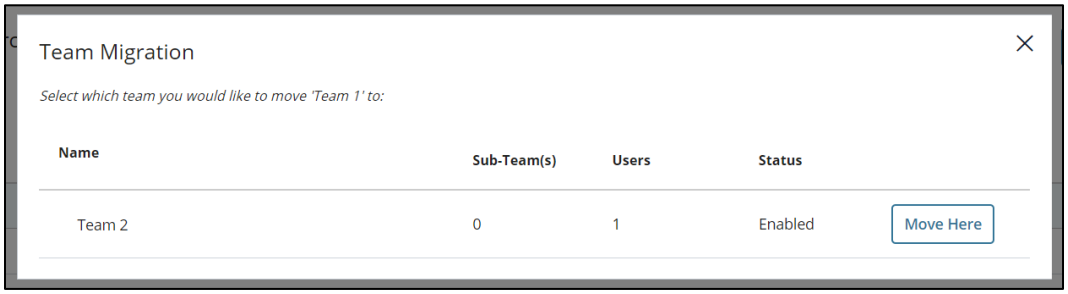


Figure 12-10: Team Migration

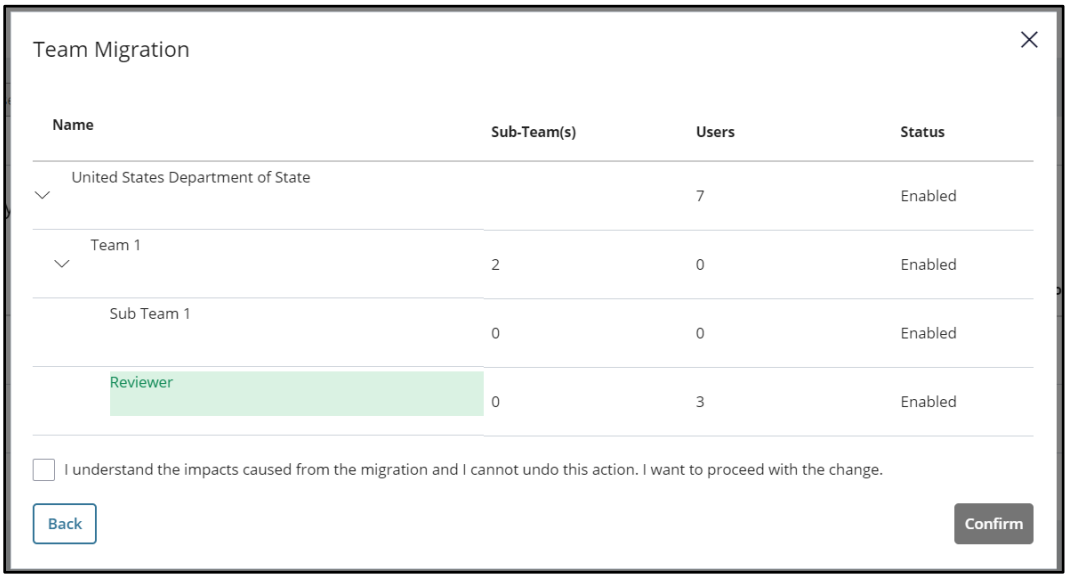


Figure 12-11: Team Migration Preview

Note: The confirmation page displays the preview of the new hierarchy after confirming the team migration.

5. Select the **checkbox,** confirming the migration.
6. Select **Confirm** to proceed with the migration.

12.5 View the Team's Worklist

The **Team Manager** has access to the **My Team's Work** tab. In this tab, you can view a list of all tasks assigned to users in your team(s).

Note: If you have the **Team Manager** role and are not assigned to a specific team, then you will not see any cases in the My Team's Work tab.

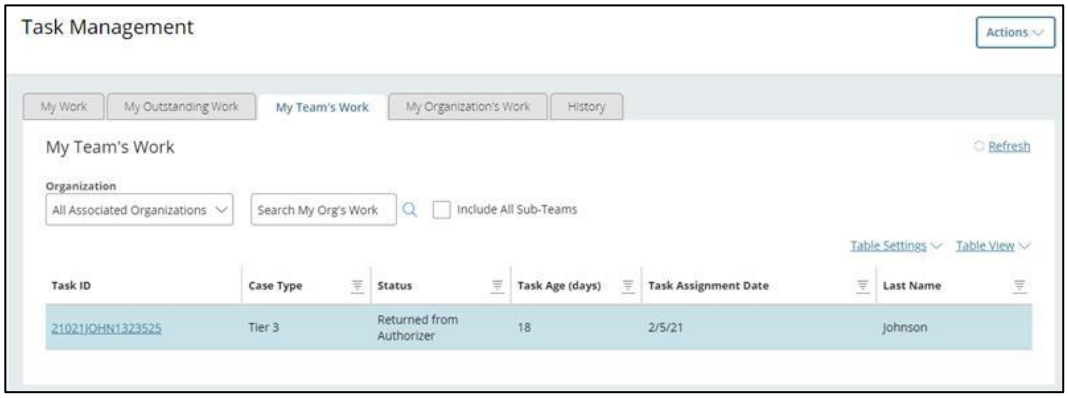


Figure 12-12: Task Management - My Team's Work

1. From the left navigation menu, select **Task Management**, and then select **My Team's Work**.
2. Select the **Organization** drop-down to choose which organization's team's tasks you want to view.
3. Note: Only organizations where you are explicitly a **Team Manager** will appear in the drop-down. You can also view all associated tasks for teams within that hierarchy if desired by checking **Include All Sub-Teams**.

13 Appendix

13.1 Acronyms, Abbreviations, and Definitions

Standard Forms

Table 13-1: Standard Form Descriptions

Form	Description
SF-85	Standard Form Number 85 – Questionnaire for Non-Sensitive Positions.
SF-85P	Standard Form Number 85P – Questionnaire for Public Trust Positions.
SF-85P-S	Standard Form Number 85P-S – Supplemental Questionnaire for Selected Positions.
SF-86	Standard Form Number 86 – The OPM's Questionnaire for National Security Positions (QSP).
SF-87	Standard Form Number 87- The fingerprint card

Software

Table 13-2: Software Terminology Definitions

Term	Description
Central Verification System (CVS)	The Central Verification System (CVS) is used to determine if there is an existing adjudication or investigation that meets the current need. It is the primary tool for facilitating reciprocal decisions, as required by Executive Orders, regulations, and policies. CVS contains information on security clearance, suitability, fitness, and Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) credentialing determinations.
Defense Information System for Security (DISS)	DISS is an enterprise-wide solution for personnel security, suitability, and credentialing management for DoD military, civilian, and contractors. It is a web-based application, a platform providing secure communications between adjudicators, security officers, and components, allowing users to request, record, document, and identify personnel security actions.
eApp	e-App is a secure web-based automated system which facilitates timely, accurate processing of investigation requests to DCSA. Agencies initiate individuals into the system, the system then collects data from the individual based on the appropriate investigative questionnaire (SF 85, SF 85P, SF 85P-S, or SF 86), and finally agencies review and submit the investigative questionnaire electronically to DCSA or another Investigative Service Provider (ISP).

Term	Description
e-QIP	e-QIP is a web-based automated system that was designed to facilitate the processing of standard investigative forms used by DCSA and other Investigation Service Providers (ISP) when conducting background investigations for Federal security, suitability, fitness and credentialing purposes. e-QIP allows the user to electronically enter, update and transmit their personal investigative data over a secure internet connection to a requesting agency.
Personnel Information Processing System (PIPS)	The system previously used to act as a repository containing background investigation records of Federal employees, military personnel, and contractors.
Position Designation Automated Tool (PDT)	The PDT is an interactive tool on the OPM website. The process determines, through the evaluation of national security and suitability requirements, what type of investigation is required and the depth that an individual is screened for a position. In order to ensure a systematic, dependable, and uniform method of determining position designations, OPM provides the Position Designation Automated Tool (PDT) for those individuals within agencies charged with position designation responsibilities.

Case Types

Table 13-3: Case Type Descriptions

Term	Description
Tier 1	Investigation required for positions designated as low risk, non-sensitive, and for physical and/or logical access, pursuant to Federal Information Processing Standards Publication 201 and Homeland Security Presidential Directive-12, using Standard Form 85, or its successor form.
Tier 2	Investigation required for non-sensitive positions designated as moderate risk public trust, using Standard Form 85P, or its successor form.
Tier 3	Investigation required for positions designated as non-critical sensitive, and/or requiring Determination for "L" access or access to Confidential or Secret information. This is the lowest level of investigation acceptable for access to classified information, using Standard Form 86, or its successor form. Requires a 10-year reinvestigation. Formerly known as National Agency Check, Local Agency Check and Credit Check.
Tier 3R	T3R is the reinvestigation product required for the same Tier 3 position.

Term	Description
Tier 4	Investigation required for non-sensitive positions designated as high-risk public trust, using Standard Form 85P, or its successor form.
Tier 4R	The reinvestigation product required for the same Tier 4 positions.
Tier 5	Investigation required for positions designated as critical sensitive, special sensitive, and/or requiring Determination for "Q" access or access to Top Secret or Sensitive Compartmented Information (SCI), using Standard Form 86, or its successor form. Requires a 5-yr. reinvestigation. Formerly known as Single Scope Background.
Tier 5R	The reinvestigation product required for the same Tier 5 positions.
National Agency Check (NAC)	Spouse/Cohabitant National Agency Check
Special Agreement Check (SAC)	Fingerprint Special Agreement Checks

Government Abbreviations

Table 13-4: Government Abbreviations and Definitions

Term	Description
Business Event Type Code (BETC)	This is up to an eight-digit alphanumeric code that indicates the type of activity being reported (payments, collections, etc.). Some agencies are using DISB if receiving services and COLL if performing services. BETC determines the transaction effect on the TAS Fund Balance with Treasury. BETC replaces transaction codes and subclasses, but at a more detailed level.
Extra Coverage Codes (EC)	Standard Form 85, 85P and 86 - Extra coverage codes are used to request information or processing beyond the normal scope of the investigation. Agencies must request extra coverage when additional information is needed to help determine a person's qualifications, suitability, or security for a particular position. Certain codes require an agreement with DCSA, and some incur additional fees. This is an optional field.
Federal Investigations Processing Center Codes (FIPC)	Codes that indicate special processing needs for an investigation request.
Intra-Governmental Payment and Collection (IPAC)	An Agency Location Code (ALC) is assigned to your agency by the U.S. Department of Treasury. The IPAC System provides a standardized interagency fund transfer mechanism for Federal Program Agencies (FPAs). IPAC facilitates the intra-governmental transfer of funds, with descriptive data from one FPA to another.
Investigative Service Provider (ISP)	A governmental organization that is actively involved in conducting investigations.
Security Office Identifier (SOI)	An agency's Security Office is responsible for receiving completed investigation reports from DCSA, controlling the agency's cases, and making the suitability and security determinations on individuals being investigated for employment. Each Security Office is issued a unique alphanumeric four-character identifier from DCSA, the Security Office Identifier (SOI), which is used to identify the appropriate agency official who will receive case results, data, or other information from DCSA.
Submitting Office Number (SON)	DCSA assigns a unique four-character alphanumeric code, known as the Submitting Office Number (SON), to each office that requests investigations from DCSA. The SON identifies the office that initiates the investigation and is recorded in the appropriate Order Form (Agency Use Block) of the SF 85, SF 85P, SF 85P-S, and SF 86.

Term	Description
Business Event Type Code (BETC)	This is up to an eight-digit alphanumeric code that indicates the type of activity being reported (payments, collections, etc.). Some agencies are using DISB if receiving services and COLL if performing services. BETC determines the transaction effect on the TAS Fund Balance with Treasury. BETC replaces transaction codes and subclasses, but at a more detailed level.
Treasury Account Symbol (TAS)	A financial code, assigned by the Department of the Treasury, comprised of many separate, component pieces/ sub-fields* totaling 27 alphanumeric characters; however, not all sub-fields apply to each fund account. Among other things, the financial code identifies the agency, the period of availability of funds, and a specific fund account.

Adjudication and Vetting Terminology

Table 13-5: Adjudication and Vetting Terms and Definitions

Term	Description
Access	The ability or opportunity to obtain knowledge of classified or sensitive information.
Additional Considerations	Determine the extent to which an issue makes the applicant unsuitable or unfit.
Adjudication Factors	Derogatory information evaluated in review of background information.
Adjudication Guidelines	A set of rules/criteria used to determine a subject's Determination to obtain access to classified information.
Compartments	Sensitive Compartmented Information (SCI) is divided into control systems, which are further subdivided into compartments and sub-compartments. Compartments protect national intelligence sources, methods, or analytical processes and measures are additional control systems used to protect intelligence sources and methods or analytical procedures.
Determination	The type of clearance for which a subject may be considered; or the determination assigned for a type of clearance, (e.g. Secret, Interim Declined, Favorable).

Term	Description
Disqualifier	Undesirable quality that renders a subject unqualified for a privilege or clearance.
DISS File	A file containing the adjudicative result data that is sent to the Defense Information System for Security (DISS) of record.
Exceptions	Exceptions identify conditions that exist and may be either monitored or unmonitored (e.g. monitored conditions include providing financial credit bureau reports on a quarterly basis; unmonitored conditions).
Homeland Security Presidential Directive 12 (HSPD-12)	Directive to mandate a federal standard for secure and reliable forms of identification. US policy to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).
Issue Event	The event that occurred with a subject, which could negatively impact their security clearance status.
Issue Tag	The qualifying language NBIS uses to identify what type of issue(s) occurred within an issue event for a subject.
Mitigators	Explanations, reasons, qualities, or actions that lessen the gravity of the disqualifier.
National Security Guidelines	Single common criteria for all covered individuals (e.g., U. S. Government civilian and military personnel, consultants, contractors, etc.) who require individual or continued Determination for access to classified information or Determination to hold a sensitive position.
Public Trust	Positions at high and moderate risk levels.
Suitability	An indication of a subject's ability to perform a job; typically based on experience or education.
Suitability Guidelines	Guidelines that identify character traits and conduct, and are sufficient to decide whether employment or continued employment would protect the integrity or promote efficiency of the service of a covered applicant, appointee, and employees.

NBIS Terminology

Table 13-6: NBIS Terms and Definitions

Term	Description
Affiliate Subject	A user must have an affiliation to an organization. From the Subject Summary, if there are no active relationships with a user's Organization, an affiliation must be created.
Agency Use Block (AUB)	A section within the legacy e-QIP system that contains information pertinent to a case's order form details, such as financial details.
Assignment Method	Controls how tasks will be assigned to users within the NBIS system or within their organization. The two assignment method options are Manually Assign or Automatic/ Manual Assignment.
Assignment Rules	Assignment Rules control the prioritization of how cases are assigned to users in the system based on certain case and user attributes.
Assignment Threshold	Defines the number of assignments a user owns before the system automatically assigns additional tasks.
Case ID	The formal identification number for the case.
Case Phase	The Phase is the highest-level grouping to describe where the case is at in the overall workflow for the personnel vetting process. It communicates to users the type of work currently being done on the case. Examples of phases include Initiation, Review, Authorize, Investigation, Continuous Vetting, Adjudication, etc.
Case Progression Engine	The progression engine pushes the case forward to the next status based on business rules of how many CV Alerts or Leads with specific attributes have been closed.
Case Status	The Status of the case communicates the specific part of the workflow the case is at within a Phase. It is a more granular indication of the case progress compared to the phase.
Case Type	Refers to the type of checks and investigation tiers available to select. Can select from the options provided for case types. Selecting "Any" will select all case types.
Expires In	How many days until the case automatically expires, which is 120 days.

Term	Description
Form Routing	Form Routing is the configuration of the workflow process for the Initiation, Review, and Authorize phase. The organization will select which organizations they want the case to be routed to in each phase.
Form Status	The status that the SF is currently in.
Hierarchy	The technical reporting structure under which an Organization and its Sub-Organizations are arranged and connected in a network tree with varying levels.
Hold Authorizer	The Authorizer can place the case request on hold by selecting Hold Authorization from the Actions drop-down, then leaving a comment explaining the reason for the hold.
Manually Assign	Manually assign tasks to specific users within an organization.
Order Form	The Order Form (previously known as the AUB), is the group of fields needed to complete the Agency Request. In NBIS, the Order Form in used in the Initiation, Review, and Authorize Phases.
Org Relationship	Organizations can establish relationships with each other when one organization is completing the work within a phase for another organization.
Organization	A government entity and/or an investigation service provider that is used to initiate requests, receive requests, conduct investigations, and adjudicate cases.
Organization Affiliation	Serves as a designator for Organizations to identify themselves as a federal or contractor Organization.
Organization Context	Organization Context refers to when you are in the Org Management tab, you are viewing all the data within that page in the context of a specific organization. It does not necessarily apply to all organizations you are in.
Organization Functions	Activities that have been identified as requirements for the Organization to perform and successfully execute the Personnel Vetting (PV) Process for each specific mission area.
Organization Roles	Based on the Organization functions, users within the Organization are granted specific user privileges/permissions to execute Org functions and activities.
Organization Type	Based on an Organization's identified mission areas, the Org Type is selected to support the implementation of those specific functions.

Term	Description
Organization Level	Identifies the placement of an Org/Sub-org that is aligned vertically within a hierarchy for executing Org functions.
Owning Organization	This is the organization that is actively providing the subject with a paycheck. They are responsible for maintaining the subject's Determination.
Persona	A user can have multiple personas within their profile. An example of when a persona might be used is when a user needs permissions for their federal and contractor profiles.
Private Program Tag	Only used by the org that created it. Other orgs cannot request to join the tag.
Program Tags	Used to label and place restrictions on cases to allow certain users to work on, view, or allow a case to appear on a list.
Program Tag Library	The Program Tag Library beneath the organization program tags contains all other program tags that are used by other organizations in the Protected or Public visibility. This is where the Program Tag Manager can become Tag Modifiers and owners of the other Program Tags.
Program Tag Modifier	Tag Modifiers have access to Program Tags, they can use a tag and can modify or edit the configuration but cannot edit Program Tag details, approve requests, or reject requests.
Program Tag Owner	A Program Tag Owner can use a tag, edit Program Tag configurations, edit Program Tag details, and approve or reject other organizations from gaining access to their organizations Program Tags.
Program Tag Permission Type	Permission Type specifies the current organization's permissions. There are two Permission Types associated with Program Tags: (1) Tag Owner and (2) Tag Modifier.
Program Tag Restrictions	Tag Restrictions determine if the Program Tag can restrict User's access to a case when the Subject is associated with the Program Tag. The different Tag Restrictions are (1) No Restrictions, (2) Work on the Case, (3) Open the Case and (4) View the Subject.
Program Tag Visibility	Determines if another organization can become a part of the tag and use it. Visibility can be set to Private, Protected, or Public.

Term	Description
Protected Program Tag	Allows other orgs to make a request to become a Tag Modifier or a Tag Owner. When in Protected status, users may either request Tag Modifier Permission or request Tag Owner Permission. When requesting, users will be required to provide an explanation for justification of the request and must be approved by the owning organization.
Public Program Tag	Allows other orgs to join the tag as a Tag Modifier without going through a request process. Orgs must still request to be a Tag Owner. When set to public status, users may become an Owner by selecting Request Tag Owner Permission, then users can make edits and approve or deny access requests.
Release Submission	Once the Authorizer believes that all fields are correct and the case should proceed, the case can be released and authorize the funds for the investigation. The Release Submission activity completes the Authorizer Workflow on the case.
Request Tag Owner Permission	When users Request Tag Owner Permission, users will be required to provide an explanation for justification of the request and must be approved by the owning organization.
Restrictive and Non-Restrictive Tags	When added to subjects, tags can be Restrictive or Non-Restrictive. Cases with Non-Restrictive tags can be worked on by anyone regardless of their capability to work on the case. All other choices (See the case lists, Open the case, Work on the case) categorizes that tag as restrictive for that organization. For restrictive tags, a user's capability to work on that case will be checked. Restrictive tags are the ones that the user must have in their user profiles/assignments in order to be able to see, work on or open a case
Routing Details	Users will create/select Workflow Type Templates for the routing of the eApp.
Service Catalog	Service Catalog requests are configurable case types to provide services for internal and external organizations.
Servicing Organization	An organization may have a servicing relationship with the subject if they need to be notified of a change in a person's Determination status or if they need to update their record.
Sponsoring Agency	A government department or agency that is sponsoring the subject's investigation request.
SSC	Security, Suitability, and Credentialing. In NBIS, SSC is an available Organization Type that gives the organization access to the Subject Management function.

Term	Description
Status	Reveals whether a user assignment template is enabled or disabled. If enabled is not checked, the user assignment template will not be available.
Sub/Child Organization	The building blocks of a hierarchy; Sub-orgs serve as the subordinate Organization to the parent Organization.
Subject	An individual who is authorized to fill out the Standard Forms via the e-App system.
Team	A Team is a group of users within an organization, that is mainly created for organizational/management purposes and is not public facing. Example would be Army (Primary Organization) - Army Brigade (Sub-Organization) - Group A (Team within either Army or Army Brigade).
User	The different government or industry employees that will be utilizing the NBIS System.
User Assignments	Manages the capabilities users have access to and can perform within the context of an organization. User assignments are what allows a case with a particular set of attributes to be routed to a user.
User Assignment Capabilities	User capabilities tell the system the types of cases and amount of work a user can take on. They are used by the assignment engine to determine which cases to assign to which users.
User Capacity	Sets the maximum number of cases a user may be automatically assigned.
User Assignment Templates	Users can create standard templates to use when completing users' assignment capabilities in their user profile for a more efficient way of filling out that information. User Assignments are what allow a user to work on cases with certain attributes.
User Level	User Levels are used to assign work to users based on their skill level. Examples could include Junior or Senior.
Workbasket	The workbasket refers to a task or case in an organization that is not assigned to a specific user yet. In Task Management, the My Team's Work or My Org's Work is equivalent to the workbasket.

Term	Description
Workflow Builder Actions	Actions are the driving component of the workflow. Actions can be available within multiple Statuses in the workflow; however, an Action can only be configured to end in a single Status. Actions can have one or multiple associated Modules. Action naming and configuration should communicate to the user what will occur when the Action is performed.
Workflow Status	The stage within a workflow that an assignment can move to and from. Statuses allow users to track case movement within a single workflow configured by their organization. Each status represents a stage within the workflow that can be associated with actions that will be available to a user when the case is active.
Worklist	The worklist refers to a task or case being assigned directly to a specific user. In Task Management, the My Work tab is equivalent to the user's worklist.

13.2 Organization Levels

Group – the group flag represents Organization levels that are on the top of their hierarchy and can only be assigned to an organization by the On-Boarding Manager user role.

CVP Flag - This Flag determines if an organization level is eligible for DoD Continuous Vetting Program.

Table 13-7: Organization Levels

Organization Level Name	Description	Example	Group	CVP flag
Branch of Government		Executive Branch	X	
Organization	The highest point of responsibility in the reporting structure of the hierarchy. Match to cabinet level department	departmental agency; independent agency; non-profit agency; law enforcement agency, DoD	X	X
Component Organization	Large, potentially independent, parts of an agency that reports directly to the head organization and oversees smaller offices	sub-agency; component; board; committee; commission; administration; center; facility		
Reporting Office	Office within the component or head organization that fulfills a specific hierarchical function and may or may not oversee other, smaller reporting offices	office; division; branch; directorate; bureau; program; unit; department		
Regional Offices	Office that carries out organizational and mission-related functions for a specific geography within the scope of a Reporting Office, Component Organization, or Organization.	field office; regional office; district office; processing center		
Functional Center	Geographically dispersed agency component that carries out mission-related activities.	laboratory; research center; airport; border station; school/university; hospital; consulate; national park		X
Military Headquarters	The headquarters-level for military branches	office of the secretary; divisions; supporting establishments	X	X
Military Operational Command	Large geographical or functional command which includes a collection of units and formations under the control of a single officer.	combat command; combatant commands; MAJCOMs		

Organization Level Name	Description	Example	Group	CVP flag
Military Installation	A facility that is controlled by or primarily supports DoD's activities. An installation may consist of one or more sites, may house equipment or personnel, and may facilitate training or other military operations.	military base; field agency	x	
Military Field Units	Tactical military units located at home or abroad and either combat, combat-support or non-combat in capability. These units may be housed inside military installations.	division; brigade; regiment; battalion		
Industry - Head Facility	The highest point of responsibility in the reporting structure of the hierarchy, the centralizing security office for the industry partner.	Accenture	x	
Industry - Component Facility	Other cleared facilities that process investigations within the hierarchy of an industry partner.	Accenture Federal Services		
Grouping	Used to gather multiple entities under a common umbrella			
Personnel Vetting Unit	Organizations that perform Personnel Vetting services in the US Government		X	
Field Operating Activity	DOD Level organization that does not have agency designation.		X	
Agency	Organizations with an agency designation that report up to another level of the government before reaching up to the presidential level.		X	
Bureau	A sub-division of an executive department in the US Government.		X	

Organization Level Name	Description	Example	Group	CVP flag
Cabinet Level Department	Cabinet Level Organizations in the US Government.	Treasury, Department of Defense	X	
Independent Agency	Organizations that report to the president directly and not through another department level organization.		X	
SSC Office	Any office preforming national security, suitability, or credentialing work.			

13.3 Role Matrix

Last Update: 01/19/2023
Release 4.3

NBIS USER ROLE	RESPONSIBILITY	WHAT SECTION(s) USER ROLE CAN ACCESS	ORG TYPE AVAILABLE
Adjudicator	Can access and select Guidelines to complete an adjudication case. Adjudicator role needs to be paired with the Case Processor role to adjudicate a case.	Guidelines Tab and tabs within Guidelines Tab	Adjudication Component Adjudication
Appeals Processor	Can complete Appeals information on a case. Appeals role needs to be paired with the Case Processor role to complete appeal actions.	Guidelines Tab and tabs within Guidelines Tab	Appeals
Authorizer	Can review entire case requests, completing financial details, editing certain order form details if needed, and deciding whether to approve, reject, or hold cases. Also, can create & search for subjects.	Task Management, Subject Management, Order Form, Global Search	Authorize
Case Processor	Can processes cases and be paired with other roles to provide additional capabilities. This role has access to view & edit a subject's profile by accessing it from the Subject Banner in a case. *This role is usually paired with other roles such as Adjudicator, or Appeals Processor, or CV, or IM, or others.	Task Management, Case Worksheet, Global Search	Adjudication Appeals Component Adjudication Investigation Screening Vetting
Component Adjudicator	Can view Case Information tab on the worksheet for cases in the Component Adjudication phase. Needs to be paired with the Adjudicator & Case Processor roles to complete adjudicative actions. Can grant determinations from the Subject Profile tab. Needs to be paired with Subject Manager roles in order to access Subject Management.	Case Worksheet - Case Information, Subject Management	Component Adjudication

NBIS USER ROLE	RESPONSIBILITY	WHAT SECTION(s) USER ROLE CAN ACCESS	ORG TYPE AVAILABLE
CV Analyst	Can view and process CV alerts. The user is responsible for processing the CV cover case which contains the data of all validated alerts. Needs to be combined with Case Processor to function. Can view Issues tab to manage issue tags.	Task Management	Vetting
Distribution Manager	Responsible for adding and removing Organizations as Distribution Organizations. Also responsible for creating, editing, and removing the rules that decide how cases will be distributed to their Distribution Organizations by Phase. The Distribution Manager also needs to be in an org with the Investigation Control function to view the Distribution Rule configurations tab.	Org Management	N/A Onboarding Manager is required to add role
Enrollment Manager	Can manually enroll & unenroll subjects from a Continuous Vetting program. Has the ability to search for & create subjects, and view their information in the Subject Profile & History.	Global Subject Search, Subject Worksheet	Vetting
Facility Security Officer (FSO)	Can manage subjects and complete actions like initiating case requests, complete mass initiation or affiliation for subjects, manually create service catalog requests to their Service Provider, add/edit subject's PII, manage contractor affiliations, manage access, complete appeals, complete adjudication sub-tasks, and submit visit requests for subjects. Can also create, edit, request, and approve visit events. Can manually reassign tasks to users in their org.	Task Management, Subject Management, Global Search, Visit Management	Facility Security Office

NBIS USER ROLE	RESPONSIBILITY	WHAT SECTION(s) USER ROLE CAN ACCESS	ORG TYPE AVAILABLE
Field Investigator	Responsible for completing field leads. Needs to be combined with Case Processor to function. Has access to Issues tab to capture issue tags when working a field lead.	Lead Worksheet	Investigation
Initiator	Can initiate subject case requests and complete Routing details, edit certain order form details before receiving the subject's SF back from eApp, and create & search for subjects. Can complete mass initiation or affiliation for subjects.	Dashboard, Task Management, Order Form, Global Search	SSC
Investigator	Can be assigned & work on leads in the Investigation phase for all Methods of Fulfillment (ARC, CRC, Batch, Field, & Voucher). Needs to be combined with Case Processor to function. Has access to Issues tab to capture issue tags when working a lead.	Lead Worksheet	Investigation
Leads Analyst	Responsible for completing leads. Needs to be combined with Case Processor to function. Has access to Issues tab to capture issue tags when working a field lead.	Lead Worksheet	Investigation
NBIS Financial Manager	Responsible for managing SON/SOI and SON/IPAC relationship tables, and IPAC, IPAC Exemption, TAS, and BETC codes at a global NBIS level.	System Settings	N/A - Onboarding Manager role only can give access to this role.
Notification Manager	Responsible for creating and managing notifications related to the case completion processes, to be sent out to organization users or subjects.	Org Management	Adjudication Appeals Authorize Component Adjudication Facility Security Office Investigation Review Screening SSC Vetting

NBIS USER ROLE	RESPONSIBILITY	WHAT SECTION(s) USER ROLE CAN ACCESS	ORG TYPE AVAILABLE
Onboarding Manager	Responsible for managing Org Levels and creating orgs with grouped Org Levels. This role also has permissions to add any function or org type to an org regardless of inherited restrictions. Also has permissions to add certain roles to orgs, regardless of org type.	Org Management, System Settings	N/A - Onboarding Manager role only can give access to this role.
Operations Manager	Responsible for managing certain Org Configurations. They also have access to Reports and all tabs in Task Management.	Task Management, Org Management, Reports, Subject Management	Adjudication Appeals Investigation Screening Vetting
Order Form Template Manager	Responsible for managing the Order Form Templates for their organization(s).	Order Form Library	Authorize Review SSC Facility Security Office
Org Assignment Manager	Responsible for managing the assignment rules for their organization(s).	Org Management	Adjudication Appeals Authorize Component Adjudication Facility Security Office Investigation Review Vetting
Org Manager	Responsible for managing the details & hierarchy for their organization(s).	Org Management	Adjudication Authorize Appeals Component Adjudication Facility Security Office Investigation Review Screening SSC Vetting

NBIS USER ROLE	RESPONSIBILITY	WHAT SECTION(s) USER ROLE CAN ACCESS	ORG TYPE AVAILABLE
Org Relationship Manager	Responsible for managing org relationships that are established between organizations outside each other's hierarchy, in the Org Relationship tab.	Org Management	N/A - Onboarding Manager role only can give access to this role.
Org Workload Manager	Responsible for managing capabilities of users in their organization and manually assigning cases to users within their organization(s).	Task Management, Org Management	Adjudication Appeals Authorize Component Adjudication Facility Security Office Investigation Review Screening Vetting
Polygraph	Responsible for adding. editing, and removing polygraph entries from a given subject. Role needs to be added on to a role that has access to the subject profile	Subject Management	Other than Adjudication Org Type - Can only be granted by the Onboarding Manager
Preparer	Responsible for adding, removing, edit leads to a case after S&S. Leads that are pre-populated are on this list for preparer. Preparer would review leads, then send. Needs to be combined with Case Processor to function.	Org Management	Investigation
Program Tag Manager	Can manage the program tags that are available for their organization(s).	Org Management	Adjudication Authorize Appeals Component Adjudication Facility Security Office Investigation Review Screening SSC Vetting

NBIS USER ROLE	RESPONSIBILITY	WHAT SECTION(s) USER ROLE CAN ACCESS	ORG TYPE AVAILABLE
Quality Reviewer	Has visibility across all phases at any time throughout an investigation. Completes investigation case in Quality Review if work has been completed appropriately. Views the case after it's successfully progressed through. Needs to be combined with Case Processor to function.	Org Management	Investigation
Question Manager	Responsible for managing question set configurations for their organization.	Org Management	Investigation
Reports Manager	Responsible for viewing and modifying reports and for managing individual report access and export configuration for users in their organization.	Reports	N/A Onboarding Manager is required to add role
Reviewer	Responsible for reviewing the subject's standard form, accepting, or rejecting their responses, and adding attachments. If rejecting they can also add comments and re-route the case back to the subject. Also, can create & search for subjects, and can specifically view the Profile, Notes, Attachments, and History tabs in the Subject Worksheet.	Subject Management, Task Management, Order Form, Global Search	Review
Scoping Manager	Responsible for all Scoping Rules configurations to support Scoping and Scheduling at this time.	Org Management	Investigation
Screener	Responsible for Managing Interim Determinations from the Subject Profile. Has access to My Subject List to view subjects in their organizational hierarchy and subjects in orgs that have a Screening org relationship with their org. Required to be paired with the Case Processor role.	Subject Management	Screening

NBIS USER ROLE	RESPONSIBILITY	WHAT SECTION(s) USER ROLE CAN ACCESS	ORG TYPE AVAILABLE
Special Security Officer (SSO)	Responsible for managing certain Access Levels and Interim Determinations for subjects. The Access Levels & Determinations they manage are controlled by the System Manager. Needs to be paired with the Subject Manager to gain access to Subject Management. The Parent Role ID should be Subject Manager	Cannot access tabs independently without Subject Manager role.	N/A - Can only be granted by the Onboarding Manager
Subject Manager	Can manage subjects and complete actions like initiating case requests, mass initiating or affiliating subjects, manually create service catalog requests for their service provider, complete adjudication sub-tasks and interim SAC & NAC cases if assigned, add/edit subject's PII, affiliations, access, and complete appeals and visit requests for subjects. Can also create, edit, request, and approve visit events. Can manage interim determinations from the subject profile.	Task Management, Subject Management, Global Search, Order Form, Visit Management, Reports	SSC
Subject Profile Editor	Responsible for updating subjects' SSN or other PII data in the subject profile if needed. Also has the ability to view the Profile, Notes, Attachments, and History tabs in the Subject Worksheet and reset the subject's eApp password.	Subject Management, Global Search, Task Management	N/A - Onboarding Manager role only can give access to this role.
Subject Viewer	Responsible for viewing the subject information from within Subject Management.	Subject Management, Global Search, Task Management, Visit Management	Authorize Review SSC Facility Security Officer
System Manager	Responsible for managing the system settings tables, org hierarchies, org details, users, and workflows.	System Settings, Org Management, Task Management	N/A - Onboarding Manager role only can give access to this role.

NBIS USER ROLE	RESPONSIBILITY	WHAT SECTION(s) USER ROLE CAN ACCESS	ORG TYPE AVAILABLE
Task Reassignment	Responsible for reassigning cases to users within their team or, if unassigned to a team, to others who are unassigned within their organization from within the Case Request Order Form. Needs to be paired with Case processor in order to access the case and perform that function. Also has the ability to manually reassign bulk tasks. Can reassign adjudication cases when they are reviewing an open case.	Order Form, Task Management	Adjudication Appeals Authorize Review Component Adjudication Facility Security Office Investigation Screening Screening Vetting
Team Manager	Responsible for managing the structure and details of teams within organizations. Can also add, remove, and reassign users to teams.	Org Management	Adjudication Appeals Investigation Screening Vetting
Team Structure Manager	Responsible for managing user skillsets and can access My Team's Work in Task Management to assign cases. Can view the hierarchy and details of a team. Can reopen adj cases that are closed if the action is configured in WFB.	Org Management, Task Management	Adjudication Appeals Investigation Screening Vetting
User Manager	Responsible for creating and managing users within their organization(s).	Org Management, NBIS Reports	Adjudication Appeals Authorize Facility Security Office Investigation Review SSC Component Adjudication Screening Vetting

NBIS USER ROLE	RESPONSIBILITY	WHAT SECTION(s) USER ROLE CAN ACCESS	ORG TYPE AVAILABLE
Validator	Responsible for reviewing cases and determining if they are ready to be scoped and scheduled. Can perform all work within this phase. Validates all required fields are present. Can view cases, but cannot open unless they are assigned. Can reroute back to agency, and can add comments for reason of reroute/pushback. Needs to be combined with Case Processor to function.	N/A	Investigation
Workflow Manager	Responsible for creating, modifying, or disabling a workflow, specifically in Form Routing.	Org Management	Authorize Review SSC Facility Security Office

For additional help and information to familiarize agency human resource and security officials with DCSA products and services go to: Government HR Security and Personnel.

13.4 Org Configuration Reference Table

Last Update: 10/24/2022
Release: 4.2 Knoxville

Table 13-8: Org Type and Configuration Reference Table

		Org Type									
		SSC	Review	Authorize	Adj	Appeals	Screening	CA	FSO	CV	Inv.
Org Level Configuration	Assignment Rules	X	X	X	X	X	X	X	X	X	X
	Notifications	X	X	X	X	X	X	X	X	X	X
	Form Routing	X							X		
	Workflow Builder				X	X	X			X	X
	Service Catalog				X	X	X			X	X
	Program Tags	X	X	X	X	X	X	X	X	X	X
	Organization Relationships	X	X	X	X	X	X	X	X	X	X
	Ingest Management				X						
	User Levels				X	X	X			X	X
	Modules				X	X	X			X	X
	User Assignment Templates	X	X	X	X	X	X	X	X	X	X
	Distribution Rules										X
	Case Category									X	X
	Case Progression Exception Rules									X	X
	Scoping Rules										X

13.5 Workflow Diagrams

13.5.1 AGENCY WORKFLOW DIAGRAM

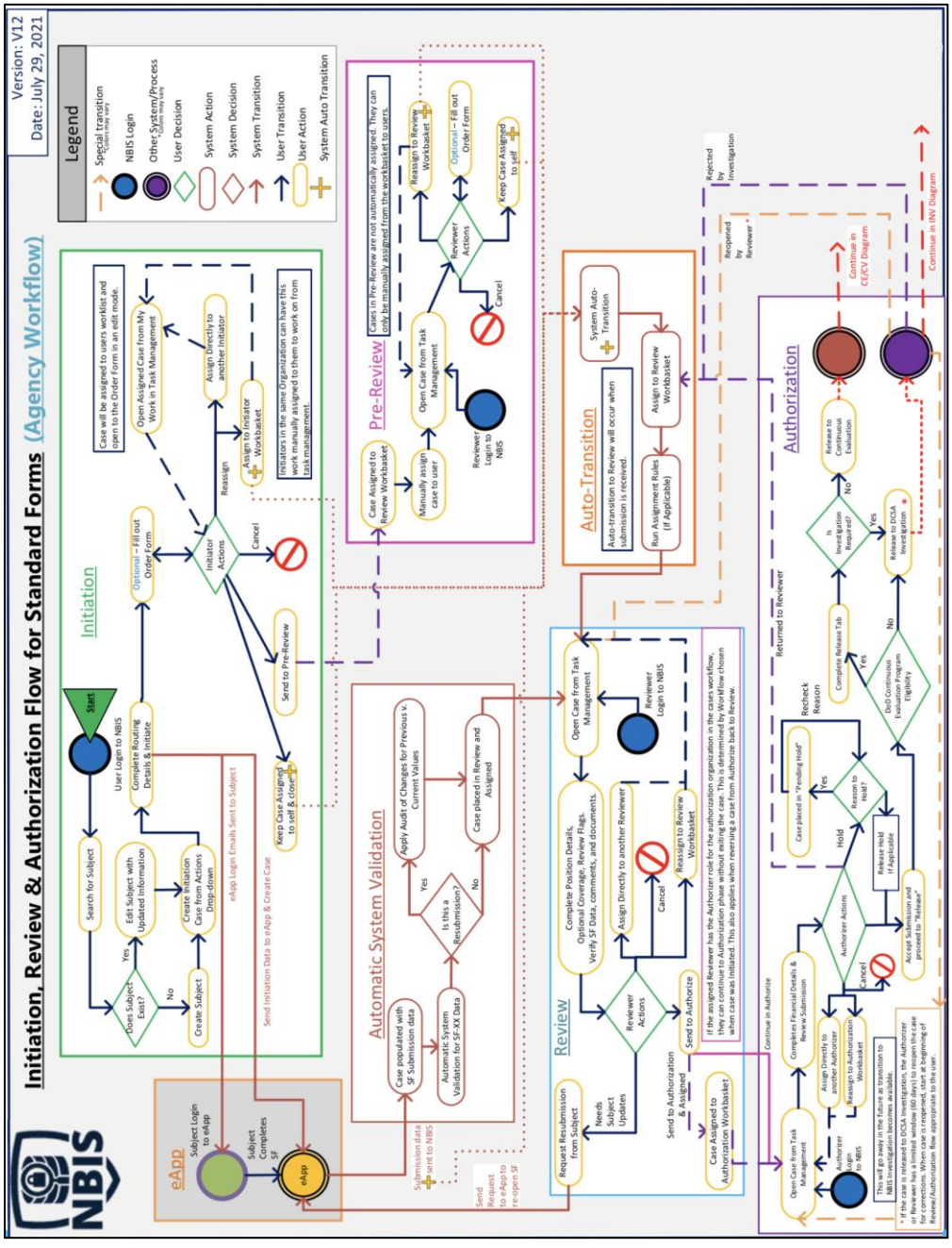


Figure 13-1: Agency SF-86 Workflow Diagram

13.5.2 OVERVIEW OF AN AGENCY CASE

From the **Subject Profile**, a **Case Request** can be created. The **Subject Manager**, **Initiator**, or **Facility Security Officer** will initiate the case which will place it in **Awaiting Subject Submission**. The user will have the option to fill out the Order Form, reassign the case, or send the case to the Review organization to work on prior to receiving the SF submission (**Review-Pending eApp**).

The case will resume in the **NBIS** system pending the subject's SF-8X from **eApp**. Once the SF Data comes in, the data will be validated, and case will be placed in **Review-eApp Received**. If the case is currently assigned to a user or a workbasket, the case will automatically be transitioned to the Review organization and then assigned.

The **Reviewer** can **Request Update** of the SF-8X documentation from the subject through **eApp** (**Awaiting Subject Revision**) or send the case to the **Authorization** phase.

Once in **Authorization**, the **Authorizer** can place the case **On-Hold**, **Return to Reviewer** for updates (**Returned from Authorizer**), or **Release** to a Service Provider (**Submitted**). If the org is **DoD CV Eligible**, the case can be released to Investigation or to Continuous Vetting. If not, it will automatically release to Investigation.

At any point, if configured for the organization, a case can expire from the **NBIS** side of the application.

If the case is assigned to the current user in **NBIS** and is editable [**Initiation, Review, Authorize, etc…**], the user can cancel the case, reassign to another user or to the organization workbasket.

If there is a communications failure with **eApp** when Submitting, Cancelling, or Expiring a case, the case will be placed in **Failed to Delete SF** and should be resolved at a later point by a **System Manager**.

13.5.3 AGENCY CASE STATUSES DIAGRAM

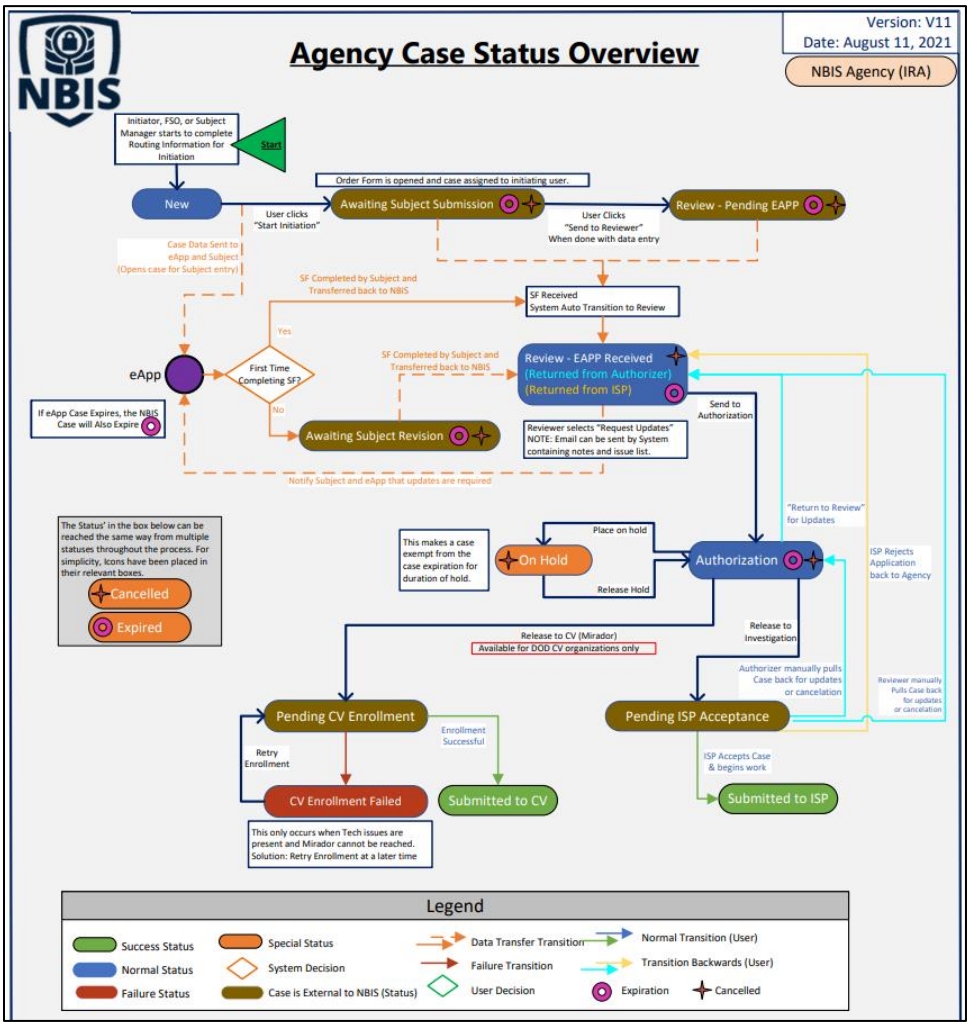


Figure 13-2: Agency Case Status Diagram

13.5.4 OVERVIEW OF ADJUDICATION WORKFLOW

There are two ways to create a case in the **Adjudication Phase** in NBIS. First, you can navigate to the **Subject's Worksheet** (depending on your role) and select the **Create Case** action and then the **Adjudication Phase**. Since the Investigation process is currently still being completed by DCSA, you can use the file **generated from PIPS** and **ingest that into NBIS** to create the Adjudication Case.

Since the Adjudicating Organization will utilize the workflow builder configuration that NBIS provides, the workflow scenario below is just an example of what could be set up by an organization. All cases will start off in the global status of **Received**. The organization might allow the user to take an action to **Phase Transition** the case to another organization or create a **Sub-Task** for the Security Manager to complete as part of the workflow. Once the case has been assigned properly and all the information needed is gathered, the **Adjudicator** will **Review Guidelines** so that they can make their determination. If this is an initial investigation, then they would be making a **Favorable or Unfavorable Initial Determination**. If it is a re-investigation, then they would decide to either **Remove or Sustain the Determination** originally given for the subject. After any determination action is taken, the information captured must be **Finalized**, to be stored with the Subject's Profile. If the Adjudicator has determined an unfavorable outcome, then the case will either move to the global status of **Closed**, or it will transition to the **Appeals Phase**. If a favorable outcome is determined, then the case will move to **Closed** status and the subject will be automatically enrolled in the **Continuous Vetting** program upon finalization.

Everything between the status of **Received** and **Closed** in the workflow, is completely configurable by the **Operations Manager**. So, they will determine the **Status** & **Action** names, and the order in which the case progresses through them.

13.5.5 ADJUDICATION/APPEALS WORKFLOW DIAGRAM

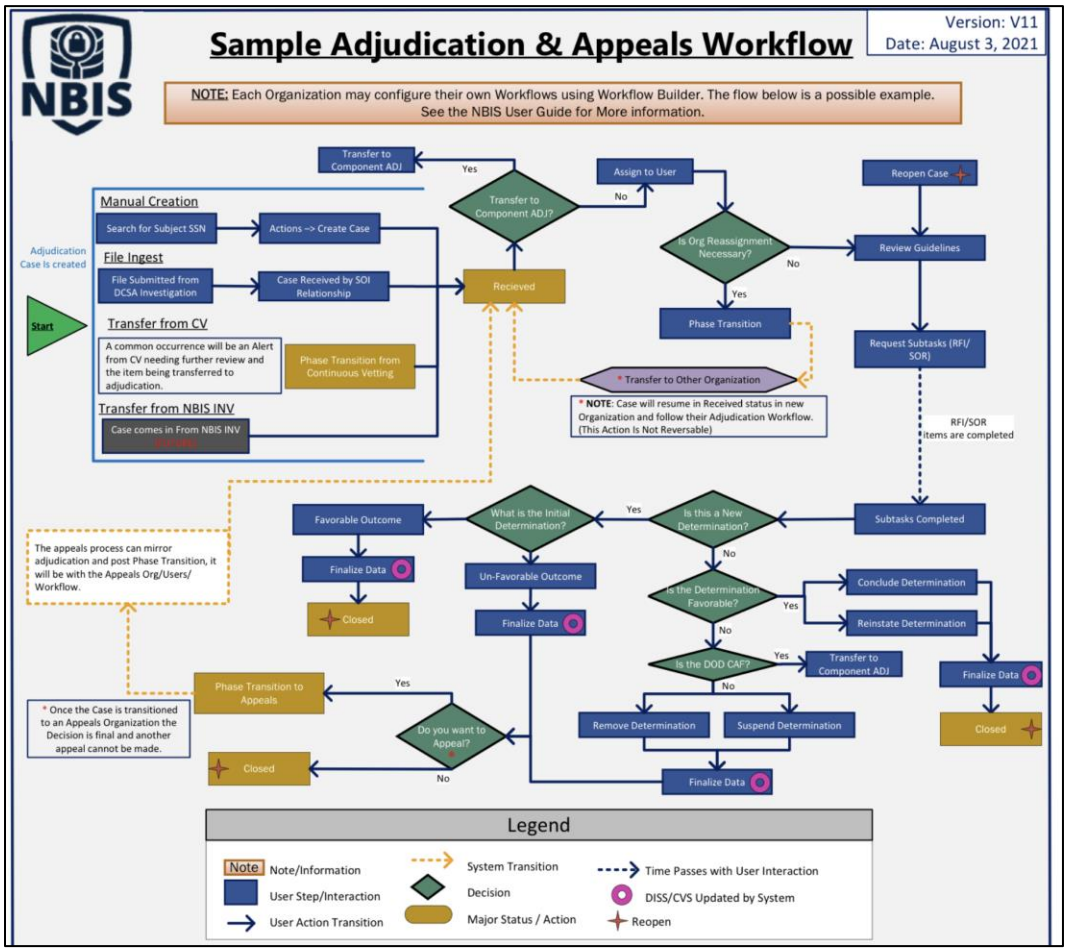


Figure 13-3: Adjudication Workflow Diagram