# MFTRP Documentation

# Introduction

**Overview of the MFTRP Attestation System**

The Malign Foreign Talent Recruitment Program (MFTRP) Attestation System is a structured framework designed to ensure compliance with institutional and regulatory requirements by verifying that researchers and associated individuals do not participate in malign foreign talent programs. This system, integrated into the university’s Research Administration Portal, facilitates the attestation process for individuals involved in research projects, ensuring transparency and accountability. It leverages a combination of database-driven workflows, user interfaces, and automated notifications to manage attestations efficiently across various user groups, including active HUIDs, inactive HUIDs, and non-HUID individuals.

**Purpose and Scope**

The primary purpose of the MFTRP Attestation System is to implement a robust process for researchers to attest their non-participation in malign foreign talent programs, as mandated by university policy. The system supports attestation at the time of proposal submission and annually thereafter for all covered individuals involved in a project. It provides role-based access to manage and monitor attestations, ensuring that only authorized personnel can view or act on sensitive data. The scope encompasses:

* **Attestation Workflow**: Managing the attestation process for active HUIDs, inactive HUIDs, and non-HUIDs.
* **Role-Based Access**: Defining permissions for roles such as MFTRP View All, MFTRP Affiliated View, Central Office Staff, and Admin users.
* **Data Management**: Utilizing materialized views and database tables to store and track attestation data sourced from the GMAS database.
* **Notification System**: Automating notifications for attestation requirements, reminders, and renewals.
* **Administrative Oversight**: Providing tools for admin users to configure roles, manage reviewers, and monitor attestation statuses.

The system is designed to streamline compliance, reduce administrative burden, and ensure accurate tracking of attestation statuses while maintaining data security and accessibility.

This documentation provides a comprehensive guide to the system’s components, workflows, and administrative functions, serving as a reference for system administrators, reviewers, and developers maintaining or extending the MFTRP Attestation System.

# **System Requirements**

**Attestation Requirements**

The Malign Foreign Talent Recruitment Program (MFTRP) Attestation System mandates a structured process to ensure that all individuals involved in research projects attest to their non-participation in malign foreign talent programs. Key requirements include:

* Every individual associated with a project, identified as a "Covered Individual," must complete an attestation confirming their non-participation in MFTRP. This applies to individuals with active HUIDs, inactive HUIDs, and non-HUIDs.
* The system supports verification of attestations through reviewer oversight, with options for individuals to select "I am not," "I am," or "I am unsure if I am" regarding their participation. Supporting documentation may be required, particularly for inactive HUIDs and non-HUIDs.

**Frequency of Attestation**

To maintain ongoing compliance, the system enforces a defined attestation schedule:

* **Initial Attestation**: Covered individuals must attest upon becoming associated with a project, triggered by their inclusion in the mv\_gmas\_mftrp\_active\_members materialized view.
* **Annual Re-attestation**: Individuals who select "I am not" are required to re-attest annually. The system sends notifications 14 days before the attestation expiry and on the exact expiry date (one year from the last attestation).
* **Pending Attestation Reminders**: For incomplete or pending attestations (e.g., "I am" or "I am unsure if I am"), the system sends up to three reminder notifications every 7 days until the attestation is completed or the reminder cycle concludes.

**Compliance and Objectives**

The MFTRP Attestation System is designed to meet institutional and regulatory compliance goals while ensuring operational efficiency:

* **Regulatory Compliance**: Ensures adherence to policies prohibiting participation in malign foreign talent programs, protecting the integrity of research activities.
* **Data Accuracy and Tracking**: Utilizes the GMAS database link to source accurate data on covered individuals, storing attestation records in structured database tables (mftrp\_attestations, mftrp\_nonhuid\_attestations, mftrp\_exclusions) to enable reliable tracking.
* **User Accessibility**: Provides a user-friendly interface within the Research Administration Portal for active HUIDs to complete attestations and for reviewers to manage attestations for inactive HUIDs and non-HUIDs.
* **Notification Automation**: Automates the delivery of attestation requirement notifications, reminders, and renewal prompts to minimize manual oversight and ensure timely compliance.
* **Role-Based Security**: Restricts access to sensitive attestation data based on roles (e.g., MFTRP View All, MFTRP Affiliated View, Central Office Staff), ensuring that only authorized personnel can view or act on specific data.
* **Flexibility for Exemptions**: Allows admin users to mark certain non-HUIDs or inactive HUIDs as "Not Required" for attestation, storing these exemptions in the mftrp\_exclusions table to streamline compliance for exempt individuals.

The system requirements ensure that the MFTRP Attestation System is robust, scalable, and capable of supporting the university’s compliance needs while providing clear workflows for all stakeholders involved in the attestation process.

# Roles and Permissions

The Malign Foreign Talent Recruitment Program (MFTRP) Attestation System defines distinct roles to manage access and actions related to attestation processes, ensuring secure and controlled handling of sensitive data. Each role is assigned specific permissions to view, manage, or act on attestation data within the Research Administration Portal, particularly through the MFTRP Admin tab. Roles are configured via the Administration screen, allowing admin users to assign HUIDs and define affiliations as needed.

**MFTRP View All Role**

* **Description**: This role grants comprehensive access to all MFTRP-related data and functionality within the MFTRP Admin tab.
* **Permissions**:
  + Full access to view and manage information for:
    - Non-HUID individuals.
    - Inactive HUIDs.
    - Active HUIDs.
    - Non-covered individuals (those no longer requiring attestation or who acted despite not being covered).
  + Authorized to perform actions on behalf of all individuals, including uploading supporting documents for existing attestations.
  + Access to all tabs in the MFTRP Admin page: Non-HUIDs/Inactive HUIDs, Active HUIDs, and Non-Covered Individuals.

**MFTRP Affiliated View Role**

* **Description**: This role provides access to the MFTRP Admin tab with permissions limited to individuals within the user’s primary or secondary affiliations.
* **Permissions**:
  + View and take actions on non-HUIDs and inactive HUIDs.
  + View active HUIDs associated with their primary affiliation and, if applicable, secondary affiliations.
  + View individuals without any affiliation.
  + Upload supporting documents for covered and non-covered individuals within their affiliation scope.
  + Access to all MFTRP Admin tabs, but data visibility is restricted to affiliated individuals.

**Central Office Staff Role**

* **Description**: This role offers read-only access to the MFTRP Admin tab, limiting actions to viewing data without modification capabilities.
* **Permissions**:
  + View non-HUID and inactive HUID information without the ability to take actions on their behalf.
  + View active HUIDs within their primary or secondary affiliations.
  + View non-covered individual information.
  + No permissions to upload documents or perform actions such as editing or creating attestations.

**Admin Users**

* **Description**: Admin users have permissions equivalent to the MFTRP View All role, with additional administrative capabilities to configure the system.
* **Permissions**:
  + Full access to the MFTRP Admin tab, identical to MFTRP View All.
  + Ability to add HUIDs and assign roles (MFTRP View All, MFTRP Affiliated View, Central Office Staff) through the Administration screen.
  + Define secondary affiliations for users to control data visibility.
  + Mark certain non-HUIDs or inactive HUIDs as "Not Required" for attestation, storing exemptions in the mftrp\_exclusions table.
  + Manage reviewer assignments and update division-specific reviewer emails in the mftrp\_reviewers table.
  + **Notification Management**: Admin users can mark covered individuals to receive or not receive MFTRP-related notifications by setting the notification\_ignored\_flag in the mftrp\_notifications table:
    - When set to Y, the covered individual (Active HUID) will not receive any MFTRP-related notifications, including Attestation Requirement, Attestation Reminder, Attestation Nearing Renewal, or Attestation Annual Requirement notifications.
    - When set to N or left unset, the individual receives notifications as per the standard workflow.
    - This flag is stored in the mftrp\_notifications table, ensuring that notification preferences are tracked and respected by the system’s automated processes.

**Role Configuration**

* **Administration Screen**: All roles are configured through the Administration page (Page 10000) under the "Attestation Management" menu. Admin users can:
  + Assign HUIDs to specific roles.
  + Define affiliations to limit data access for MFTRP Affiliated View and Central Office Staff roles.
  + Update the mftrp\_reviewers table to assign reviewer emails to divisions, ensuring notifications are routed correctly.
  + Set the notification\_ignored\_flag for Active HUIDs in the mftrp\_notifications table to control whether individuals receive MFTRP-related notifications.
* **Access Control**: Role-based permissions ensure data security by restricting access to sensitive information based on user roles and affiliations. For example:
  + MFTRP Affiliated View users see only data within their assigned affiliations.
  + Central Office Staff have view-only access, preventing unauthorized modifications.
* **Dynamic Role-Based Display**: The MFTRP Admin tab dynamically displays data based on the user’s role, using Authorization Schemes to filter content in the Non-HUIDs/Inactive HUIDs, Active HUIDs, and Non-Covered Individuals tabs.

These roles and permissions ensure a secure, efficient, and controlled environment for managing MFTRP attestations, balancing accessibility with data protection and compliance requirements.