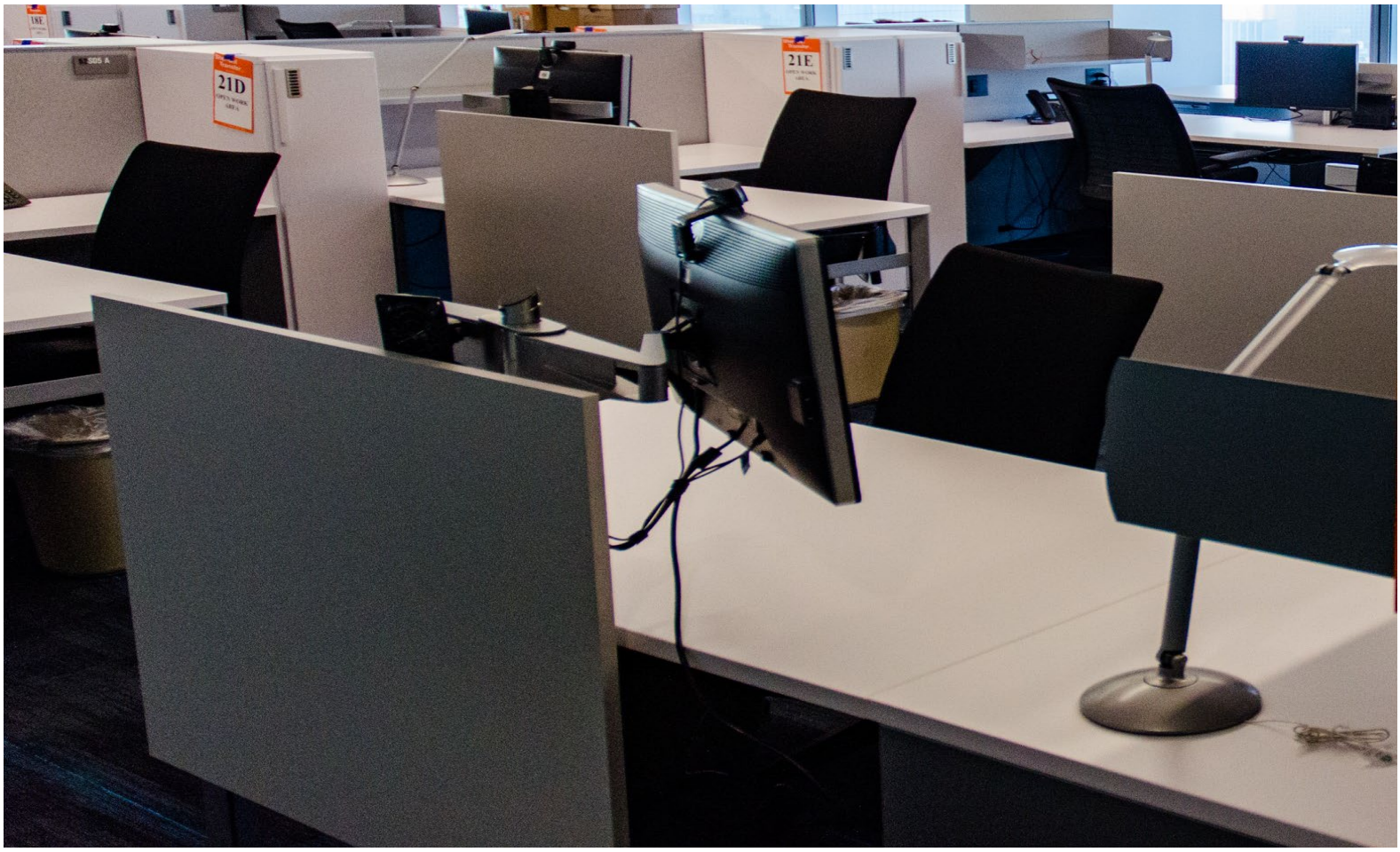


RAM Access Portal User Guide

February 2024

FEMA

This page intentionally left blank

Table of Contents

1. How to Use this Guide

The RAM Access Portal (RAP) provides a secure, single-sign-on (SSO) capability to access RAM Access Portal applications requiring FEMA's approval for access. The RAM Access Portal provides the ability for users to request and manage application account access and role permissions in one location. This guide includes instructions and workflow screenshots to assist users with the portal.

Attention

This exclamation point alerts the user to important information to the subject it references. Please note these references as you use the RAM Access Portal (RAP).

2. User Types and Roles

2.1. Types of RAM Users

The RAM Access Portal is not intended for public use. Users are FEMA employees and their partners requiring access to the RAP's applications. These users include:

- Federal Users
- Contractors
- Cooperating Technical Partners (CTP)
- CTP Subcontractors
- Interagency Partners

2.2. RAP User Roles

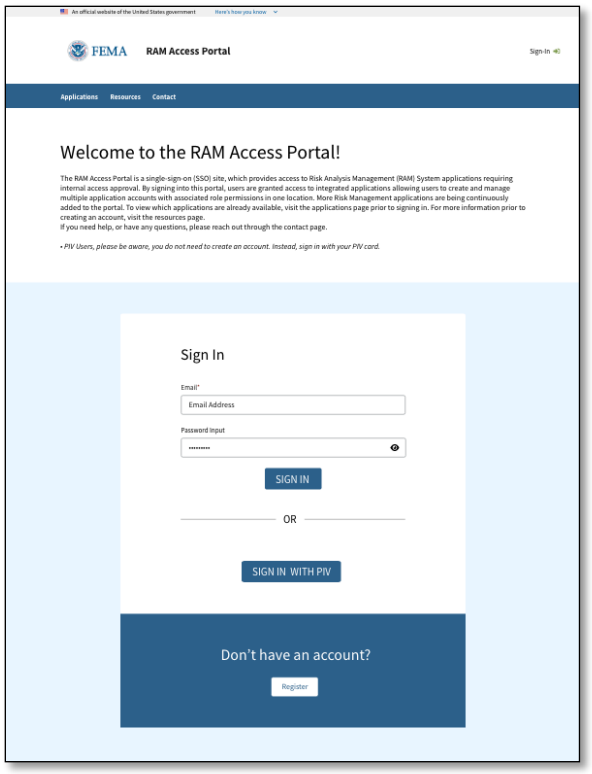
Each user has a defined role, which determines the accesses, permissions, and responsibilities within RAP. These roles are:

- General User – This is the standard user type. This user has the ability to create a RAP account, edit their profile information, request access to any application available in RAP, and access any RAP application they already have access to.
- Supervisor – A supervisor user has all of the same permissions as a general user but also has the ability to approve any application requests, approve profile updates, and view and revoke any application accesses for any user they supervise.
- Authorizer – An authorizer user has all of the same permissions as a general user but also has the ability to approve any application requests, approve profile updates, and view and revoke any application accesses. Requests will be automatically routed to the correct authorizer based on the information of the user who submitted the request.
- Product Owner – A Product Owner has all of the same permissions as a general user but can also view and manage access for users under the applications they are a product owner for.

3. Reference Information

3.1. First Accessing RAP

The RAM Access Portal can be accessed at the following link. When you first access the system, you will see the following sign-in page. From this page, you can access three pages of reference and contact information without needing to log into the system.



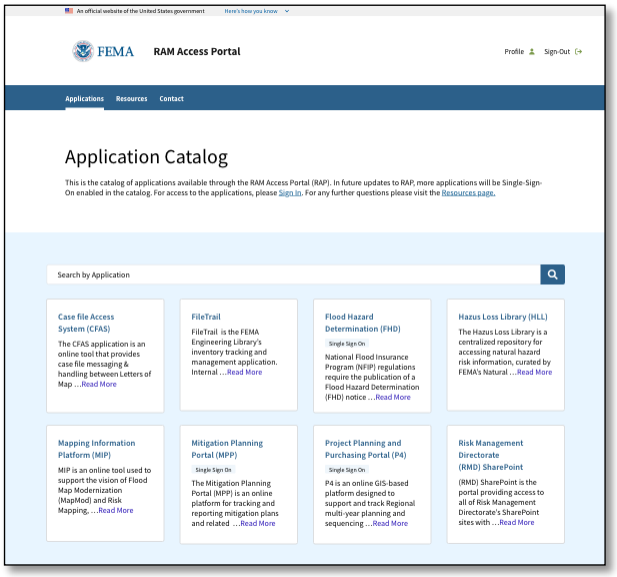
For all pages of the RAP system, there is a menu bar along the top containing three navigational hyperlinks. The navigation options here are:

- Applications, which provides the catalog of all applications available on the system
- Resources, which launches the Resources page with links to additional information relevant to RAP users, required training information, and other useful information that is detailed later in this Guide
- Contact, which returns the user to the Contact Support form. Users provide their contact information along with a description of their reason for contacting support

3.2. Applications Catalog

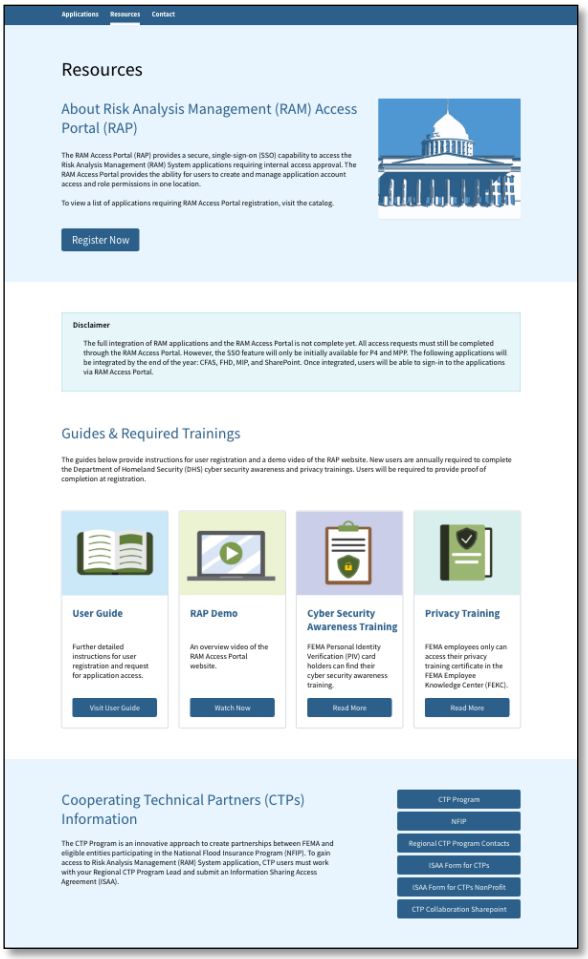
The Applications Catalog page can be accessed by clicking the Applications tab on the navigation bar. The Catalog section shows the full list of RAP applications, a basic overview of those applications, and provides access to visit the sites or request application access for users that have an existing RAP account. Users without a RAP account can still see the Catalog and application information without logging in.

More information on each application in RAP can be found in Appendix 7.1.



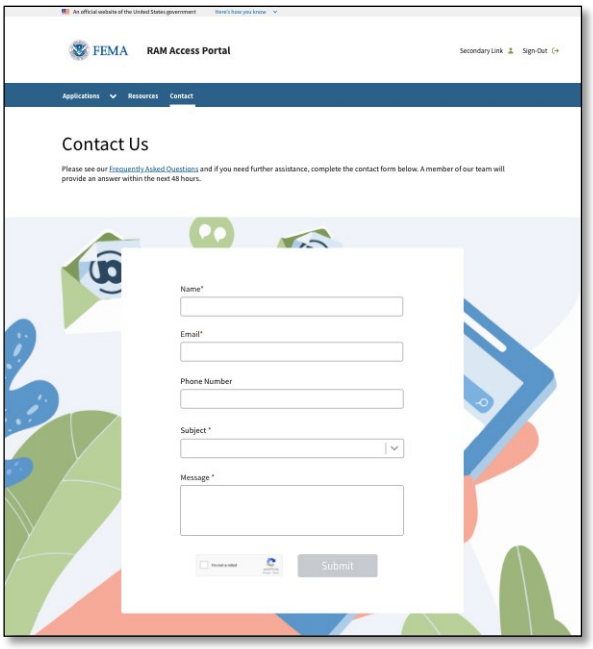
3.3. Resources Page

This page can be accessed without needing to be signed into a RAP account by clicking the Resources tab in the top navigation bar. The Resources Page provides additional information relevant to RAP users, including necessary privacy and security training requirements, CTP information, and Frequently Asked Questions (FAQs).


Applications
Resources
Contact
Resources
About Risk Analysis Management (RAM) Access Portal (RAP)
The RAM Access Portal (RAP) provides a secure, single-sign-on (SSO) capability to access the Risk Analysis Management (RAM) System applications requiring internal access approval. The RAM Access Portal provides the ability for users to create and manage application account access and role permissions in one location.
To view a list of applications requiring RAM Access Portal registration, visit the catalog.
Register Now
Disclaimer
The full integration of RAM applications and the RAM Access Portal is not complete yet. All access requests must still be completed through the RAM Access Portal. However, the SSO feature will only be initially available for P4 and MPP. The following applications will be integrated by the end of the year: CFAS, FHD, MIP, and SharePoint. Once integrated, users will be able to sign-in to the applications via RAM Access Portal.
Guides & Required Trainings
The guides below provide instructions for user registration and a demo video of the RAP website. New users are annually required to complete the Department of Homeland Security (DHS) cyber security awareness and privacy trainings. Users will be required to provide proof of completion at registration.
User Guide
Further detailed instructions for user registration and request for application access.
Visit User Guide
RAP Demo
An overview video of the RAM Access Portal website.
Watch Now
Cyber Security Awareness Training
FEMA Personal Identity Verification (PIV) card holders can find their cyber security awareness training.
Read More
Privacy Training
FEMA employees only can access their privacy training certificate in the FEMA Employee Knowledge Center (FEKC).
Read More
Cooperating Technical Partners (CTPs) Information
The CTP Program is an innovative approach to create partnerships between FEMA and eligible entities participating in the National Flood Insurance Program (NFIP). To gain access to Risk Analysis Management (RAM) System application, CTP users must work with your Regional CTP Program Lead and submit an Information Sharing Access Agreement (ISAA).
CTP Program
NFIP
Regional CTP Program Contacts
ISAA Form for CTPs
ISAA Form for CTPs NonProfit
CTP Collaboration Sharepoint

3.4. Contact Support and FAQs

The "Contact Us" form can be found under the "Contact" tab on the main header. Be sure to complete all fields before clicking "Submit." This form will submit a request to the Risk Map IT Help desk, where they will be able to review your issue and reach out to the necessary parties. Please provide as much detail as you can. The Message box can be expanded using the indicator in the bottom right-hand corner of the box. You will receive a response via email. This form can be accessed without needing to be logged into RAP. If you are logged in, your name, email, and phone will be filled in automatically from your profile information.



Underneath the form is a list of Frequently asked Questions. Please review them prior to contacting RM-IT Help. Your question may be answered there.

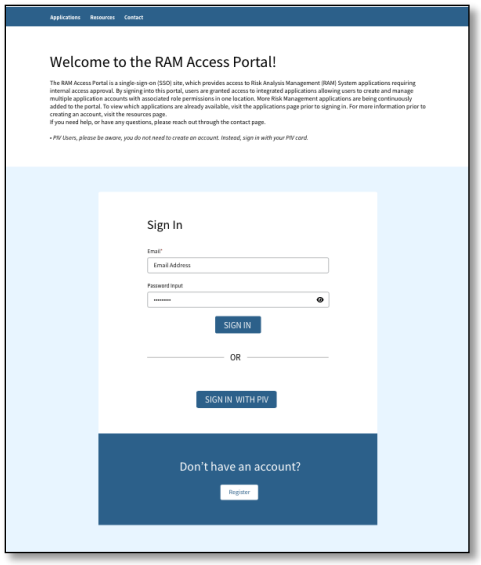
4. User Functionality

4.1. Who Needs to Create an Account?

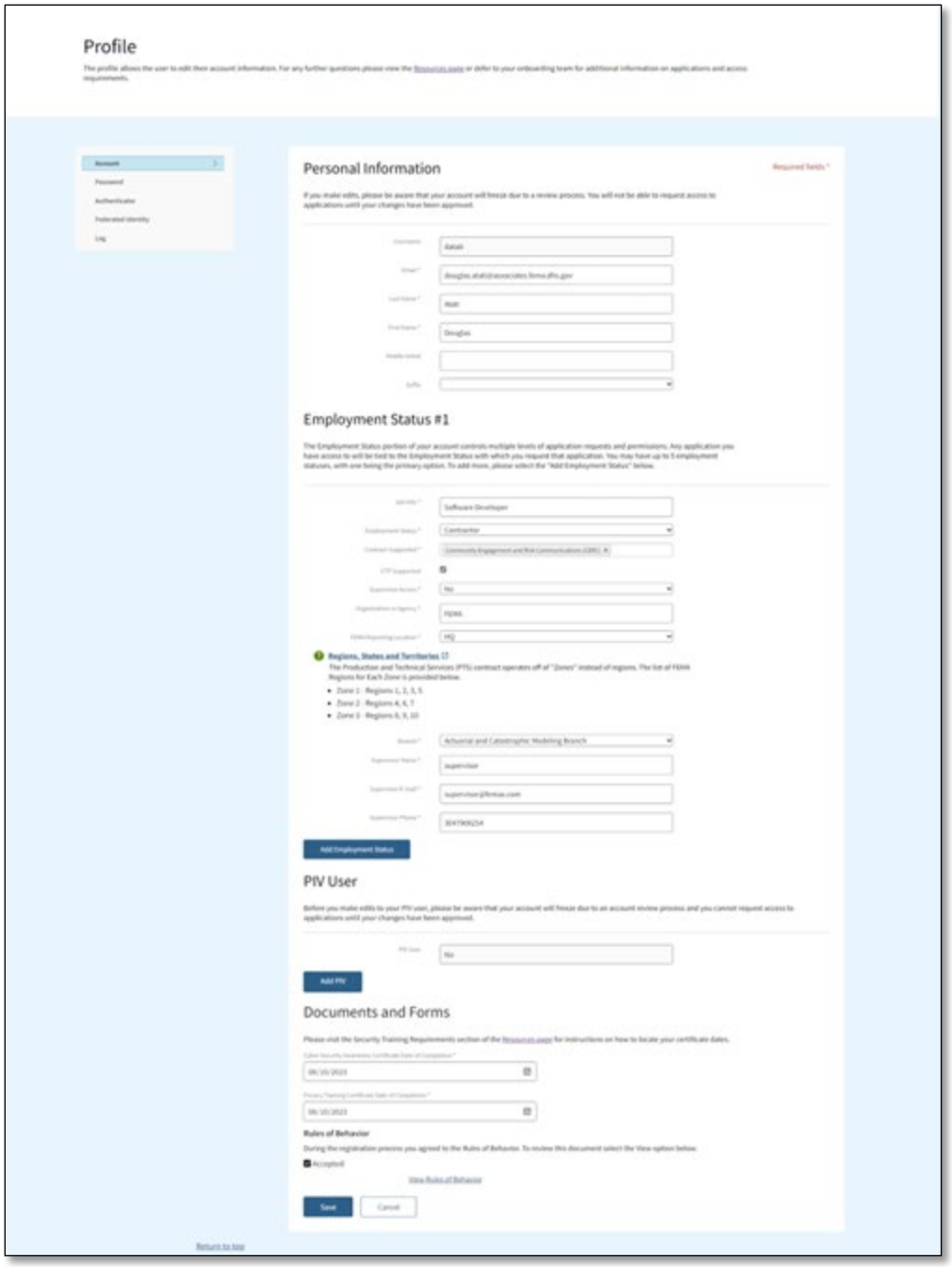
- All new users requesting first time access to any application in RAP
- All users of applications that are newly migrated into RAP, even if the users already have accounts in the migrated application.
- All users who need to update or remove their access for any RAP application
- Anyone who supervises someone who needs access to any of the RAP applications
- All authorizers that approve requests for RAP applications

4.2. Creating an Account

If you do not have an existing account and need to create one, go to the login screen. If you are a non-PIV user, click the “Register” button. If you are a PIV user, click the “Sign In With PIV” button, which will redirect you to a page which allows you to enter in the rest of your profile information.



Complete all the required fields on the profile setup form. If the information is complete and accurate, your new account will be created. You must enter your certificate expiration dates and read and accept the Rules of Behavior by clicking “View Rules of Behavior.”



If you have more than one role that you need to capture, you can do so with a single account by entering more than one Employment Status for appropriate access across the applications. This is not an option for any Federal user or State Partner. You can edit, add, or remove employment statuses after creating an account as well. Note that when you have more than one employment status, each access role will be tied to a specific status so that when that status is removed, the role is removed as well.

4.2.1. Designating Your Supervisor

One of the required sections during account creation is designating your RAP supervisor. Note that this is not necessarily your typical position supervisor, and this designation depends on factors such as, your organizational or contract affiliation, or the FEMA regions you support. While there may be exceptions, supervisors are generally assigned as follows:

- FEMA or other Federal employee users: A FEMA employee supervisor in their office or another RAP supervisor as designated by the RAP team
- Federal Contractors: The designated contractor RAP supervisor for each contract
- Cooperating Technical Partners: The designated regional contact (please see below)

The supervisor that you enter needs to have an account in RAP with a supervisor role attached to allow for application requests and profile updates to be approved in the system. The Supervisor Access drop down allows you to request Supervisor access upon registration.

If you are unsure of who to assign as your supervisor, contact Risk MAP IT Help for assistance.

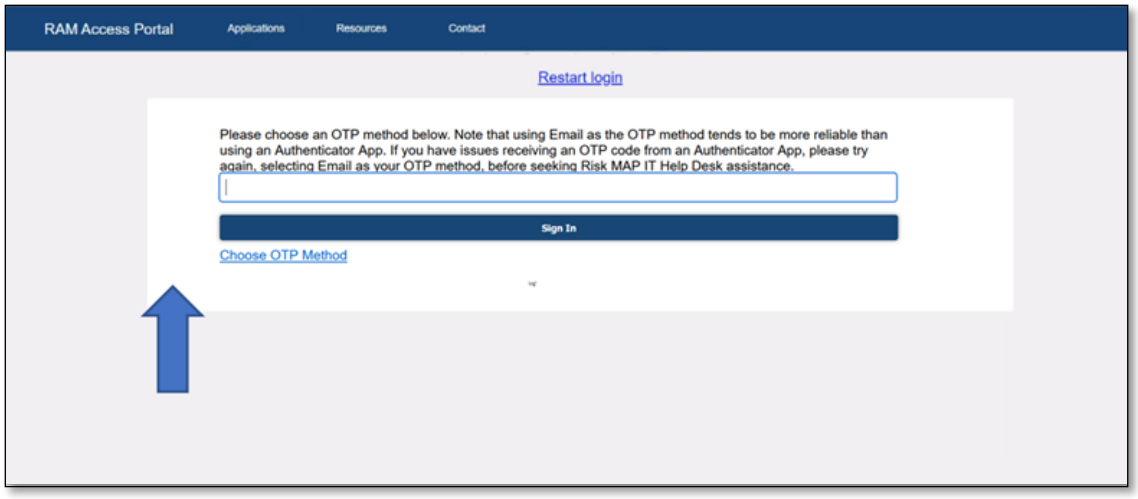
4.2.2 SUPERVISOR INSTRUCTIONS FOR COOPERATING TECHNICAL PARTNERS

To avoid any issues or confusion, Cooperating Technical Partners (CTPs) should enter their Regional CTP Program Lead as their RAP supervisor upon account creation. Their organizational supervisors often do not have RAP accounts, and Regional CTP Program Leads are knowledgeable about to which applications CTPs in their respective regions require access.

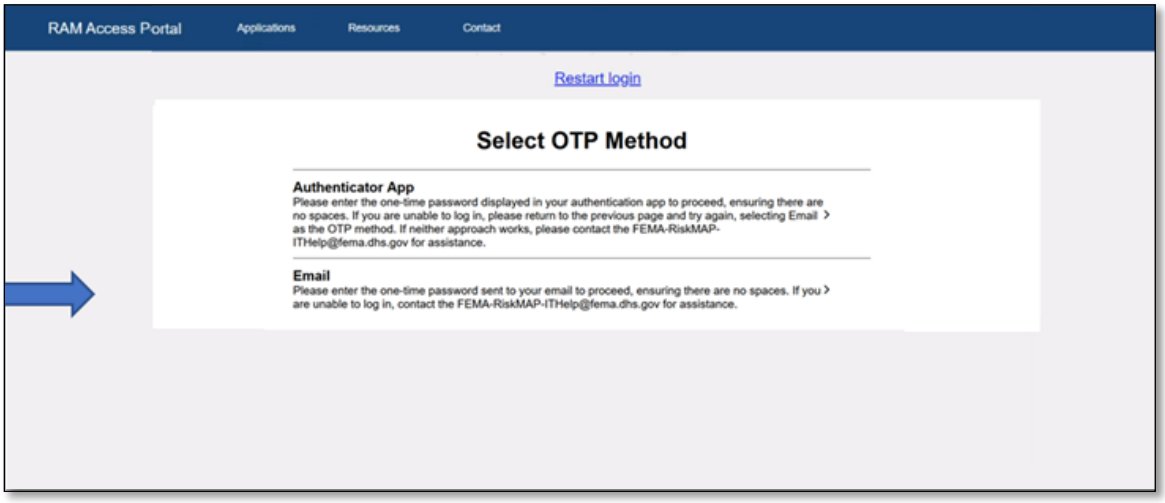
The webpage Regional Contacts for Cooperating Technical Partners lists the regional FEMA staff member for each region. CTPs can reference this list to identify their proper RAP supervisor.

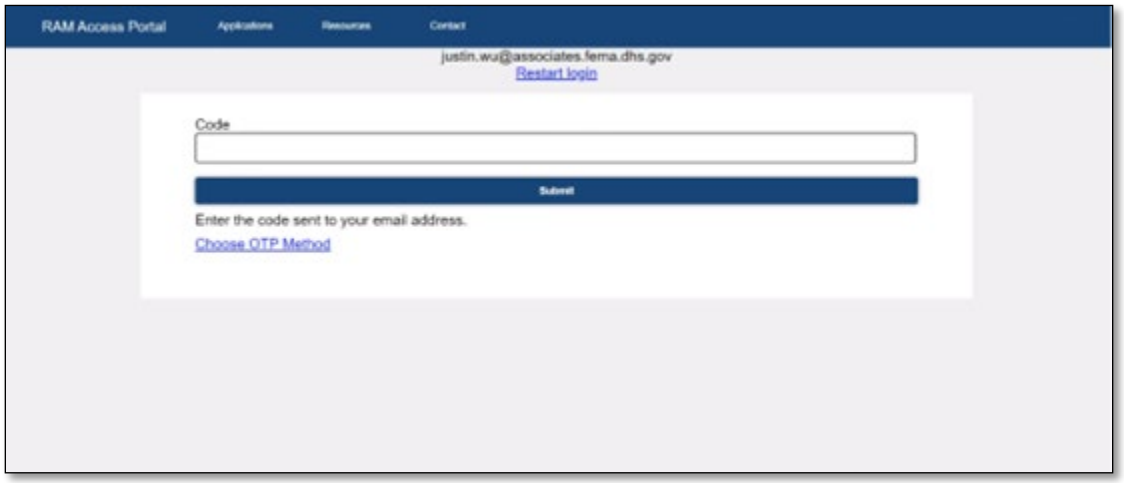
4.3. Multi-Factor Authentication

After registering an account, non-PIV users will be required to set up Multi-Factor Authentication (MFA).



Users can choose between using email or an authenticator app to receive a one-time password (OTP).

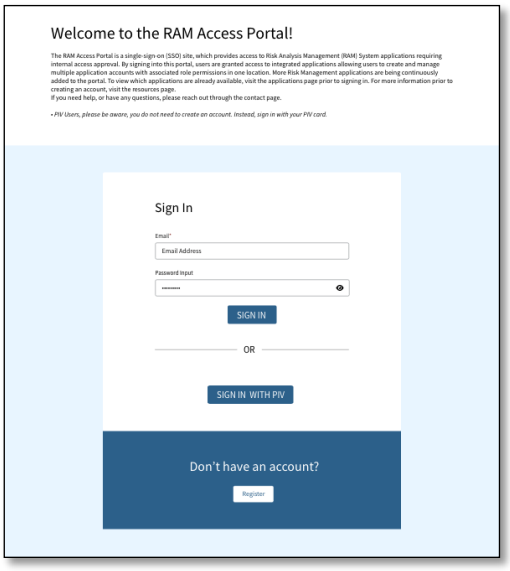




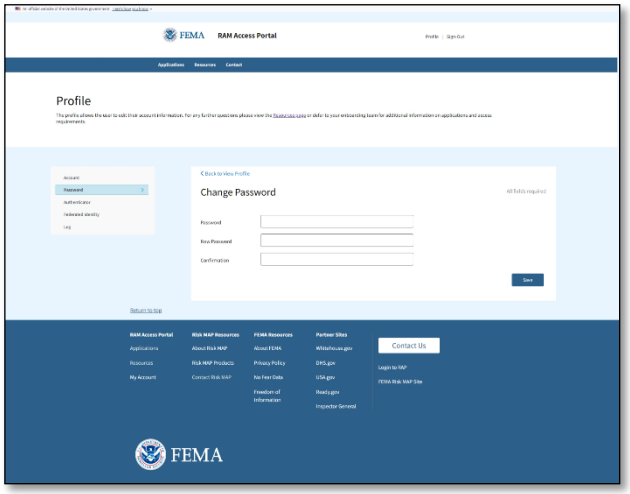
Follow the instructions to receive and enter the code either sent to your email or displayed on your authenticator app to complete the MFA process.

4.4. Signing into Your Account

Once you have created an account, they will have the ability to sign in. To sign in, select “Sign In” in the top right corner. For a non-PIV user, enter your username and password then click sign in. You will be asked to enter a one-time security code using the authenticator app or email to confirm your account. If you are a PIV user, click the Login with PIV button to log in.



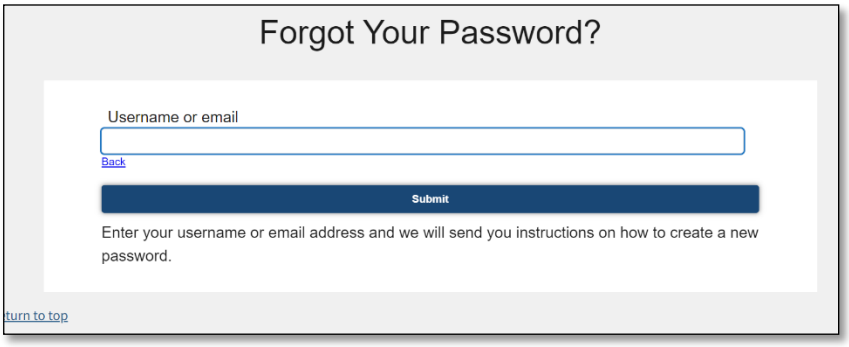
If you’re a non-PIV user, you can change your password from your Profile.



4.5. Resetting a Password

To reset a forgotten password, click “Forgot Password?” from the sign-in page, enter your username or email, and click submit. You will receive instructions on how to create a new password.

To change your password, click on the User icon in the top right corner and select Edit Profile from the drop-down menu Select Password from the left side bar. Enter the current password and the new password and press Submit.



4.6. Signing Out

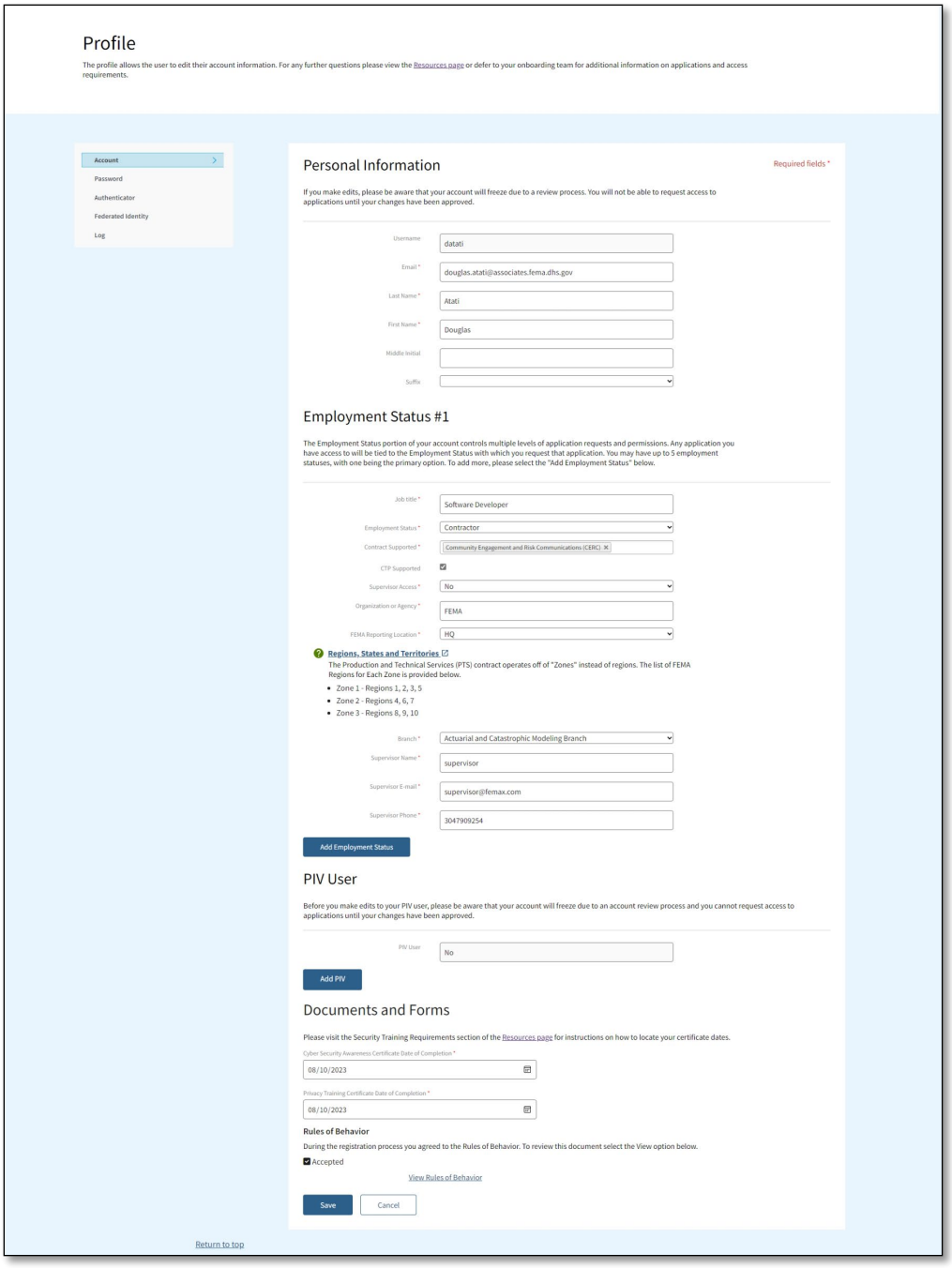
To log out, click on the “Sign Out” icon in the top right corner.

4.7. Viewing and Editing Your Profile Data

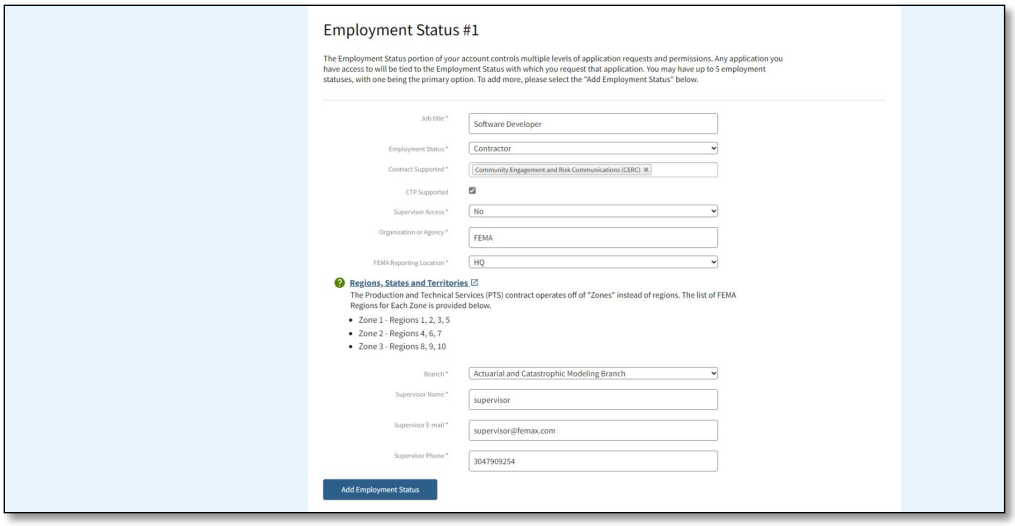
To view your Profile Data, click on the Profile icon in the top right corner.

On the Profile page, you will see the below screen. Here you can edit your Personal Information, Employment Status, transition a username/password account to a PIV account, and update your Cyber Security and Privacy Certificate information.

Profile edits will go through an account review process and the user will not be able to request access to applications until the changes have been approved



If you are transitioning to PIV but have an existing account, certain profile information, such as name and email, on your RAP profile will be automatically updated with information that comes from FEIMS.

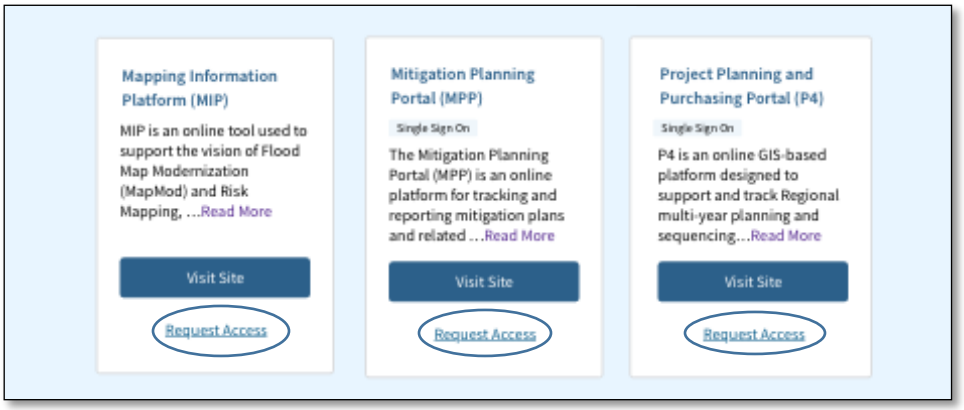


Note that you may update any of your Employment Statuses from this page. You may have up to five Employment Statuses on your profile at once. If you have multiple statuses, each application access will be tied to a specific Employment Status. When that status is removed, all application roles associated with the Employment Status will also be removed.

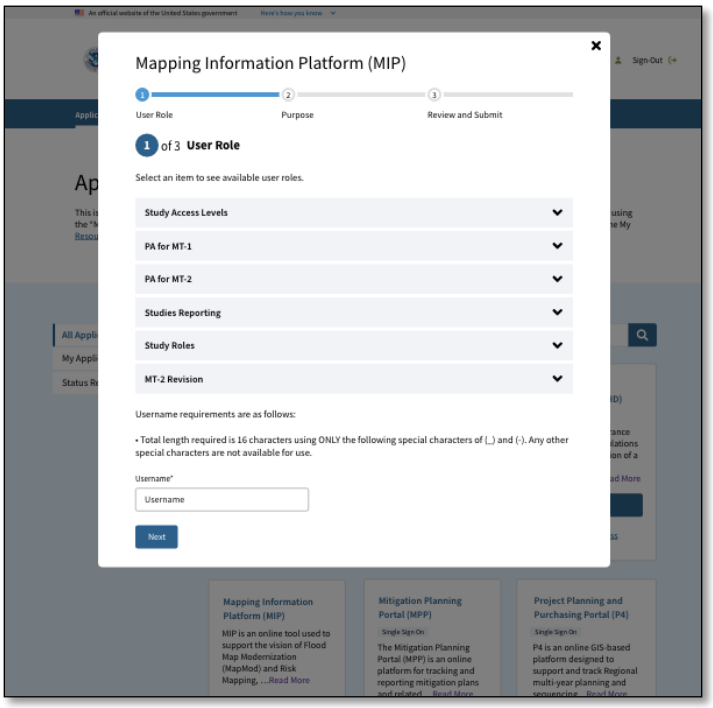
You can also update any device associated with Multi-Factor Authentication for the account by clicking on the Authenticator option on the Left menu.

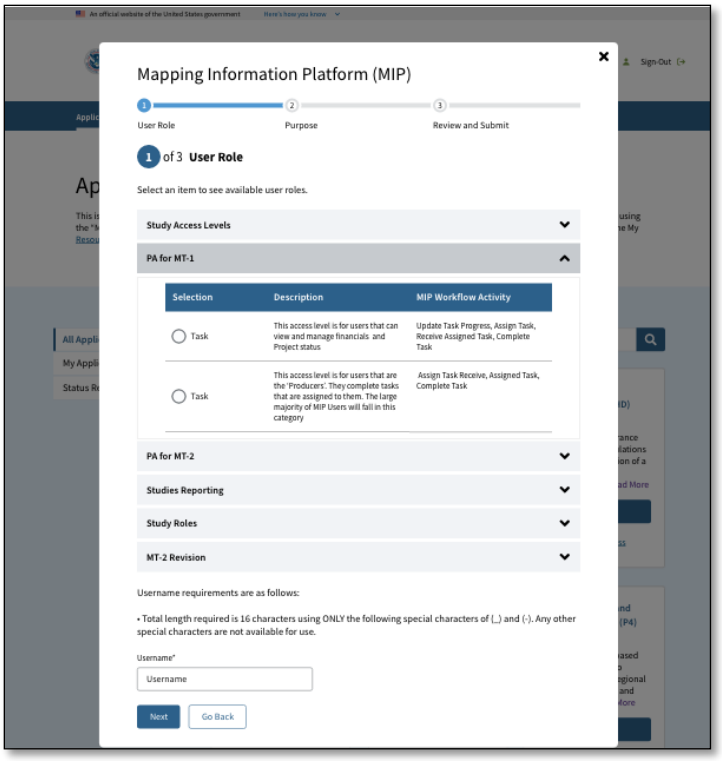
4.8. Requesting Access to an Application

To request access to an application, log in to RAP, select the “Applications” tab, and click “Request Access” beneath the application you need access to in the Catalog.

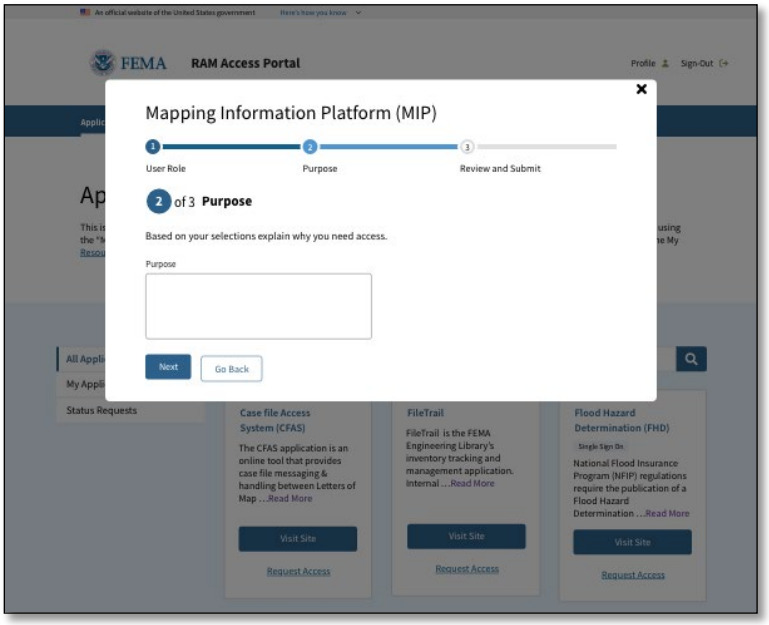


A pop-up will appear that guides you through the application request process.

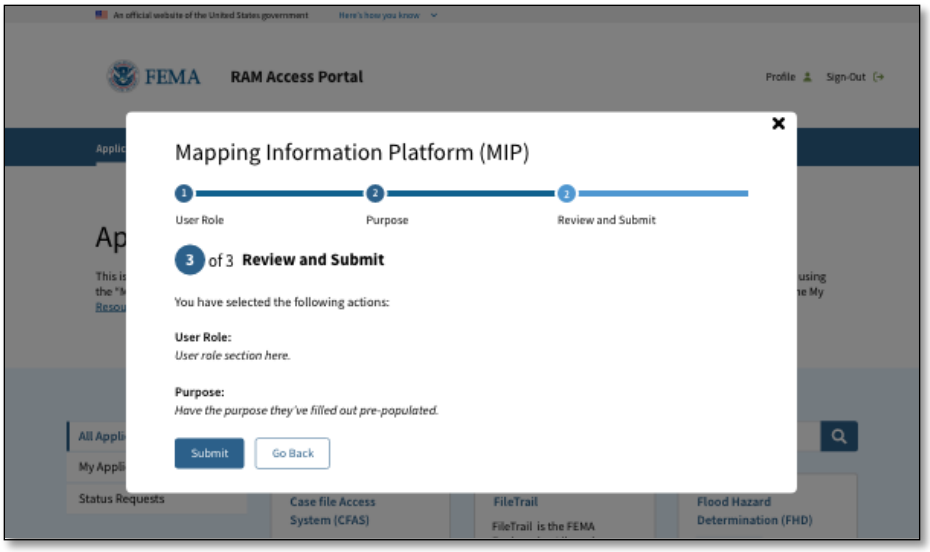




Note that the request process differs slightly depending on the application you are requesting. For example, as shown above for MIP, the user must choose a specific user role(s) to request.



You are required to enter a justification for your application request, which helps your supervisor and authorizer make their decision to approve or deny it.



After entering all necessary information, you'll have the opportunity to review and submit your access request.

The list below identifies the applications accessible through the RAP.

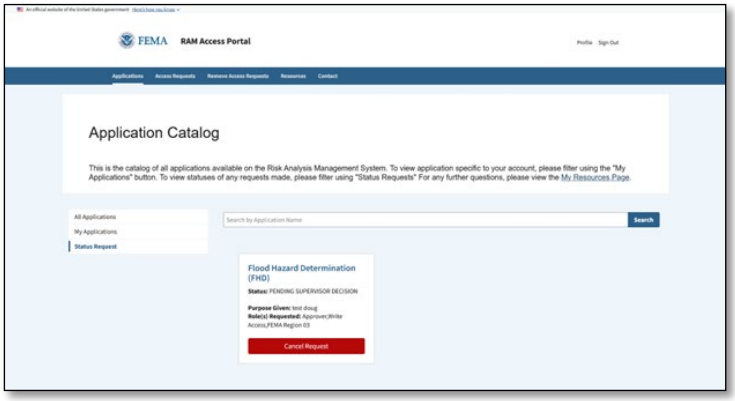
- Case File Access System (CFAS)
- FileTrail
- Flood Hazard Determination (FHD)
- Hazus Loss Library (HLL) – Data Import Dashboard
- Mapping Information Platform (MIP)
- Mitigation Planning Portal (MPP)
- Project Planning and Purchasing Portal (P4)
- Risk Management Directorate (RMD) SharePoint

User requests go through an approval process. The request will be routed to your supervisor for approval. Once the supervisor approves, it will be automatically routed to the authorizer. If the request is for an SSO-enabled application (currently MPP, P4, FHD, FileTrail, HLL Data Import Dashboard, and RMD SharePoint), the user will receive the roles automatically when the authorizer approves. For other applications, the request will then be routed to RM-IT Help who will update your access. You will receive an email at each step in this process and can monitor the current status for requests on the Status page.

Usernames will be displayed on Approval Requests within the Requests/Approvals section of RAP for PIV users. Supervisors, Authorizers, and Product Owners will be able to see the username for requests they are approving or rejecting.

4.9. Request Status

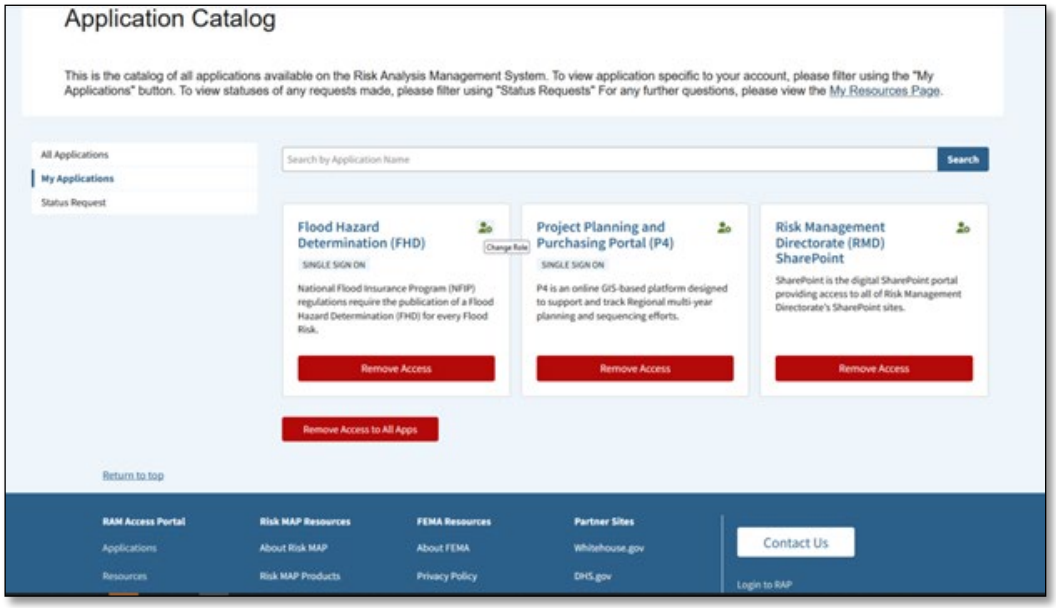
If you have an in-process request, it will display under the “Status Requests” section on the “Applications” page. It will display the status of the request and the information you selected when completing the request. Any in-process request will show up in this section. This can include Application requests, profile updates, change role requests, or access revocation requests.



4.10. Changing Role

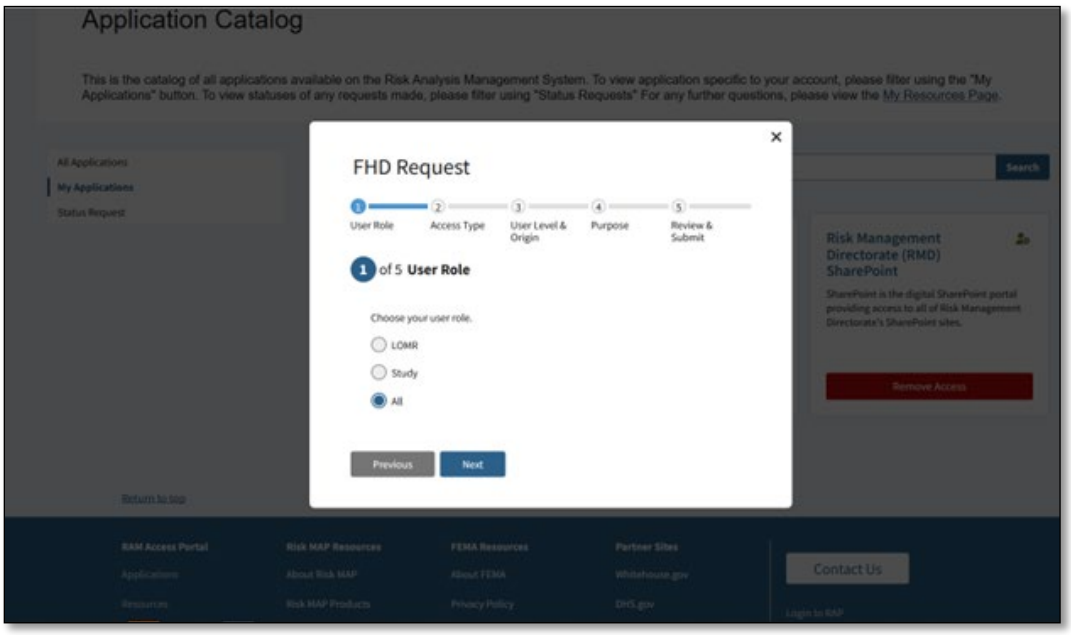
4.10.1. Adding or Updating a Role

If you have existing access to an application and need to add a role or update an existing role, navigate to the My Apps section on the Applications page.



Click the green icon in the corner of the box of the application for which you need to update your role. This will give you the option to Change role. Click that button.

A popup will appear that is very similar to the Application Request screen, but your current role will already be filled in. Pick the new role which corresponds with your needed access, enter your justification, and submit the request. This request will go through the same approval process as a standard application request and can be tracked on the status page. For non-SSO applications, you will also need to enter your application username along with the request.



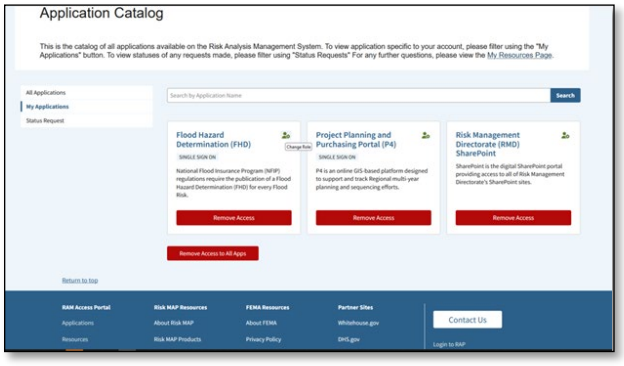
4.10.2. Removing a Role

To remove a role, select the application and uncheck the box next to the current role. Fill in the purpose of the change and submit the request.

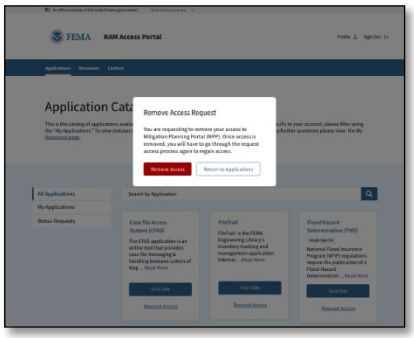
Users can also adjust their Access Type and User Level based on the change in role

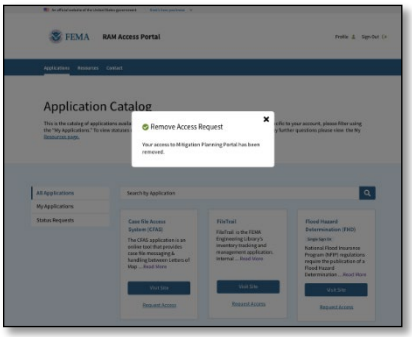
4.11. Removing Access

To remove access to an application, navigate to the “My Applications” section on the Applications page. Click the red “Remove Access” button at the bottom of the application to which you’re removing your access.



Once you click the “Remove Access” button, a confirmation window will appear. If you confirm to Remove Access to that application, a request will be submitted to RM-IT Help to remove your access. If the application is already SSO-enabled, your access will be removed automatically.



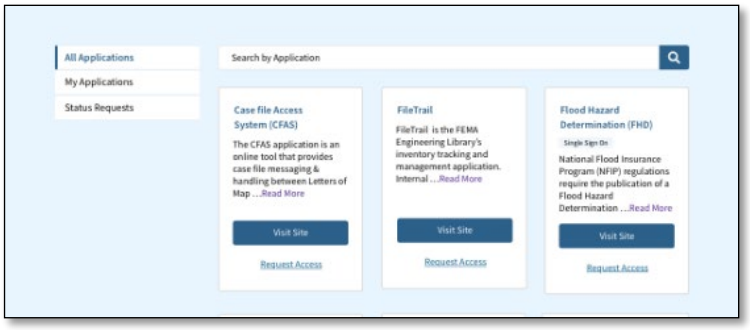


4.12. Single Sign-On Through RAP

4.12.1. MPP, P4, FHD, FileTrail, RMD Sharepoint and HLL Data Import Dashboard

MPP, P4, FHD, FileTrail, RMD SharePoint and HLL Data Import Dashboard are fully integrated with SSO in RAP. To access these applications from RAP, log in to RAP and navigate to the applications page. Here you will see a section at the top of the page called My Apps. This section will display any applications you have access to.

To access an application, click the “Visit Site” button in the box for the desired application. This will launch the selected application and automatically log you in.



If the user has an existing account with RAP, the user can also access an SSO-enabled application using the standard links. When the user accesses those links, the user will be redirected to the RAP landing page. Once the user signs in there, they will be redirected back to the application and logged in.

4.12.2. Other Applications

For every other non-SSO enabled application, you will be able to access the site from the Application Catalog once you’re logged into RAP. You will not be logged in automatically as these are not SSO enabled. You can also access these applications using the standard links.

5. Supervisors

Supervisors are federal employees, contract leads, primary managers, control access managers, or other employees who have the authority to attest to the user's/requester's need for access to the RAM Access Portal. Supervisors are the first line of defense to ensure secure access is granted to users.

The Supervisor is responsible for:

1. Providing initial approval or denial of their user/requester access request
2. Understanding and attesting to user/requester "need for access" and ensuring their compliance with system rules
3. Monitoring user access validity and currency, as well as compliance with all applicable contract clauses regarding access control or other information sharing agreements by providing oversight on:
    - Understanding and maintaining accurate records of their users' access needs
    - Ensuring completion and currency of cyber security, privacy training, and security agreements as a prerequisite for access to the system
    - Monitoring and enforcing authorized use of the system by their users/requesters
    - Timely initiation of the authorization revocation process for their users/requesters in the event access to PII is no longer needed, if violations have been committed regarding appropriate use, or if unauthorized accessing of PII has occurred

Supervisors **WILL** be required to request supervisor role access during RAP account registration or on their account profile. This request will be validated. Once approved, supervisor roles and responsibilities will be administered, and supervisors will then be granted access to additional approvals/requests tabs on the RAP dashboard. **A supervisor must be granted the RAP Supervisor role before a user can select them as their supervisor.**

5.1. Becoming a Supervisor

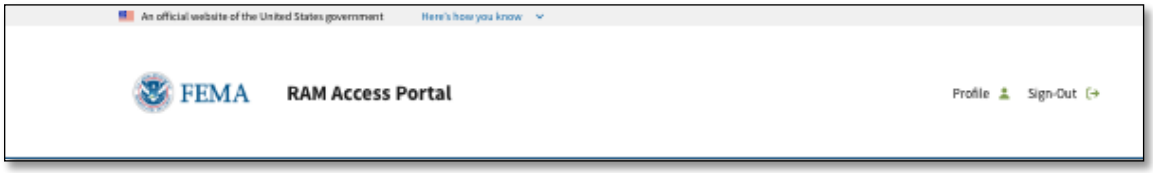
You can request supervisor access during registration while creating an account or from the Edit Profile screen.

5.1.1. Requesting During Registration

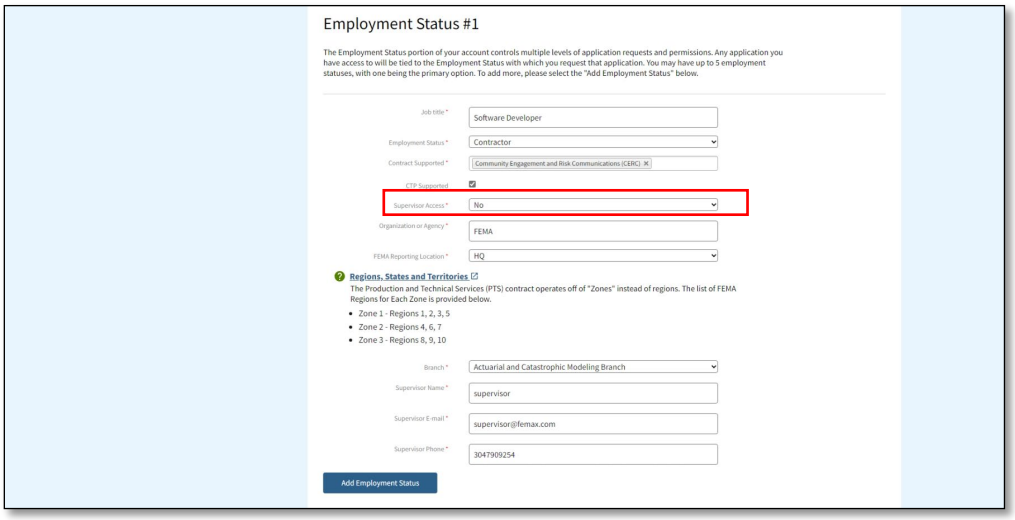
Please refer to section 4.2 for more information on how to register for a RAP account. On the registration page, under the employment status section, there is a field called Supervisor Access. When registering a new account, if you select “Yes” in that dropdown, a request will automatically be submitted to add the Supervisor role to your account.

5.1.2. Requesting for an Existing Account

Existing users can request Supervisor access through the Profile page. To access the Profile page, click on your profile icon in the top right corner of the navigation bar.

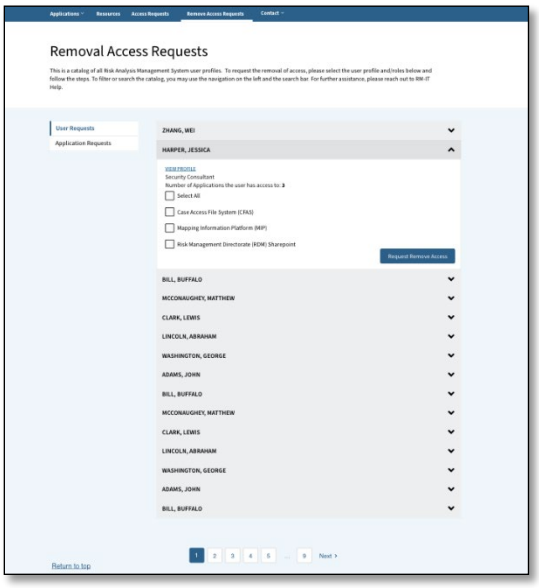


On the Edit Profile screen, the Supervisor Access Field is found under the Employment Status section. Supervisor access can be granted for any employment status. Select “Yes” for this dropdown and then click Save. A request to add a Supervisor role to your profile will be submitted.

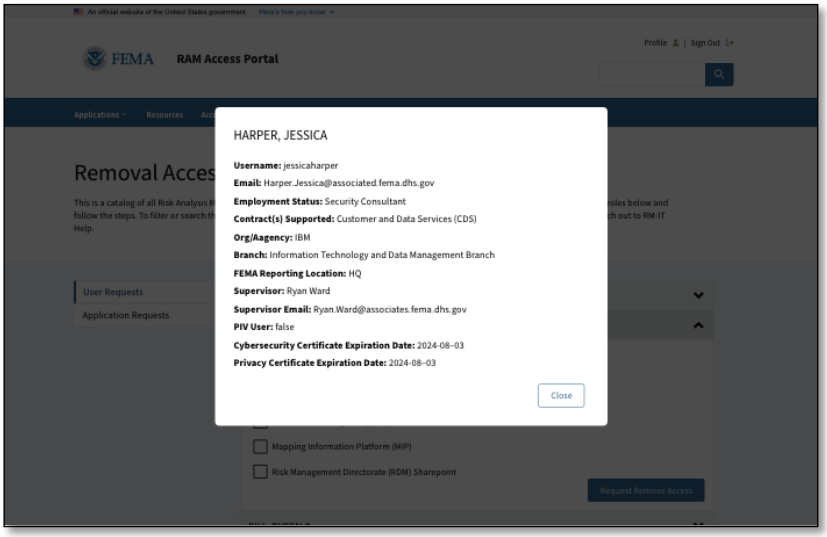


5.2. Revoke User Access

To request access to an application be revoked from a user that you supervise, log in to RAP and select Remove Access Requests from the header. This tab is not available for general users.

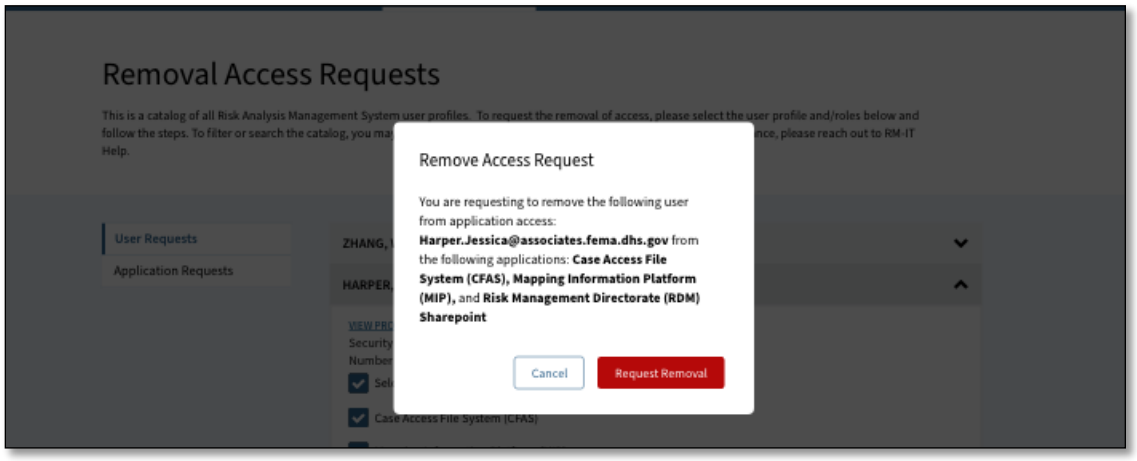


You can also search for access by a specific user by selecting the User View tab. The View Profile button on this page allows you to see details for a specific user.

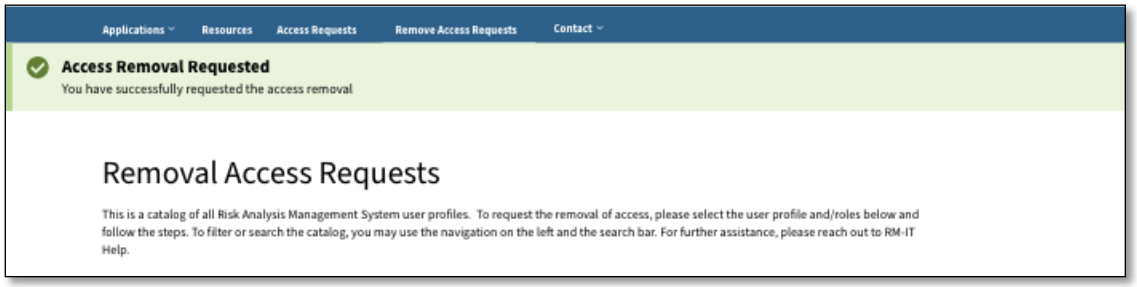


Under either the Application View or User View options, you can select the Select All checkbox or select individual applications to remove.

Once you select the access to be removed, press the Request Remove Access button. A pop-up will appear asking you to confirm your request.



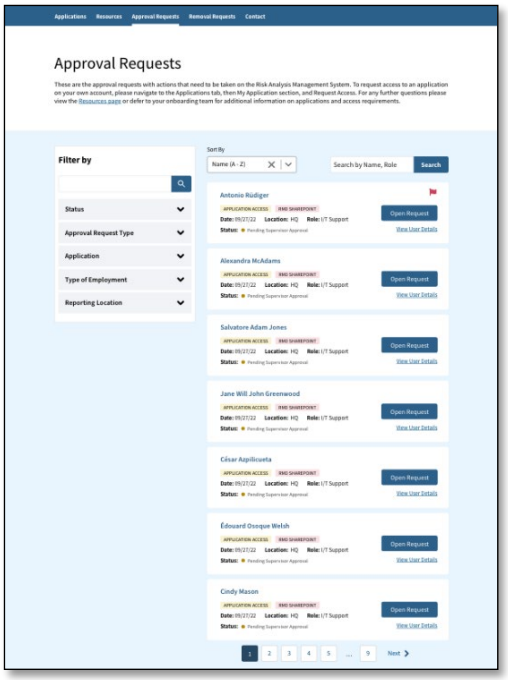
Once you confirm, the request will be submitted. For SSO enabled applications (currently MPP, P4, and FHD), the roles will be removed automatically. For other applications, a request will be submitted to RM-IT Help. You will receive an email notification once your request has been completed.



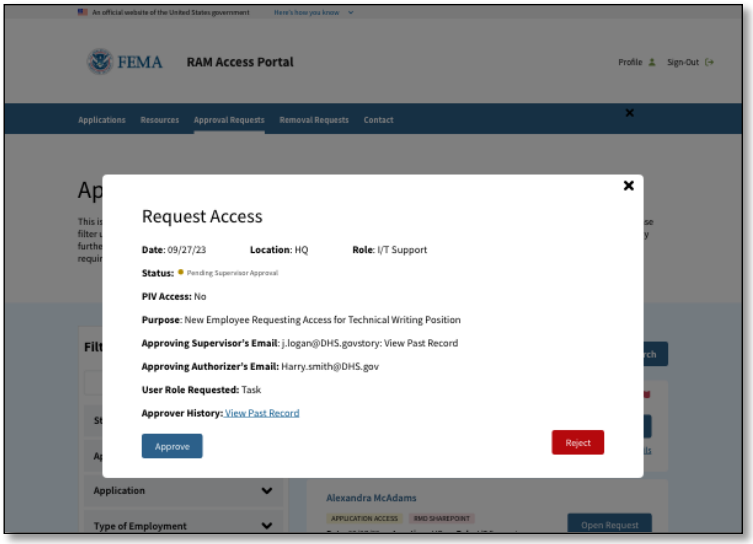
5.3. Responding to Requests

5.3.1. Application Access Requests

You will receive an email notifying you of the pending requests in your queue. You can click the link in the email or navigate to the RAP application and select the Requests/Approvals tab from the header. This tab is not available for general users.



If you click “Open Request,” the request will expand to show more information. It will also give you the option to view additional user details by clicking the View User Details button.



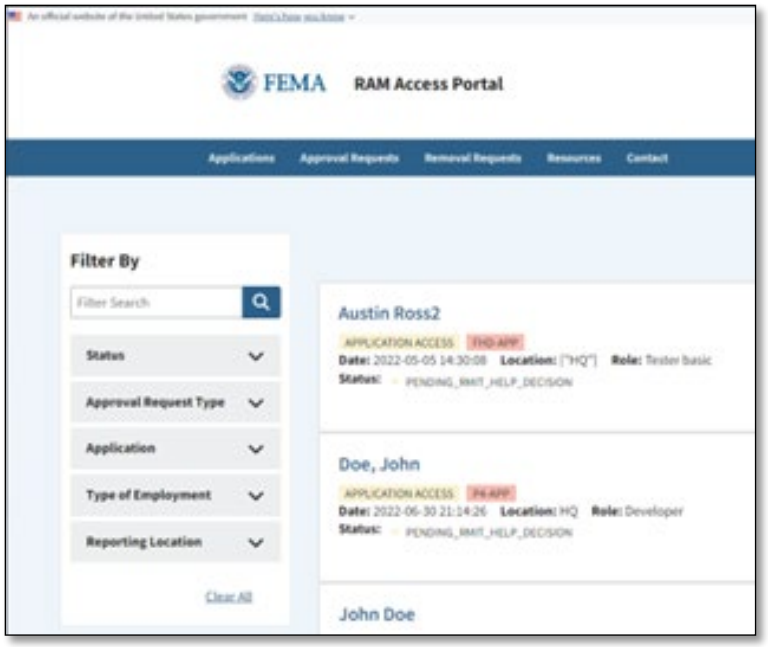
Once you are ready to advance the request, you can either select “Approve” or “Reject.” Each option will give you the opportunity to type in a comment to go along with your request. To Approve a request, click the approve button, enter your reasoning in the Comments box, and press Submit. This will advance the request to the Authorizer for their approval. If you Deny the request, it will be returned to the user with the reasoning for the denial.

5.3.2. Change Role Requests

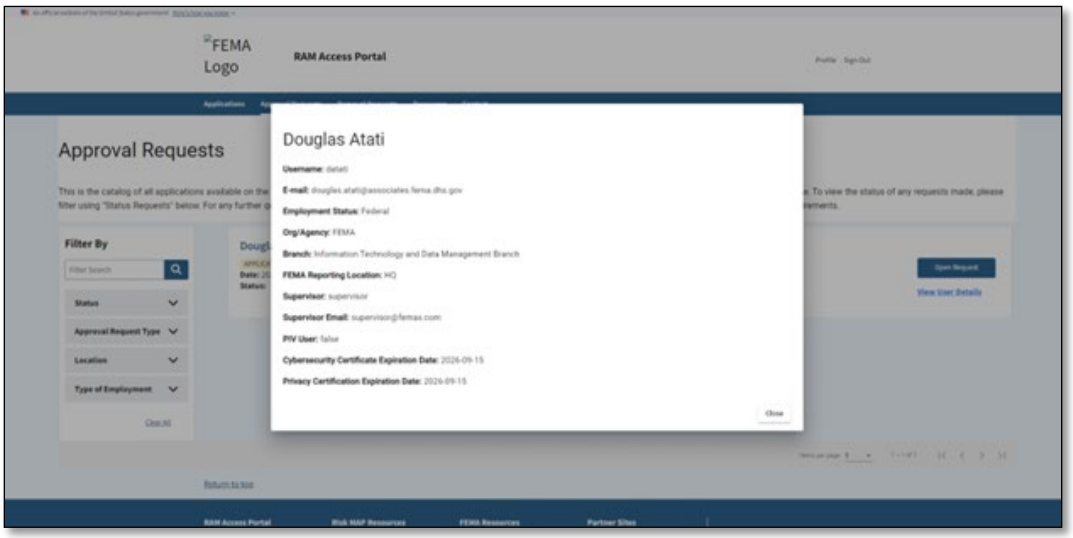
A user can also request to Change roles to an application. This request will work in the same way as an application access request for the Supervisor but will be marked as a Change Role request. Role requests must follow the same full procedure as application access requests.

5.3.3. Profile Update Requests

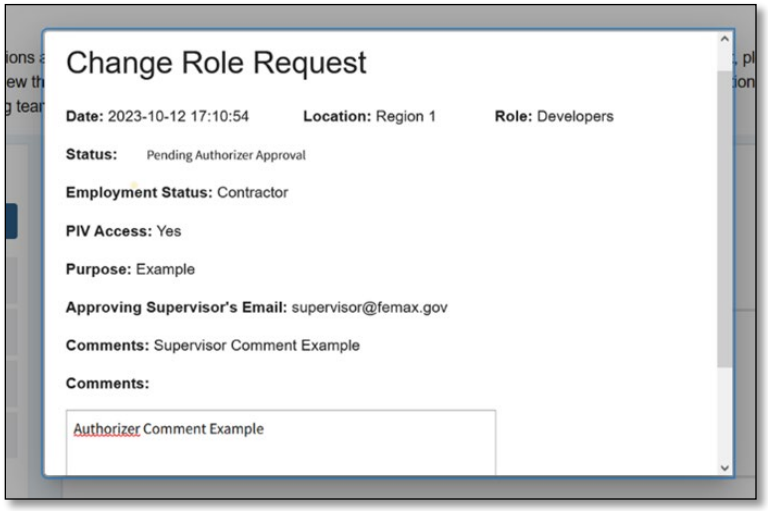
You will receive an email notifying you of a pending profile update request. You can click the link in the email or navigate to the RAP application and select the “Approval Requests” tab from the header.



On this page, you will see a list of pending requests. You can update how the requests are sorted using the Filter By drop down in the top left. Once you have found the profile update request you would like to approve, click on the box to expand the request. This allows you to see the request details. This will show you any field that has been updated, what the old value was, and what the user changed the field to. You can also click the View User Details button to see a more detailed summary of the user's information.



Once you are ready to advance the request, you can either select Approve or Deny. Each option will give you the opportunity to type in a comment to go along with your request. To Approve a request, click the approve button, enter your reasoning in the Comments box, and press Submit. This will advance the request to the Authorizer for their approval. If you Deny the request, it will be returned to the user with the reasoning for the denial. Once a Profile update is fully approved, the user's profile will be updated. If a request is denied, any profile changes will be reverted.

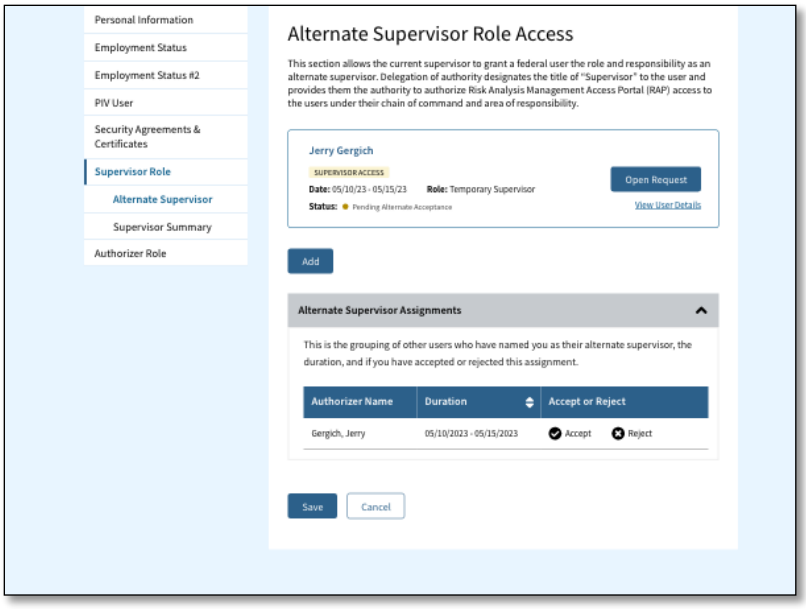


5.4. Alternate Supervisors

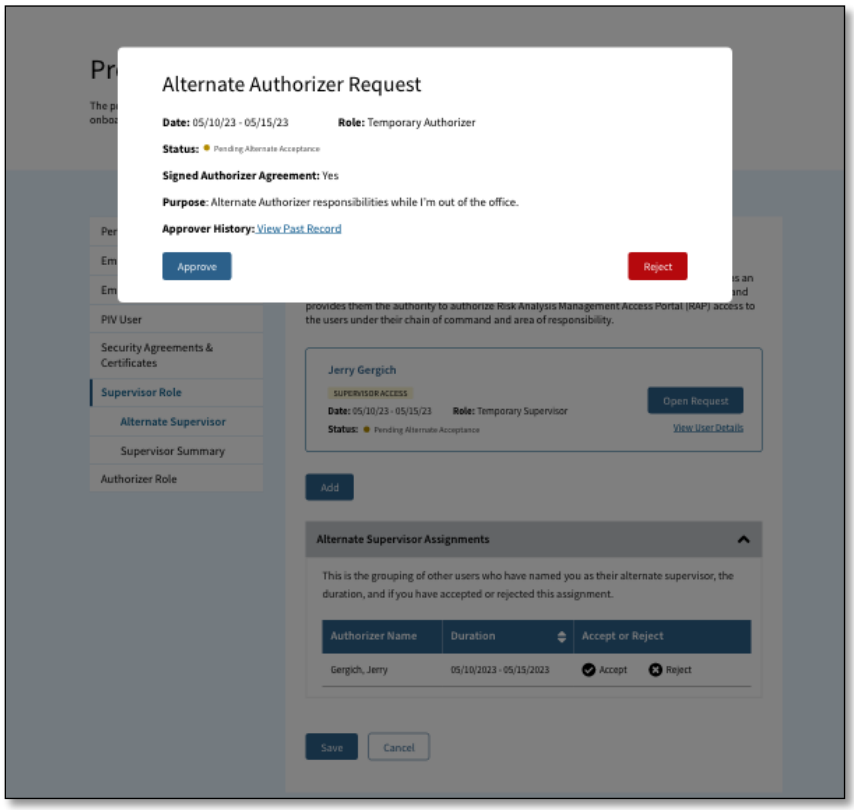
In cases where you are out of the office and unable to respond to requests from users you supervise, you can grant up to three other supervisors the role and responsibility to accept and deny requests for the period in which you're unavailable. Others can also request you as their alternate supervisor.

5.4.1. Being assigned as others' alternate supervisor

On the "Alternate Supervisor Role Access" page, you can view any supervisors who have requested you to be their alternate supervisor and for what duration.



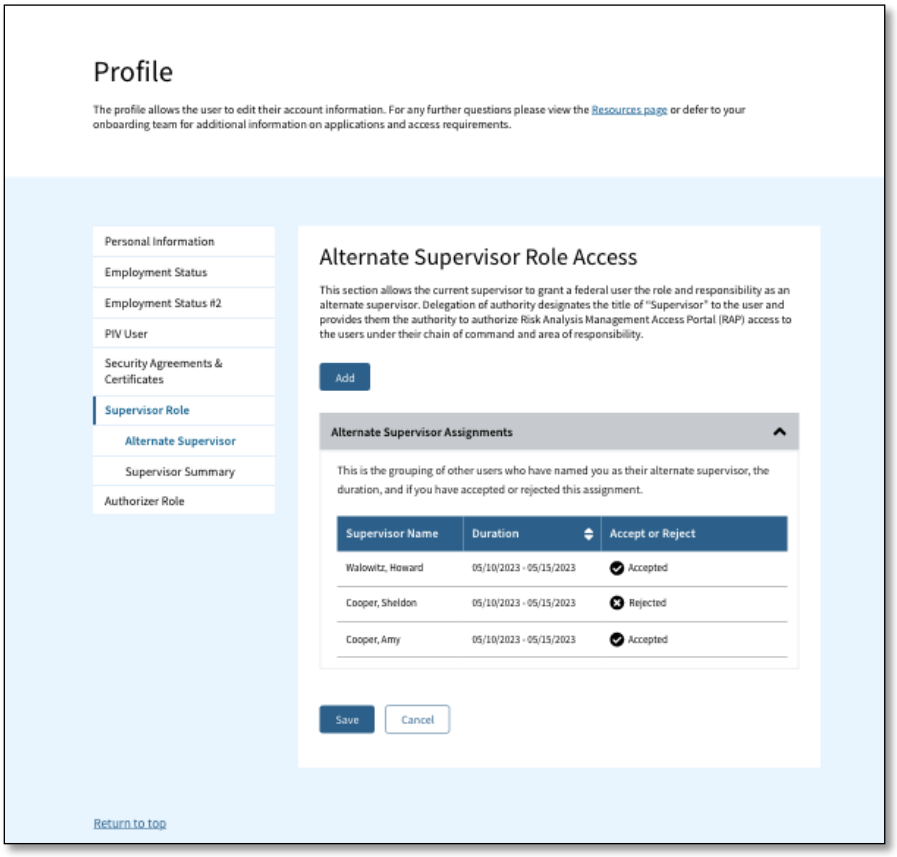
On the "Alternate Supervisor Role Access" page, you can see any requests you've received to be an alternate supervisor. Click the "Open Request" button to view request details.



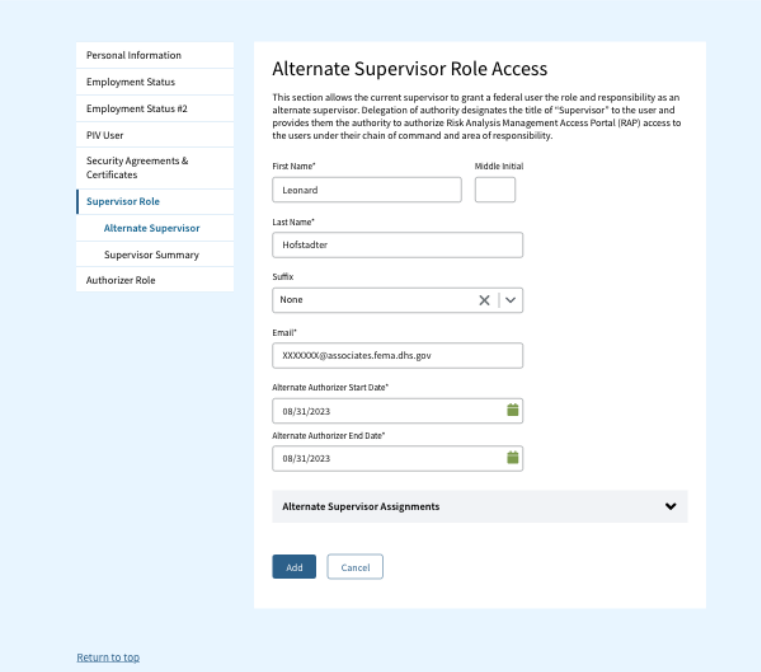
Depending on if you will be available and feel you are fit to be the person's alternate supervisor, choose "Approve" or "Reject."

5.4.2. Assigning an Alternate Supervisor

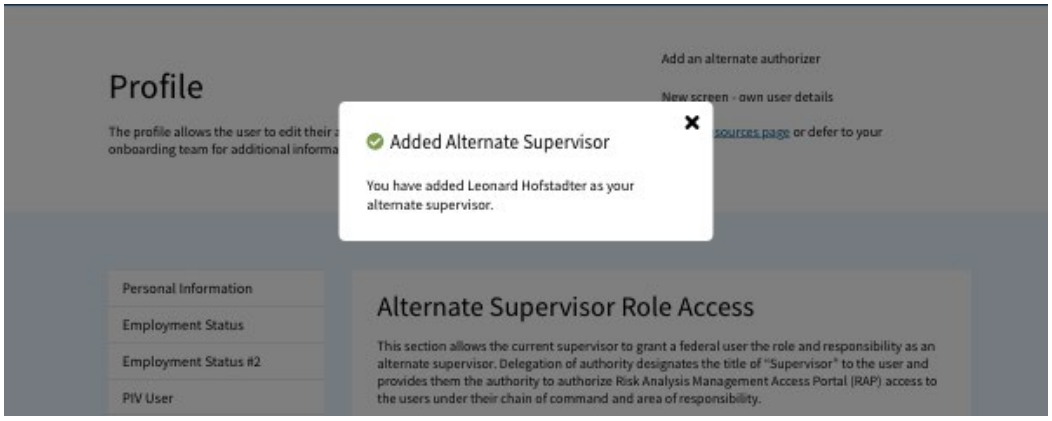
To designate others as your alternate supervisors, navigate to the "Alternate Supervisor Role Access" page. There is a button to "Add" alternate supervisors, as well as a list showing your previous supervisor requests, if any, and if the request was accepted or rejected.



If you click "Add," you'll be taken to a form to input information about your alternate supervisor and the time frame for which they'd assume your responsibilities.



After completing the form and again clicking "Add," a confirmation pop-up will appear. Note that the alternate supervisor must still accept the request through their own account, as shown in 5.4.1.



6. Authorizers

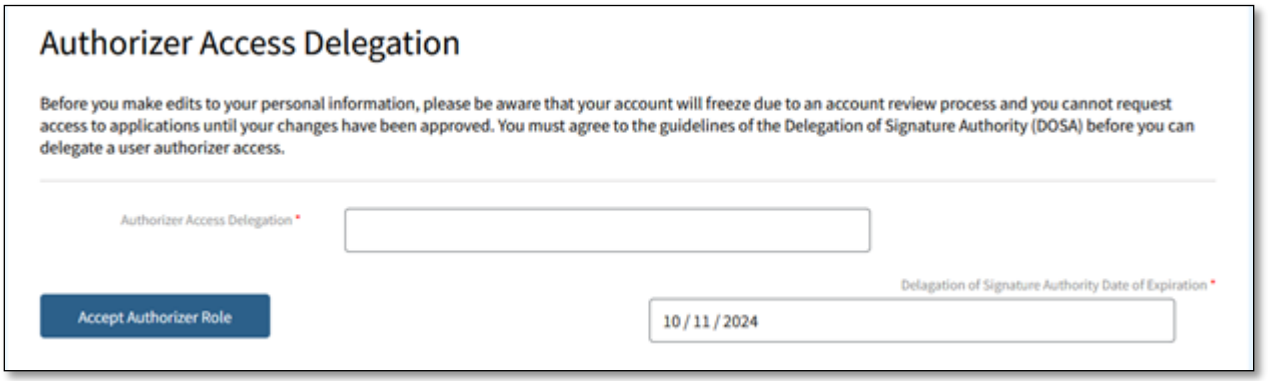
Authorizers are designated federal employees who serve as the Authorizer for the RAM Access Portal. The RAM System Owner is responsible for selecting the authorizers to assist in the authorization process.

The Authorizer is responsible for:

1. Providing final approval or denial of their users/requesters access request.
2. Verifying "need to access" and compliance with system rules as well as being able to support or defend them during any audit or review of system access.
3. Ensuring the monitoring of and compliance with all applicable contract clauses regarding access control or other information sharing agreements by providing oversight on:
    - Understanding and maintaining accurate records of their users' access needs
    - Ensuring completion and currency of cyber security, privacy training, and security agreements as a prerequisite for access to the system
    - Monitoring and enforcing authorized use of the system by their users/requesters
    - Timely initiation of the authorization revocation process for their users/requesters in the event access to PII is no longer needed, if violations have been committed regarding appropriate use, or if unauthorized accessing of PII has occurred

6.1. Authorizer Updates

If there is a change in authorizers, an existing authorizer has the ability request the authorizer role be added to another user's account. To do this, click on the profile icon in the top right corner of the screen and select Edit Profile. Anyone with an Authorizer role will have access to a special authorizer section of the profile page which will appear in the account section. If you input the email address of any user that needs an Authorizer role and press Save, a request will be submitted to add the role to their account. Once the user has the role, please let RM-IT Help know which employment area they are becoming the authorizer for so that they can ensure the correct requests are routed to them for approval.



You may also reach out to RM-IT Help to notify them of the change. Please provide the name and email of the new authorizer, the name of the old authorizer, and what Region or Branch they will be an authorizer for. The help desk will work with CDS to update this information and ger the new authorizer set up with the correct roles.

6.2. Revoke User Access

The process of revoking user access is the same for supervisors and authorizers. For detailed instructions, see **Section 5.2**.

6.3. Responding to Requests

The process of responding to requests is the same for supervisors and authorizers. Please refer to **Section 5.3** for detailed instructions.

6.4. Alternate Authorizers

In cases where you are out of the office and unable to respond to requests from users you authorize, you can grant another authorizer the role and responsibility to accept and deny requests for the period in which you're unavailable. Others can also request you as their alternate authorizer. Please refer to **Section 5.4**, as the process for authorizers is the same as for supervisors.

6.5. Authorizer Delegation of Authority

Every Authorizer needs to review the Delegation of Signature Authority at least once per year. If you are an Authorizer who does not have a review date within the past year, your account will be locked until the review is complete

To complete the review, access the profile page by clicking the profile icon on the top right corner of the screen and selecting Edit Profile. Authorizers have a special section of the profile screen where you can review the Delegation of Authority letter.

In order to complete your review, please click the blue button that says “Accept SA”. Upon clicking the button, a pop-up will appear with the Delegation of Signature Authority.

Review the letter and then click the checkbox to Accept and Acknowledge the review. You will then be able to click the Accept button. The Delegation of Signature Authority Date of Expiration will then

be updated to one year from the current date. You may review the delegation letter again at any point to ensure that you are always up to date with your review.

7. Appendix

7.1. RAP Application Catalog

The table below details the list of applications accessible through the RAP.

Risk Analysis Management System	Description
Case File Access System (CFAS)	CFAS is an online tool that provides file synching between Letters of Map Change (LOMC) Clearing house and CFAS
FileTrail	File Trail is the FEMA Engineering Library's inventory tracking and management application. Internal requesters (FEMA staff, contract providers, and CTPs) may use File Trail as the primary means for requesting NFIP technical and administrative data from the Engineering Library.
Flood Hazard Determination (FHD)	National Flood Insurance Program (NFIP) regulations require the publication of a Flood Hazard Determination (FHD) notice for every Flood Risk Project, including Physical Map Revisions (PMRs), and LOMRs that include new and/or modified FHDs. The FHD tool allows the user to create FHD notices quickly and consistently. Users enter information specific to a Flood Risk Project or LOMR to create the notice and this information then generates the appropriately formatted html notices for FEMA's Flood Hazard Mapping Website. This data also feeds the interim and proposed notice Federal Register docket templates that FEMA HQ uses for Federal Register publication
Hazus Loss Library (HLL) - Data Import Dashboard	The Hazus Loss Library Data Import Dashboard is the platform for the Hazus team to upload Hazus analyses into the Hazus Loss Library. The Hazus Loss Library is a free, public, and centralized repository for accessing natural hazard risk information, curated by FEMA's Natural Hazards Risk Assessment Program (NHRAP), and can be accessed outside of RAP. The Data Import Dashboard is intended for uploads only, not access of the public application.
Mapping Information Platform (MIP)	MIP is an online tool used to support the vision of Flood Map Modernization (MapMod) and Risk Mapping, Assessment and Planning (Risk MAP) to record progress and upload data for a study project. The MIP Studies Workflow is a series of tasks and activities completed by

	the PTS or CTP, the Regional Service Center (RSC) and FEMA to complete a studies project. The MIP also documents and tracks the MT-1 and MT-2 workflows
Mitigation Planning Portal (MPP)	The Mitigation Planning Portal (MPP) is an online platform for tracking and reporting mitigation plans and related data elements across all ten Federal Emergency Management Agency (FEMA) Regions. Users can enter mitigation plan and jurisdiction data into this single database system and use the MPP Reporting System to query information
Project Planning and Purchasing Portal (P4)	P4 is an online GIS-based platform designed to support and track Regional multi-year planning and sequencing efforts. The system allows for the creation and tracking of projects with specific geographical footprints. These projects are then comprised of multiple geographically tagged purchases which contain scope, quantity, and cost information. The information is used to generate procurement information, specifically and ordering template and a Statement of Priorities (SOP) for Planned purchases. P4 also capture planned and realized program metrics (deployment & NVUE initiated) and generates national and regional reports on current and planned progress
Risk Management Directorate (RMD) SharePoint	SharePoint is the digital SharePoint portal providing access to all of Risk Management Directorate's SharePoint sites. The intent of the RMD SharePoint portal is to encourage information sharing and collaboration across all program teams. Sites are represented across all 10 Regions, as well as the HQ RMD Divisions: Communications and Management Division, Engineering and Modeling Division, and the Planning, Safety, and Building Sciences Division