This page intentionally left blank
# Table of Contents

1. **How to Use this Guide** ................................................................................................. 1

2. **Types of Users** ........................................................................................................ 2
   2.1. Types of RAM Users: ................................................................................................. 2
   2.2. RAP User Roles ......................................................................................................... 2

3. **Reference Information** ............................................................................................ 3
   3.1. First Accessing RAP ................................................................................................. 3
   3.2. Applications Catalog ............................................................................................... 4
   3.3. Resources Page ........................................................................................................ 5
   3.4. Contact Support Form ............................................................................................. 6

4. **User Functionality** ................................................................................................ 7
   4.1. Who Needs to Create an Account? ........................................................................... 7
   4.2. Creating an Account ................................................................................................. 7
   4.3. Multi-Factor Authentication ..................................................................................... 10
   4.4. Signing into Your Account ....................................................................................... 10
   4.5. Resetting a Password .............................................................................................. 11
   4.6. Signing Out .............................................................................................................. 12
   4.7. Viewing and Editing Your Profile Data ..................................................................... 13
   4.8. Requesting Access to an Application ....................................................................... 14
   4.9. Request Status ........................................................................................................ 16
   4.10. Changing Role ....................................................................................................... 17
      4.10.1. Adding a Role .................................................................................................. 17
      4.10.2. Removing a Role ............................................................................................. 18
   4.11. Removing Access .................................................................................................. 18
   4.12. Accessing an Application Through RAP ................................................................. 18
      4.12.1. MPP and P4 .................................................................................................. 18
      4.12.2. Other Applications ......................................................................................... 19

5. **Supervisors** ........................................................................................................... 20
5.1. Becoming a Supervisor .......................................................................................................... 21
  5.1.1. Requesting During Registration .............................................................................. 21
  5.1.2. Requesting for an Existing Account ...................................................................... 21
5.2. Revoke User Access ........................................................................................................... 23
5.3. Responding to Requests ...................................................................................................... 24
  5.3.1. Application Access Requests ................................................................................. 24
  5.3.2. Change Role Requests ........................................................................................... 26
  5.3.3. Profile Update Requests ........................................................................................ 27

6. Authorizers ............................................................................................................................... 30
  6.1. Authorizer Updates .......................................................................................................... 31
    6.1.1. Initial RAP Launch .............................................................................................. 31
    6.1.2. Authorizer Changes ............................................................................................ 31
  6.2. Revoke User Access .......................................................................................................... 31
  6.3. Responding to Requests .................................................................................................. 33
    6.3.1. Application Access Requests ................................................................................. 33
    6.3.2. Change Role Requests .......................................................................................... 35
    6.3.3. Profile Update Requests ........................................................................................ 36

7. Appendix .................................................................................................................................. 39
  7.1. RAP Application Catalog ................................................................................................... 39
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 internal access approval. 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 application.

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. Types of Users

The RAM Access Portal is not intended for public use. FEMA employees and partners (contractors, CTPs, and interagency users) requiring access to the Risk Analysis Management (RAM) system applications may register.

2.1. Types of RAM Users:

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

2.2. RAP User Roles

- 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 (listed below), and a Sign In or Profile icon at the far right, which takes you back to the main landing page above.

- **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 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. For users without a RAP account, you can still see the Catalog and application information without logging in. This page can be accessed by clicking the Applications tab in the navigation bar.

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

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

The Contact Support 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 RM-IT Help 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.
4. User Functionality

4.1. Who Needs to Create an Account?

- All current users of P4 and MPP will have their accounts migrated into the RAP system. Any new users will need to create a RAP account and request access

- All new users requesting first time access to any application in RAM system

- 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, head to the login screen. If you are a non-PIV user, click the Register link under the Sign In button from the screenshot below. If you are a PIV user, click the Login With PIV button at the top of the box and it will redirect you to a page which allows you to enter in the rest of your profile information.

Welcome to the RAM Access Portal!

By logging in here, you will be able to access all applications that RAM has to offer. If you would like to see the catalog of applications before logging in, please click here.

Login with Username and Password

Username or email
Password

Remember me
Forgot Password?

Sign In

Next user? Register

Complete all the required fields on the registration form below, submit it, and if completed correctly, your new account will be created. Users must enter their certificate expiration dates and read and accept the Rules of Behavior by clicking the View button under the Rules of Behavior label. 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 a user to request Supervisor access upon registration.

Be sure to select if you are PIV or Non-PIV User
If a user has more than one role that they need to capture, they 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. A user will be able to edit, add, or remove employment statuses after creating an account as well.
4.3. Multi-Factor Authentication

After a user Registers an account, non-PIV users only will be required to set up Multi-Factor Authentication. After downloading one of the recommended authenticators (see below screenshot) or another of their choice, the user can scan the QR code, set up their device, and enter in the code to access the RAP system. This is not required for PIV users.

![Mobile Authenticator Setup](image)

4.4. Signing into Your Account

Once the user has an account created, they will have the ability to sign in. To sign in, select Sign In in the top right corner. This will take the user to the Sign In page. For a non-PIV user, enter your username and password then click sign in. The user will be asked to enter a one-time security code using the authenticator app the user connected when creating their account. If you are a PIV user, click the Login with PIV button to log in.
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 View Profile from the drop down and click Edit Profile. 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 profile icon in the top right corner and then select Sign Out from the drop down.
4.7. Viewing and Editing Your Profile Data

To view User Profile Data, click on the User icon in the top right corner and select Edit Profile from the drop down.

After clicking on Edit Profile, the user will see the below screen. Here the User can edit their Personal Information, Employment Status, add PIV, and update their 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.
The user 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 into RAP, select the Applications tab, and click the Request Access button next to the application you need access to in the Catalog. A popup will appear that allows you to enter a justification for your request, select the role you are requesting access to, and select the geography you need access for if applicable. Complete the form and click submit.
Once you submit the request, this request will need to go through the 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 and P4), 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.
4.9. Request Status

If a User has an in-process request, it will display under the Status of Requests section on the Applications page. This is found just under the My Applications section. It will display the status of the request and the information the user 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.

The Status of Requests section is hidden if there are no requests in process.
4.10. Changing Role

4.10.1. Adding a Role

To add a role, navigate to the My Apps section on the Applications page. Click the three dots in the corner of the box for the application you need to update your role for. 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.
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 Apps section on the Applications page. Click the three dots in the corner of the box for the application you need to update. This will give you the option to Remove 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 (currently MPP and P4), your access will be removed automatically.

4.12. Accessing an Application Through RAP

4.12.1. MPP and P4

MPP and P4 are both fully integrated with RAP with SSO. 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.
If you need to access an application, click the Launch App 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 MPP and P4 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 application other than MPP and P4, you will be able to access the site from the Catalog on the Applications page once 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 another employee that holds the role of supervisor and has the authority to attest to the user/requesters need to know 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 of 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.
5.1. Becoming a Supervisor

In order to gain the supervisor role, you can request supervisor access during registration while creating an account or from the Edit Profile screen.

5.1.1. Requesting During Registration

Please reference 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

To access the Edit Profile page, click on your profile icon in the top right corner of the navigation bar and select Edit Profile.
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.

<table>
<thead>
<tr>
<th>Employment Status #1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before you make edits to your personal information, please be aware that your account will freeze due to an account review process and you cannot request access to applications until your changes have been approved.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supervisor Access</th>
<th>Yes</th>
</tr>
</thead>
</table>

Documents and Forms:

Expiration Date of Cyber Security Certificate: 06/01/2022
Expiration Date of Privacy Certificate: 06/28/2022
5.2. Revoke User Access

Once a user becomes a Supervisor, they will have access to two new tabs on the top navigation.

To request access to an application be revoked from a user that you supervise, log into RAP and select Request Remove Access from the header. You can search for access by application to search for the user that you need to revoke by selecting the Application View tab.

You can also search for access by a specific user by selecting the User View tab. The View Full Profile button on this page allows you to see details for a specific user.
For an application or user, you can select the Select All checkbox or select an individual application 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 and P4), 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

When a new request is in your queue, you will receive an email notifying you of the pending request. You can click the link in the email or navigate to the RAP application and select the Requests/Approvals tab from the header. This is the other additional tab that is not available for general users.
On this page, you will see a list of pending requests. You can update how the requests are sorted using the Sort By drop down in the top right. Once you have found the request you would like to approve, click on the box to expand the request.

This allows you to see the request details. 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.

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 as
indicated below. Change Role requests must follow the same full procedure as application access requests.

5.3.3. Profile Update Requests

When a new profile update is in your queue, you will receive an email notifying you of the pending request. You can click the link in the email or navigate to the RAP application and select the Requests/Approvals tab from the header. This is the other additional tab that is not available for general users.

On this page, you will see a list of pending requests. You can update how the requests are sorted using the Sort By drop down in the top right. 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.
6. Authorizers

Authorizers are designated federal employees 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

6.1.1. Initial RAP Launch

For the initial launch of RAP, an account will be created by CDS for each authorizer with the Authorizer role already added. When you log in for the first time, select the Sign in with PIV option on the Landing Page.

Once you enter your PIN, you will receive the option to merge your PIV information with an existing account. Select to merge the accounts. You will then be able to fill in the rest of your profile information and access your account with the correct roles already loaded. Please see section 4.2 for more information on the registration screen.

6.1.2. Authorizer Changes

If there is a change in authorizers, please 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 get the new authorizer set up with the correct roles.

6.2. Revoke User Access

Once a user becomes an Authorizer, they will have access to two new tabs on the top navigation.

To request access to an application be revoked from a user, log into RAP and select Request Remove Access from the header. You can search for access by application to search for the user that you need to revoke by selecting the Application View tab.
You can also search for access by a specific user by selecting the User View tab. The View Full Profile button on this page allows you to see details for a specific user.

For an application or user, you can select the Select All checkbox or select an individual application 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 and P4), 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.
6.3. Responding to Requests

6.3.1. Application Access Requests

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

On this page, you will see a list of pending requests. You can update how the requests are sorted using the Sort By drop down in the top right. Once you have found the request you would like to approve, click on the box to expand the request.
This allows you to see the request details. 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. For SSO enabled applications (currently MPP and P4), this will grant the user the approved roles automatically. For other applications, this will submit a request to RM-IT Help to update the access. If you Deny the request, it will be returned to the user with the reasoning for the denial.

6.3.2. **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 as
indicated below. Change Role requests must follow the same full procedure as application access requests.

6.3.3. Profile Update Requests

When a new profile update is in your queue, you will receive an email notifying you of the pending request. You can click the link in the email or navigate to the RAP application and select the Requests/Approvals tab from the header. This is the other additional tab that is not available for general users.

On this page, you will see a list of pending requests. You can update how the requests are sorted using the Sort By drop down in the top right. 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 respond to 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 finalize the request and update the user’s profile. If you Deny the request, it will be returned to the user with the reasoning for the denial. If a request is denied, any profile changes will be reverted.
Approve Request

You are about to approve access to John Doe for with user role:

Comments:

[Submit]
7. Appendix

7.1. RAP Application Catalog

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

<table>
<thead>
<tr>
<th>Risk Analysis Management System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case File Access System (CFAS)</td>
<td>CFAS is an online tool that provides file synching between Letters of Map Change (LOMC) Clearing house and CFAS</td>
</tr>
<tr>
<td>Flood Hazard Determination (FHD)</td>
<td>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</td>
</tr>
<tr>
<td>Mapping Information Platform (MIP)</td>
<td>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</td>
</tr>
<tr>
<td>Mitigation Planning Portal (MPP)</td>
<td>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</td>
</tr>
<tr>
<td><strong>Project Planning and Purchasing Portal (P4)</strong></td>
<td>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 &amp; NVUE initiated) and generates national and regional reports on current and planned progress</td>
</tr>
<tr>
<td><strong>Risk Management Directorate (RMD) SharePoint</strong></td>
<td>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</td>
</tr>
</tbody>
</table>