Identity Management Approach

Overview

Florida PALM will use an enterprise IAM tool to provide identity management for Florida PALM users. Florida PALM's authentication approach will be similar to how the STMS authenticates agency users. For agencies using an identity provider to authenticate their users, Florida PALM will use a standards-based authentication protocol such as Open Authentication 2 (OAUTH2), OpenID Connect (OIDC), or Security Assertion Markup Language (SAML2) to interface with identity providers. The Project plans to offer a federated sign-in option to agencies where agencies may use their identity provider to authenticate users in Florida PALM. Agencies will be responsible for identity management and authentication controls (e.g. password policies) for their users, as well as for configuring and maintaining their identity provider interface with Florida PALM. If your agency does not have an identity provider, please contact your Readiness Coordinator for more information.

Agencies will retain full-control over their agency's user-base. The following account administrative functions will be maintained and controlled through your agency's identity provider:

- Account creation
- Account deactivation/deprovisioning
- Password management functionality
- Account lock and unlocking
    - Any additional security mechanisms that are currently provided by your agency such as Multifactor authentication offering
- Device/workstation management

In addition, agencies will be responsible for managing user access to functionality within the Florida PALM Solution. Future activities will occur for role mapping and user access management.

Agency IAM Activities

You are encouraged to use the information gathered when responding to the Identity Provider Questionnaire (MRW Task TECH08) and collaborate within your agency to define the activities to design and document IAM activities. Existing Change Champion Network activities, including recurring Readiness Touchpoints and MRW tasks, may be leveraged to address your questions or provide new/updated Project information on IAM activities.

Activity	Timeline	Description
Confirm Identity Provider for Florida PALM	July 2020	Agencies will confirm which identity provider(s) will store or contain their users for Florida PALM.
Establish Identity Interface	August 2020	Agencies will provide credential and connection information to agency identity provider to Florida PALM.
Complete IAM Design Activities and Checklist	September 2020	Agencies will complete their IAM interface build activities, leveraging the Project-provided Identity Provider Interface Design and the IAM activities checklist.

Test IAM Interfaces	November 2020 – June 2021	The Project will conduct IAM testing with agencies beginning in November 2020. IAM interfaces will be tested during interface testing, user acceptance testing, and just prior to deployment.
Deploy IAM Interfaces	July 2021	Deployment is the final step in the IAM interface lifecycle wherein interface programs are deployed in support of the Florida PALM Solution for ongoing processing.