ACCOUNT MANAGEMENT PROCESS FOR FAI CSOD

October 2026

Account Management Process in FAI CSOD

1.0 Purpose

This process document outlines the guidelines to help Acquisition Workforce members, Acquisition Career Managers (ACMs), and Small Agency Representatives (SARs) ensure the accuracy of user profile records in the Federal Acquisition Institute (FAI) Cornerstone OnDemand (CSOD) system. Ensuring up-to-date profile information allows acquisition workforce members to meet certification and training requirements while supporting role transitions across agencies. By following this process, users, ACMs, and SARs can maintain data integrity, enhance workforce mobility, and reduce administrative burdens. This document supports government-wide human capital initiatives, enhances workforce planning, and ensures compliance with federal policies for acquisition workforce management.

2.0 Policy

The following policies establish the foundation for managing acquisition workforce training and development within the federal government:

- OMB, Policy Letter 05-01 (April 15, 2005): Defines workforce competencies and training requirements for federal acquisition professionals.
- OMB, OFPP, (September 3, 2013) Memorandum: Increasing Efficiencies in the Training, Development, and Management of the Acquisition Workforce

3.0 Roles and Responsibilities

Maintaining accurate and up-to-date user records in the FAI CSOD system is a shared responsibility among AWF users, ACM/SARs, and FAI. Each plays an essential role in ensuring the system supports the needs of a mobile and evolving federal AWF.

3.1 Acquisition Workforce System Users

Each user is responsible for maintaining the accuracy of their profile information in FAI CSOD. Users are responsible for:

- Ensuring their user profile information is current and accurately recorded, to support records management and compliance with federal AWF requirements.
- Updating organizational affiliation information whenever there is a change in employment status triggered by transfer, organizational move, separation from the government service, or retirement.

- Responding promptly to system notifications or reminders about their profile.

3.2 ACMs and SARs

ACMs and SARs are vital in bridging the gap between individual users and system oversight. Their responsibilities include:

- Periodically reviewing user profiles to ensure data is accurate and complete. Each agency is responsible for maintaining accurate and complete FAI CSOD user records.
- Communicating and enforcing profile maintenance requirements during onboarding, offboarding, and role changes.
- Supporting users in updating their profiles when changes occur, such as transfers to new organizations, retirements, or shifts into roles that no longer require FAI CSOD access.
- Removing users from elevated roles when a user's affiliated organization changes.
- Monitoring compliance with data quality requirements.

3.3 Federal Acquisition Institute (FAI)

FAI manages and oversees the overall functionality of the CSOD system to ensure it operates smoothly and supports all users. Specific responsibilities include:

- Providing FAI CSOD training materials and task aids to help ACMs, SARs, and users navigate and maintain their profiles.
- Ensuring high-quality data throughout the system by establishing clear data standards and monitoring compliance.
- Sending out system alerts and generating reports to help track and improve FAI CSOD user profile accuracy.
- Offering support to monitor and update user profiles, ensuring they reflect current roles, contact information, and organizational affiliations.

By working together, FAI, ACMs, SARs, and users can ensure the FAI CSOD system provides reliable, accurate information supporting the federal acquisition workforce's professional growth and mobility.

4.0 Process

This section outlines the processes for onboarding new users, maintaining FAI CSOD accounts, offboarding users, and facilitating employee transfers. These procedures ensure accurate and up-to-date user profiles while supporting smooth transitions as users join or leave the Federal AWF.

4.1 New FAI CSOD User Onboarding

Step 1: Verify Eligibility

In accordance with OFPP policy, new Federal AWF members are required to request an FAI CSOD account. New users must meet WarU account eligibility criteria and submit a System Authorization Access Request (SAAR) form for approval.

Agencies should provide general guidance on the system functionality and training record expectations to their AWF members.

Step 2: Account Creation

Once the SAAR is approved, WarU creates the account, and the user receives a welcome email with login details, system guidelines, and training task-aids. Based on the SAAR form input, WarU will populate six data fields in the user's FAI CSOD profile. See Section 6.3 Appendix C for details.

Step 3: Initial Setup

New users must log in to FAI CSOD and complete their user profile within 30 days of receiving account access. The profile updates will include validating and adding information on the user's organizational affiliation, job series, and contact details.

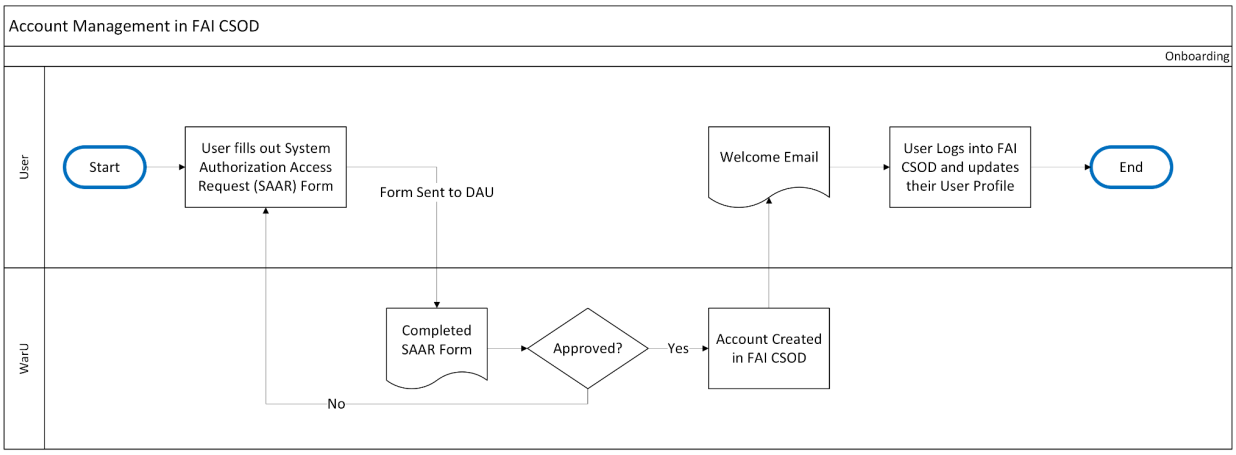


Figure 1. Onboarding Process

4.2 FAI CSOD Account Management

Users, ACMs, or SARs should perform the following tasks, as needed, to ensure user profiles remain accurate and current:

Profile Updates

- Users must update their profiles within 30 days of changes, such as a new job series, organizational transfer, or updated contact details.
- ACMs or SARs will review profiles quarterly to ensure compliance.

Inactivity Monitoring

***NOTE**: Okta is a secure authenticator application used for multi-factor authentication (MFA) and two-step verification. Okta policy as of July 2026 is to disable any Okta account that has not logged into Okta in 120 days. Since Okta is the login gate to FAI CSOD, if a user does not login into FAI CSOD every thirty days, their Okta account will be disabled and the user will be required to contact the WarU Help Desk to get the Okta account re-enabled. If the Okta account passes 450 days with no activity, it is deleted from Okta, requiring the user to submit a new SAAR form to get a new Okta account created. The WarU Help Desk will send out emails to Okta users near the 90 day mark of inactivity explaining that failure to login within 30 days will disable their Okta account.*

If a user has not recorded any learning activity on their transcript during the first 12 months of the current CLP period, FAI will send automated reminders quarterly to both the user and their ACM or SAR. The one year reminder outlines the CLP compliance requirements and FAI CSOD user activity expectations.

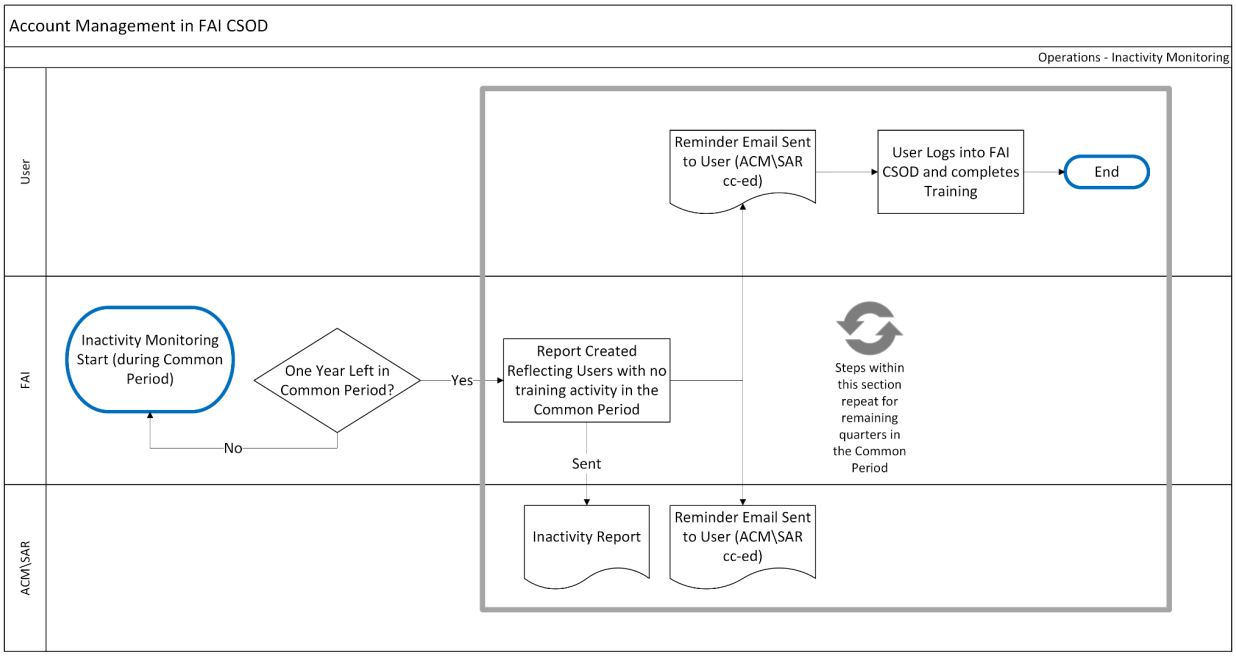


Figure 2. Inactivity Monitoring Process

Compliance Tracking

ACMs and SARs are expected to gain access and monitor user profile accuracy using reports and dashboards available at the FAI's Business Intelligence (BI) reporting webpage on GSA's Data 2 Decisions (D2D) portal. ACMs and SARs should meet FAI's Key Performance Indicators (KPIs) targets or be working on a corrective action plan. At a minimum, ACMs and SARs should conduct quarterly reviews to identify data quality issues and take corrective action to correct user profile inaccuracies.

Corrective Actions

ACMs and SARs are responsible for improving profile data accuracy:

- Individual Updates: ACMs, SARs or their delegates with Student Support roles can make updates to their agency user profiles directly in FAI CSOD.
- Bulk Updates: For updates affecting 100 or more users, ACMs or SARs should define the scope of updates and submit a bulk update request via a New Agency Request (NAR) form. FAI recommends using an MS Excel spreadsheet format to document all user profile changes in the bulk update request. The spreadsheet can be attached to the NAR request form. FAI needs to identify each user included in the update request. For each user included in the update request, ACMs and SARs should add the following **mandatory** data fields:

- WarU ID
- First Name
- Last Name
- Email Address

In addition, ACMs and SARs must specify current and desired changes for each user profile data field that needs updates (e.g., old and new organization IDs). For a complete list of user profile data fields, please refer to the FAI Data Standards document.

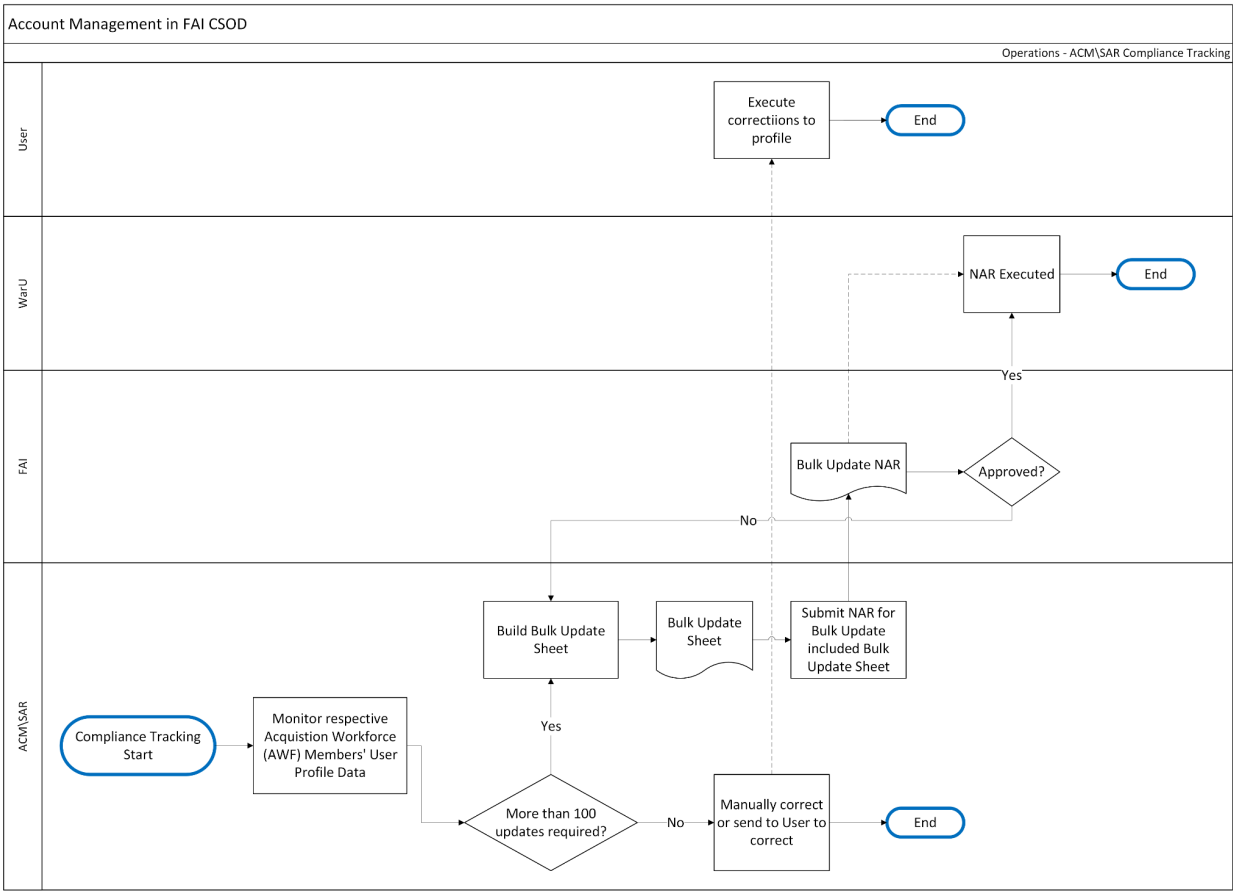


Figure 3. ACM\SAR Compliance Tracking Process

4.3 User Offboarding

The following tasks apply to users who retire, transfer, separate from their organization, or no longer meet FAI CSOD eligibility criteria:

Account Deactivation

Users and/or the Agencies should request FAI CSOD account deactivation when a user is no longer an active member of their AWF. Please see Appendix A for definitions of account deactivation and activation terms.

- Users, ACMs, or SARs can submit individual deactivation requests to the WarU Help Desk.
- If an individual needs an elevated role removed, due to deactivation, the user, ACM, or SAR should submit a NAR request.
- Employees retiring or no longer considered a part of the AWF per their agency's guidelines should:
    - Notify their ACM or SAR about the change and update their Organization field in the FAI CSOD user profile within 30 days **before** the last day of employment or affiliation with AWF.
    - The employee should update the organizational affiliation to the following User Profile Organization field options:
        - Not a Federal Employee - 100 (NotFedEmp)

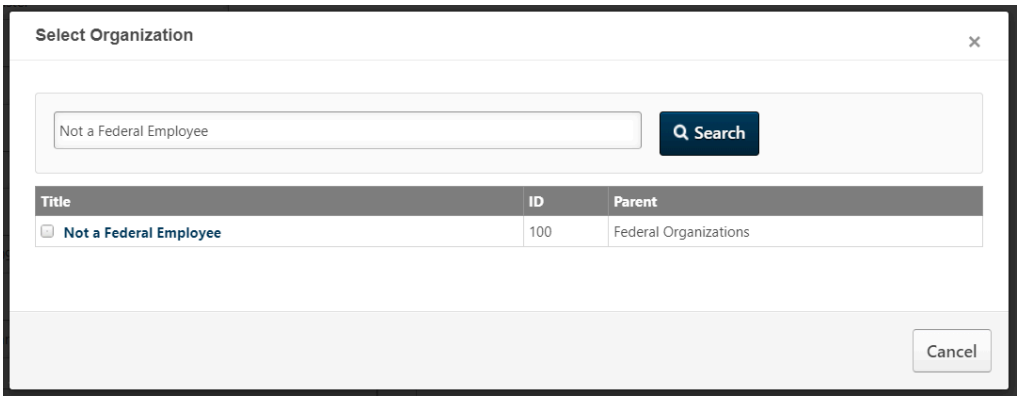


Figure 4. Not a Federal Employee Organization Selection Pop-up

- ACMs and SARs are responsible for tracking employee retirement and separation requests, ensuring all employees maintain accurate organizational FAI CSOD affiliation records through periodic review of agency HR data, FAI CSOD reports and D2D dashboards.
- Bulk deactivation requests (updates affecting 100 or more users) can be submitted by ACMs or SARs via a NAR form.

Account Reactivation

- Users can reactivate their FAI CSOD account by contacting the WarU Help Desk.
- Archived user data, including training records and certifications, is retained for reporting and records management purposes.

4.4 Employee Transfers

This section outlines the responsibilities and procedures for managing employee transfers within the FAI CSOD system. The goal is to ensure accuracy of organizational affiliation records for all employees.

1. An employee is transferring from one Federal Government agency to another.
    a. An employee should update the Organization affiliation user profile data field within 30 days of transfer to another federal agency.
    b. ACMs and SARs are responsible for tracking employee transfer requests to other federal government agencies and ensuring all employees maintain accurate FAI CSOD organizational affiliation records through periodic review of internal employee transfer requests and FAI CSOD reports and KPI dashboards.
    c. Employees should send a courtesy notice within ten business days before the transfer informing their current and future ACM or SAR about the change and updating their Organizational Affiliation in the FAI CSOD user profile.
2. A Federal Government employee is transferring to or from a DoW-affiliated agency.
    a. An employee is responsible for notifying their ACM or SAR about the change and updating their Organizational Affiliation in the FAI CSOD user profile within 30 days **before** the transfer to a DoW-affiliated agency.
    b. An employee transferring from a DoW affiliated organization to a Federal Organization or from a Federal Organization to a DoW affiliated organization must contact the WarU Help Desk to complete this FAI CSOD account update.
    c. ACMs and SARs are responsible for tracking employee transfer requests to and from DoW-affiliated agencies and ensuring all employees maintain accurate FAI CSOD organizational affiliation records through periodic review of internal employee transfer requests and FAI CSOD reports and KPI dashboards.

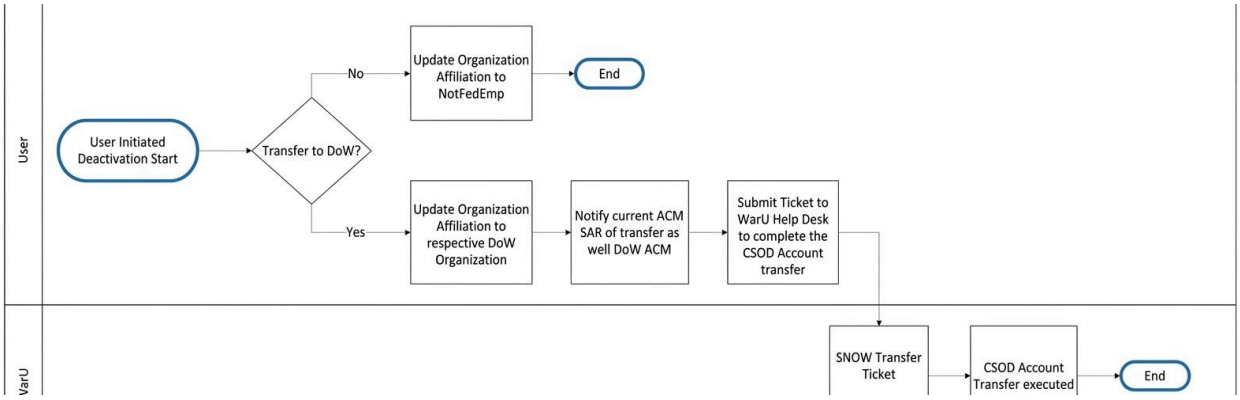


Figure 5. User Initiated Offboarding (Separation or Transfer to DoW)

4.5 Returning Employees to the Federal Government

This section outlines the responsibilities of a user who returns to an agency as a Federal Employee after previously leaving the Federal government. When a user returns to federal service, they should not create a new FAI CSOD account. Instead, they must update and reactivate their existing profile.

1. Log into FAI CSOD Using Existing Credentials
    a. If credentials are expired or forgotten, request assistance from the WarU Help Desk.
2. Update User Profile Information
    a. Update employment status, new agency affiliation, organization, and any other profile data to reflect an accurate employee record.
3. ACM/SAR Review and Validation
    a. ACMs/SARs will verify the user profile is accurate and complete
    b. They will reassign any needed roles and ensure data quality as part of onboarding (this will include reactivation of elevated roles)

4.6 FAI CSOD Account Management for Users Without Certification or CLP Requirements

Some users may access FAI CSOD to enroll in learning activities but do not intend to pursue FAC certifications or meet CLP (Continuous Learning Point) compliance requirements. These users may include managers, temporary learners, or those participating in elective courses without formal certification goals.

To manage accounts for this user category, FAI will implement the following procedure:

- **Activity Monitoring**: FAI will collect CLP activity data at regular intervals. As a general rule, FAI defines an inactivity threshold for FAI CSOD users with no

completed CLP courses on their transcripts within the last completed Continuous Learning period.
    - NOTE: Users that exist only to populate a user's Manager field in the User's record will not be deemed inactive for the purposes of Account Deactivation.

- **Account Deactivation**: FAI will deactivate user accounts meeting the inactivity threshold by moving them to the **NotFedEmp** organization at the end of a Continuous Learning period or at ACMs or SARs discretion. This reassignment ensures accurate system usage reporting, proper license management, and alignment with FAI data governance practices. For additional details, check the Account Deactivation section in Appendix A.

- **Individual and Bulk Account Deactivation options**:

    - Individual Updates: ACMs, SARs or their delegates with Student Support roles, can make updates to their agency user profiles directly in FAI CSOD.
    - Bulk Updates: For updates affecting 100 or more users, ACMs or SARs should define the scope of updates and submit a bulk update request via a NAR form. FAI recommends using an MS Excel spreadsheet format to document all user profile changes in the bulk update request. The spreadsheet can be attached to the NAR request form. FAI needs to identify each user included in the update request. For each user included in the update request, ACMs and SARs should add the following **mandatory** data fields:
        - WarU ID
        - First Name
        - Last Name
        - Email Address

- **Account Reactivation**: Users can regain access by contacting the WarU Help Desk, which will verify eligibility and restore their organizational affiliation as appropriate.

5.0 Data Quality Monitoring and Updates

1. ACMs and SARs are responsible for tracking all employee affiliation changes and ensuring the accuracy of organizational affiliation records in employee FAI CSOD user profiles.

2. In cases where employees separated or retired but failed to update the FAI CSOD organizational affiliation record, ACMs and SARs can use the following option in the User Profile Organization field to reflect employee's organizational affiliation changes:
    a. Not a Federal Employee - 100 (NotFedEmp)
3. The NotFedEmp organizational record serves as a temporary placeholder for identifying employees who are separating or retiring from a federal government agency. Annually, on August 1st, FAI will run batch jobs to remove employee records from NotFedEmp and place them into the INDUSTRY - OTHER organization.
    a. **NOTE:** As part of the user's move to INDUSTRY - OTHER, FAI will remove any elevated FAI CSOD roles from the account, place any Active FAC certifications to "On Hold", and clear the user's Manager field. If the user returns to a federal organization, and has an "On Hold" FAC certification, the WarU Help Desk will advise them to contact their ACM or SAR to discuss the requirements to reactivate the certification. The ACM or SAR can also request reactivation of elevated FAI CSOD roles as well if applicable. If a student in INDUSTRY needs a copy of their certification certificate for the On Hold FAC Certification, they can contact FAI who will print it for them.

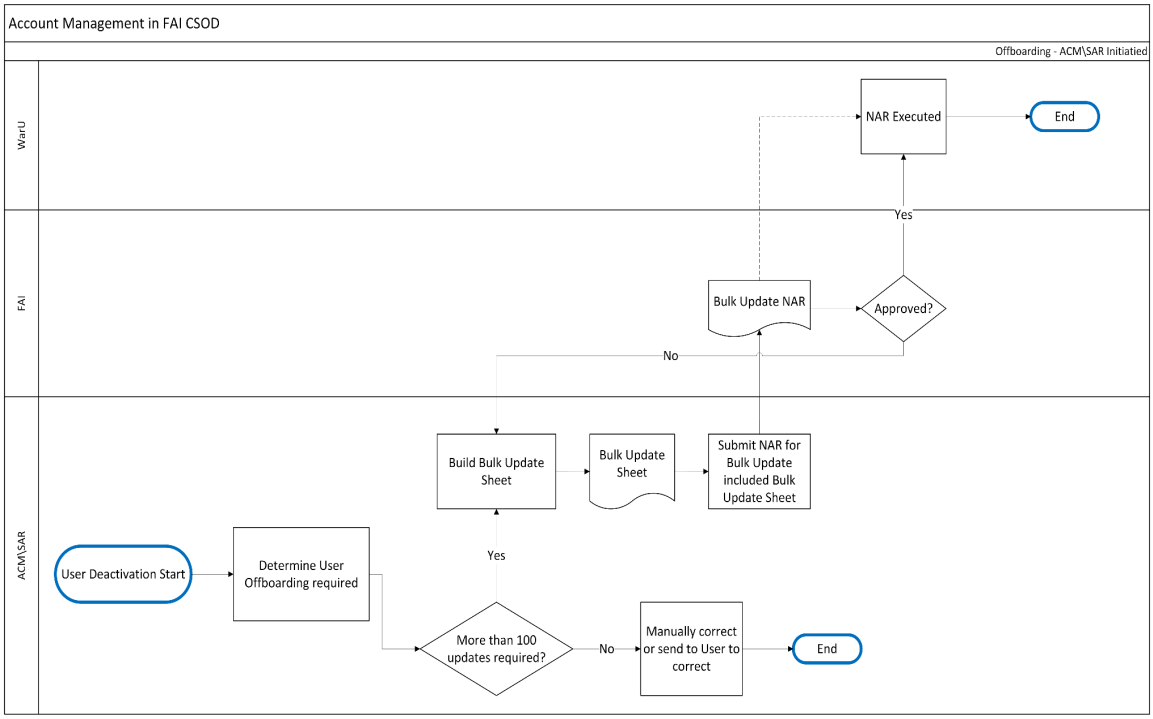


Figure 6. ACM\SAR initiated offboarding

6.0 Appendix

6.1 Appendix A: Rule-based User Status

A FAI CSOD User is considered active if they have any learning completion activity - with CLPs - on their transcript within the two year common period and are not in the NotFedEmp organization within FAI CSOD. The one exception being if the FAI CSOD User is designated as a Manager on a User Record.

User Status Definitions:

Active User Status:

- A user is active if they meet both of the following requirements:
    - Maintain an **organizational affiliation** with any federal organization except **NotFedEmp** in the FAI CSOD system
    - Comply with the **Continuous Learning Points (CLP)** requirements by participating in at least one learning activity, with CLPs, recorded in their transcript during a two-year common learning period.

Inactive User Status:

- A user is **inactive** if they meet either of the following criteria:
    - Assigned the **NotFedEmp** organization to the FAI CSOD system.
    - As reflected in their transcript, they have not participated in any learning activities within the past two years that have CLPs.

NOTE: HR-related changes (e.g., role transition, agency transfer, retirement, or separation from government service) are not automatically transferred to or recorded in FAI CSOD. Users might no longer be AWF members but still have an active FAI CSOD user account because they neglected to update the FAI CSOD User Record in time. ACMs or SARs are responsible for monitoring agency-level HR changes and updating the user's FAI CSOD profile as needed to maintain the accuracy of the AWF affiliation data.

At the end of the common period, FAI will run a query to identify any user that does not have completion activity - with CLPs - on their transcript and move them to the NotFedEmp organization, triggering the user’s account deactivation process. However, before the move, users that are designated in the Manager field of active FAI CSOD users will be removed from the inactivity list.

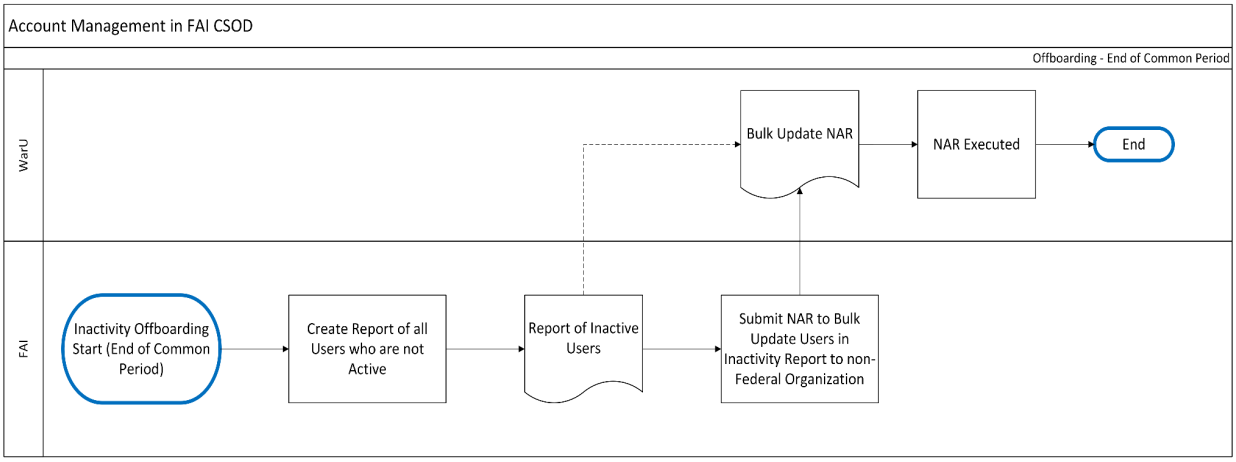


Figure 7. End of Common Period Deactivation

FAI will preserve all user training records for all inactive users. Inactive users can reactivate their FAI CSOD accounts by contacting the WarU Help Desk.

FAI CSOD User Account Deactivation and Activation

Account Deactivation

Account deactivation is the process of changing a user's organizational affiliation from a federal organization to a designated placeholder organization called NotFedEmp (Not a Federal Employee). This deactivation process ensures that:

- The user's training transcript and historical records are preserved.
- The user will not appear in any FAI CSOD reports.
- The user will not consume FAI CSOD licenses (assuming they have not logged in during the current Period of Performance (PoP)).
- The user will not be able to process equivalency requests for external training.
- The user's profile is later moved to a broader category in the FAI CSOD system hierarchy, labeled INDUSTRY - OTHER to maintain organizational data integrity.
- The user will only be able to access and enroll into online training on the WarU Virtual Campus; they will not be able to access the FAI CSOD portal. CLPs associated with completing online training on the WarU Virtual Campus will be recorded in the user's transcript and counted towards meeting the common period CLP requirements.

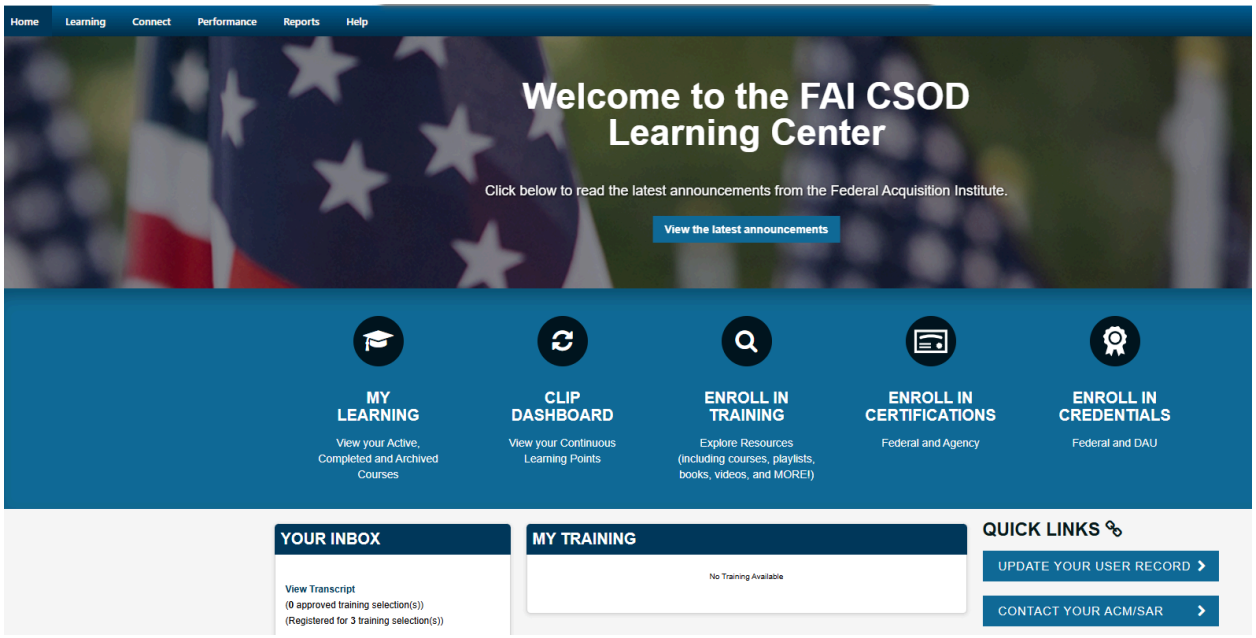


Figure 7. FAI CSOD Virtual Campus.

Account Activation

Account activation is the process of restoring user's access to the FAI CSOD when they regain eligibility, typically by rejoining the federal acquisition workforce. This process involves:

- Updating the user's organizational affiliation from INDUSTRY - OTHER back to a federal agency.
- Restoring system privileges that allow the user to enroll in FAI courses and process training equivalency requests.
- Making the user's records available in FAI CSOD reports.
- Ensuring the user is included in workforce compliance tracking and training requirement evaluations and reviewing any "On Hold" FAC certifications.
- Ensuring the user's Manager field is properly filled in.

6.2 Appendix B: FAI CSOD User Status Maintenance

Conditions for Maintaining Active Status:

- **Accurate Profile Maintenance:** Users must ensure their FAI CSOD user profile contains up-to-date and accurate information (e.g., organizational affiliation, job series).

- **CLP Compliance:** Users must complete learning activities that fulfill biannual CLP requirements.

Process for Changing User Status:

- **From Active to Inactive:**
  - Users aware of upcoming changes in employment status can trigger user profile updates by changing Organization affiliation user profile field to NotFedEmp organization or by requesting ACM/SAR to complete the change.
  - ACMs, SARs, or the WarU Help Desk run periodic reviews and update the user's organizational affiliation to **NotFedEmp,** moving them to inactive status.
- **From Inactive to Active:**
  - Users must contact the WarU Help Desk, which will verify eligibility and update their organizational affiliation and status.

Consequences of Implementing the New User Status Definition:

- **Operational Adjustments:**
  - Due to its limitations, the **User Status** data field in FAI CSOD no longer enforces compliance. Instead, FAI will apply business rules defined in this process document and periodic data updates to manage user status changes.
- **Reporting Impacts:**
  - FAI recommends excluding filters based on the **User Status** field from all custom FAI CSOD reports.
- **User Visibility and Licenses:**
  - Users with inactive status will:
    - No longer appear in reports.
    - Do not consume FAI CSOD licenses.
    - Unable to process equivalency requests for external training.

FAI will preserve all user training records for all inactive users. Inactive users can reactivate their FAI CSOD accounts by contacting the WarU Help Desk.

6.3 Appendix C: SAAR data fields transferred to the FAI CSOD User Profile

Six data fields are transferred from the WarU SAAR form to the FAI CSOD User Profile when creating a new user account.

SAAR Form Field	FAI CSOD Profile Field
First Name	First Name
MI (Middle Initial)	Middle Name
Last Name	Last Name
Telephone	Phone
Email	Email
Sub Org	Organization

6.4 Appendix D: Student Support Role

Only ACMs, SARs, and individuals with ACM-delegated authority are authorized to submit Student Support Role requests on behalf of their agency. Additionally, they can only manage users within their same organization. An individual responsible for updating the FAI CSOD user profiles for employees must coordinate with their ACM or SAR to obtain the FAI FAI CSOD Student Support role. This role is necessary to change the organizational affiliation in the FAI CSOD user profiles for agency employees.

6.5 Appendix E: Inactive User Certification Status

Federal AWF members can leave the workforce for various reasons (e.g., retiring, separation of service, transferring to DoD, Reduction in Force (RIF) or any other reason). In case of a user's separation, the system does not automatically change the user's certification status from 'active' to 'revoked' or 'on hold.'

Process

1. After a user separates from the AWF, FAI will reassign their FAI CSOD account from NotFedEmp to the INDUSTRY - OTHER Organization (annually) so this separation is recorded correctly.
2. FAI manages all users' certifications by CLP requirements. As such, if the individual has not obtained the necessary CLPs at the end of the common

period, FAI will revoke their certification(s), leveraging the current revocation process for AWF members in Federal Organizations and enforcing the two-year CLP compliance rule.

3. Suppose a user returns to the Federal AWF within the standard period they left. In that case, their CLPs will be the same as when they left. They can continue to achieve the requirements for their certification(s). However if their FAC Certification was set to “On Hold” (as described in Section 5.0) they will need to reach out to their ACM\SAR to discuss the requirements to get the certification reactivated.