DCMA Manual 4301-05, Volume 9

Financial Systems and Interfaces: Defense Agencies Initiative User Management

Office of Primary Responsibility	**Stewardship Capability**
Effective:	April 1, 2019
Releasability:	Cleared for public release
New Issuance	
Implements:	DCMA-MAN 4301, "Stewardship," July 18, 2018
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://360.dcma.mil/sites/policy/ST/SitePages/4301-05v9r.aspx
Approved by:	David H. Lewis, VADM, USN, Director

Purpose: This issuance, in accordance with the authority in DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," implements policy and:

- Assigns responsibility for practices established by DCMA Defense Agencies Initiative User Management
- Defines the expected user management processes required for access to the Defense Agencies Initiative financial management system

TABLE OF CONTENTS

TABLES

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to all DCMA users of DCMA's financial management system, Defense Agencies Initiative (DAI) activities unless higher-level regulations, policy, guidance, or agreements take precedence. DAI is the official data entry and repository system for DCMA's financial management.

1.2. POLICY. Accurate DAI User Management (UMX) procedures are a fundamental responsibility of all DCMA employees. All DCMA employees have a fiduciary responsibility inherent in their roles as stewards of government resources and must comply with the guidance set forth in this Manual. It is DCMA policy to execute this manual in a safe, efficient, effective, and ethical manner.

a. Scope. DAI is the approved financial management system for DCMA operations used to oversee all aspects of the Agency's financial processes. The purpose of this Financial Systems and Intefaces: DAI User Management Manual is to outline the DCMA business processes pertaining to the DAI UMX module and related User Management processes.

b. Usage. DAI leverages financial management integration and improvement processes by streamlining financial management capabilities, eliminating material weaknesses, and achieving financial statement auditability for the Agencies across the DoD.

1.3. OVERVIEW.

a. Background. Defense Logistics Agency (DLA) manages DAI, complying with the DoD's transformation goals to modernize the Defense Agencies' financial management systems. DAI is an Enterprise Resource Planning (ERP) tool which delivers the basis for an integrated enterprise level solution to manage the business processes of the Agency. The goal of the DAI Architecture is to allow agencies to manage internal and external resources including tangible assets, financial resources, materials, and Human Resources (HR). The design also facilitates the flow of information between all business functions inside the boundaries of the organization, and manages connections to outside stakeholders. This Manual defines the processes for managing users and implementing user access controls as it relates to the usage of the DAI system and DCMA processes.

b. DAI Effort. DAI is a critical DoD effort to modernize financial management capabilities that compile the budget, finance, and accounting operations of the DoD Defense Agencies to:

(1) Achieve accurate and reliable financial information.

(2) Deploy a standardized system solution to improve overall financial management and comply with the Department's Business Enterprise Architecture (BEA) including Standard Financial Information Structure (SFIS) and Office of Federal Financial Management (OFFM) requirements.

(3) Attain Chief Financial Officer (CFO) compliant business environments with accurate, timely and authoritative financial data.

c. Managing Users.

(1) UMX is the process of establishing user access controls, providing the ability to configure users with the appropriate level of access to networks or systems. Processes described in this document will assist DCMA in validating the steps necessary to clarify and confirm User Management and the use of the UMX module. UMX provides system administrators control over user provisioning and allows the flexibility to implement enhanced authentication-based policies while integrating industry authentication methods and procedures.

(2) Objectives. The major objectives of UMX include:

(a) Identify DCMA UMX Points of Contact (POC) and Stakeholders.

(b) Identify UMX Tools and Templates.

(c) Define DCMA UMX Processes and Procedures.

d. Solution Assumptions/Constraints. The DCMA DAI UMX solution is based on the following assumptions and constraints:

(1) DCMA utilizes UMX – User Access Control Standards and provisioning processes that are set-forth and defined in the DAI system.

(2) DCMA business processes will be modeled to include the UMX solutions and provide training to all DCMA DAI users.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, DCMA. The Director, DCMA, retains the final authority over the Financial Systems and Interfaces: DAI User Management Manual by representing DCMA with leadership and providing decisions as required.

2.2. EXECUTIVE DIRECTOR, FINANCIAL AND BUSINESS OPERATIONS DIRECTORATE (FB)/COMPTROLLER. The FB Executive Director must oversee, administer, and verify the documented procedures in this Manual for completion and processing of DD Form 2875, "System Authorization Access Request (SAAR)," for DAI and DAI User Account approval.

2.3. EXECUTIVE DIRECTOR, INFORMATION TECHNOLOGY DIRECTORATE (DCMA-IT)/ CHIEF INFORMATION OFFICER (CIO). CIO must submit a memorandum to the DLA Program Management Office (PMO) annually, confirming DCMA has a process to collect and maintain all DD Form 2875's for user access to the DAI system and ensure Information Assurance (IA) training is renewed according to DCMA-IT policy.

2.4 DCMA SECURITY MANAGER, DIRECTORATE OF CORPORATE OPERATIONS. The Security Manager must process system access requests and:

a. Validate user trustworthiness by confirming appropriate clearance level.

b. Digitally sign the DD Form 2875 for system access requests.

2.5 INFORMATION ASSURANCE OFFICER (IAO), DIRECTORATE OF INFORMATION TECHNOLOGY. The IAO must process system access requests and:

a. Verify the completion of appropriate IA training.

b. Digitally sign the DD Form 2875 for system access requests.

2.6. INFORMATION OWNER (IO). The IO must process system access requests and:

a. Verify completion of the DD Form 2875 and ensure all required signatures are present.

b. Verify that the roles requested on the DD Form 2875 are applicable for the user's duties/responsibilities and approve or reject the DD Form 2875 as applicable.

2.7. DAI PMO HELP DESK. The DAI PMO Help Desk is the backup to manage the provisioning of user roles in the DAI automated processes. When requested, the DAI PMO Help Desk will:

a. Register User accounts.

b. Assign user roles in DAI.

c. Deactivate user roles in DAI.

d. Deactivate user accounts.

e. If processes are managed manually, the PMO will notify the users via standard email.

2.8. FINANCIAL ACCOUNTING SUPPORT TEAM (FAST) ACCOUNT MANAGER. The FAST Account Manager is the DCMA DAI Team member responsible for the final approval step of the DD Form 2875. The FAST must:

a. Approve and validate user accounts in accordance with the approved DD Form 2875 and applicable supporting documents.

b. Digitally sign the DD Form 2875 as the final reviewer/validation.

2.9. FINANCIAL MANAGEMENT ANALYST, FINANCIAL SYSTEMS OPERATIONS BRANCH (FBSO). FBSO must:

a. Process DAI account and role approval requests within DAI.

b. Submit the Manual Responsibility Request Form (MRF) to DAI PMO when required.

c. End date user roles upon receipt of modification or deactivation DD Form 2875 or Help Desk ticket requests.

d. Deactivate user account upon receipt of DAI support requests submitted via Help Desk tickets, deactivation DD Form 2875, Human Capital (HC) Separation Report, DAI HR Customer Service Representative (CSR) employee status, Military Departure Report, or Defense Civilian Personnel Database System (DCPDS) identification of ex-employees.

e. Initiate and approve deactivation requests in the UMX system of both User roles and User accounts.

f. Perform quality assurance reviews on user requests prior to submitting to the DAI PMO Help Desk for role provisioning and manual setup of users for all process areas, when applicable.

g. Perform periodic reviews of DAI access and maintain documentation and results based on Financial Improvement and Audit Readiness (FIAR) requirements.

2.10. HR SPECIALIST (INFORMATION SYSTEMS), HUMAN CAPITAL DIRECTORATE (HC). The reports manager for HC must provide employee rosters and separation reports from DCPDS to the FBSO. Historical reports used for DAI UMX approvals can be requested from HC.

2.11. APPOINTMENT/TERMINATION RECORD - AUTHORIZED SIGNATURE (DD FORM 577) POC. DD Form 577 POC from the Planning and Budgeting Center (FBA) must provide FBSO personnel access to listings of DCMA employees who have a signed DD Form 577 for DAI role approvals and complete DD Form 577 reviews as requested.

2.12. DCMA MILITARY PERSONNEL OFFICE, DIRECTORATE OF CORPORATE OPERATIONS. The Military Personnel Office (DCM) must provide an up-to-date listing of both active and departed military personnel assigned to DCMA.

2.13. AGENCY MANAGERS/SUPERVISORS. Managers/Supervisors must:

a. Approve and sign DD Form 2875 requests for DAI account access.

b. Ensure roles listed on the DD Form 2875 are required for completion of the employee’s job duties.

c. Ensure employee’s Internal Web Access Management (IWAM) accounts are deactivated upon departure from the Agency to initiate the DAI account deactivation process.

d. Ensure all transferred employees only have access to DAI roles required for their current position.

2.14. AGENCY USER/DAI USER. The Agency User/DAI User must:

a. Initiate requests to gain access to DAI and digitally sign the DD Form 2875.

b. Initiate self-registration process in DAI for initial account activation.

c. Initiate request for approved roles in the DAI Application.

d. Update the DD Form 2875 as required when duties/responsibilities change.

e. Ensure roles on the DD Form 2875 align with assigned roles in DAI.

SECTION 3: USER MANAGEMENT OVERVIEW

3.1. INTRODUCTION.

a. Overview. DCMA utilizes the DAI Financial System to process financial transactions and human resources activities. User account provisioning is also managed within the DAI framework. This section will provide a global review of the different processes that are included in the management of users as it relates to DAI.

b. Mandatory Training. DCMA requires all DAI users to complete the Annual IA and Personally Identifiable Information (PII) Training. This training must be renewed annually.

(1) Annual IA Training. Also called Cyber Awareness Training is monitored by DCMA IT Cybersecurity. Completion is required to gain access to the DCMA network and computer systems and required to be renewed annually to maintain DAI access. Users are automatically sent notifications from the Agency's system of record to complete IA Training. DCMA IA Policy and processes are governed by DCMA Manual (DCMA-MAN) 4401-05, "Cyber Workforce Improvement Management."

(2) Privacy Act and PII Training. Reference DCMA-MAN 4502-13, "Privacy and Civil Liberties," for guidance on Privacy Act and PII Training.

3.2 SYSTEM ACCESS AUTHORIZATION REQUEST (SAAR) REQUIREMENTS.

a. Overview. DCMA utilizes the current Agency system of record for the electronic System Authorization Access Request (eSAAR) that allows users to initiate a DD Form 2875 to request system access. The DD Form 2875 contains the following records:

(1) Individual user identification and digital signature.

(2) Verification of current IA Annual Awareness Training completed.

(3) Supervisor endorsement.

(4) Appropriate active background investigation or security clearance.

(5) Appropriate supporting documentation, if required.

b. DCMA Use of the DD Form 2875. The DD Form 2875 will be used to authorize access to the DAI system and grant approval of specific DCMA Roles and Responsibilities.

(1) DCMA Notifications. This DAI Responsibility is automatically granted with DAI account creation and therefore not required on the DD Form 2875. UMX is configured to use the Notification module as the collaboration tool that manages the creation and delivery of notifications and emails to the designated approvers and users. These notifications contain action-based command buttons that allow for the approval or rejection of the request by clicking

the appropriate command button. In addition, any notification that does not require an action to be taken is configured as a For Your Information (FYI) notification.

(2) DAI Roles. The DD Form 2875 will contain all roles the user requires access to in order to perform assigned daily job functions. These roles will be reviewed and approved by the employee's supervisor and updated as the user's job functions or position changes. The DD Form 2875 will be periodically reviewed by the FBSO to ensure the approved DD Form 2875 matches the approved roles within the DAI system.

3.3. DD FORM 577 REQUIREMENTS.

a. Overview. DoD 7000.14-R, "Financial Management Regulation (FMR)," Volume 5, Chapter 5 and Volume 14, Chapter 2 establishes guidance for use of the DD Form 577. The FMR governs the appointment of Certifying Officers (CO) and Departmental Accountable Officials (DAO) via a DD Form 577. Users who require access to the listed roles in order to perform assigned job duties must have an approved DD Form 577. The DD Form 577 must be approved prior to the employee requesting the DAI role via the DD Form 2875 (SAAR for DAI) process. The DD Form 577 submissions are managed by FBA. The FBSO Team will ensure the DD Form 577 is approved and valid before approving the below roles on the DD Form 2875.

b. DD Form 577 Required Roles. The following Procure to Pay (P2P) and Order to Cash (O2C) DAI roles require a DD Form 577:

(1) O2C Cost Accounting (CA) Project Manager DCMA.

(2) P2P Procurement Officer DCMA.

(3) P2P Miscellaneous Pay DCMA.

(4) P2P Cost Distribution DCMA.

c. Eligibility. Those eligible to be appointed via a DD Form 577 include any DoD civilian employee or member of the U.S. Armed Forces.

3.4. DAI UMX System. UMX implements Access Control Procedures that contribute to DAI's compliance with the Federal Information System Controls Audit Manual (FISCAM) and Internal Controls – A-123 audits. UMX module inherent to DAI provides:

a. Access Request Management.

b. Segregation of Duties (SoD) Rules Engine.

c. Role Management Monitoring/Reporting.

d. Single Sign-On (SSO) via integration with Oracle Identity Management (OIM).

e. User Access Verification.

(1) All UMX Access Control processes and procedures are centered on the goal of preventing SoD violations that expose the system and DCMA to risk of fraud and mistakes.

(2) Procedures will address the following current and future end-to-end processes:

(a) How a user will gain access to DAI.

(b) How a user will request a system role(s).

(c) How the system will manage out-processing tasks related to deactivation of the account and assigned roles.

(d) How SoD violations will be prevented and/or mitigated for requests to create a new role or update an existing role.

(e) How high risk roles and issue resolution will be managed.

3.5. END OF MONTH PROCESSING. End of Month Processing occurs on the first few days of every month as communicated by the DAI PMO. Agency users will be unable to access responsibilities that can create or approve financial transactions during the period of restricted access in order for DCMA and Defense Financial and Accounting Services (DFAS) to perform month-end closeout transactions. During this process, the following collaboration and rules will be enforced:

a. No financial transactions can be entered or approved.

b. DCMA Notifications will not be available except for Oracle Time and Labor (OTL) processes.

(1) Employees/Supervisors/Timekeepers may enter time cards and leave/premium requests.

(2) Supervisors with the OTL Supervisor Approver DCMA role will retain the ability to approve time cards and leave/premium requests.

(3) All time and labor reports are available.

c. All inquiry and reporting responsibilities remain available (including P2P Inquiry and Oracle Business Intelligence Enterprise Edition (OBIEE) Reports).

SECTION 4: DCMA DAI UMX Process

4.1. OVERVIEW. Requests for User Access to DAI are managed via the UMX self-registration and responsibility request processes. These processes are designed to create user accounts and assign responsibilities. Designated Agency users and Help Desk personnel will maintain user account and responsibility approvers in accordance with specific internal business processes. On an exception basis, User Access requests may also be processed by the DAI PMO Help Desk by following the DAI MRF process. See paragraph 4.4.c. for more information on the MRF process.

4.2. NEW EMPLOYEES. All DCMA users who require access to DAI must complete the 3-Steps for DAI Account approval. See Figure 1, DAI 3-Steps to Account Creation.

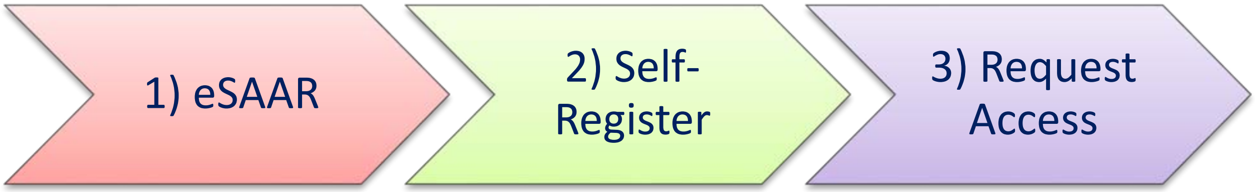
a. DD Form 2875. Submit a DD Form 2875 to access the DCMA computing arena along with the specific roles required for the employee's position.

b. Self-Register in DAI. After the DD Form 2875 has been approved, follow the Account Request process to submit a request for access to the DAI System. Upon completion of self-registration, the DAI Account has been created and approved.

c. Role Request in DAI. The Role Request process allows for additional access to specific capabilities of the DAI system that enable users to complete assigned task(s).

(1) The initial request should only include time entry roles as this will ensure that the individual would not have a delay in obtaining an account for time entry.

Figure 1. DAI 3-Steps to Account Creation



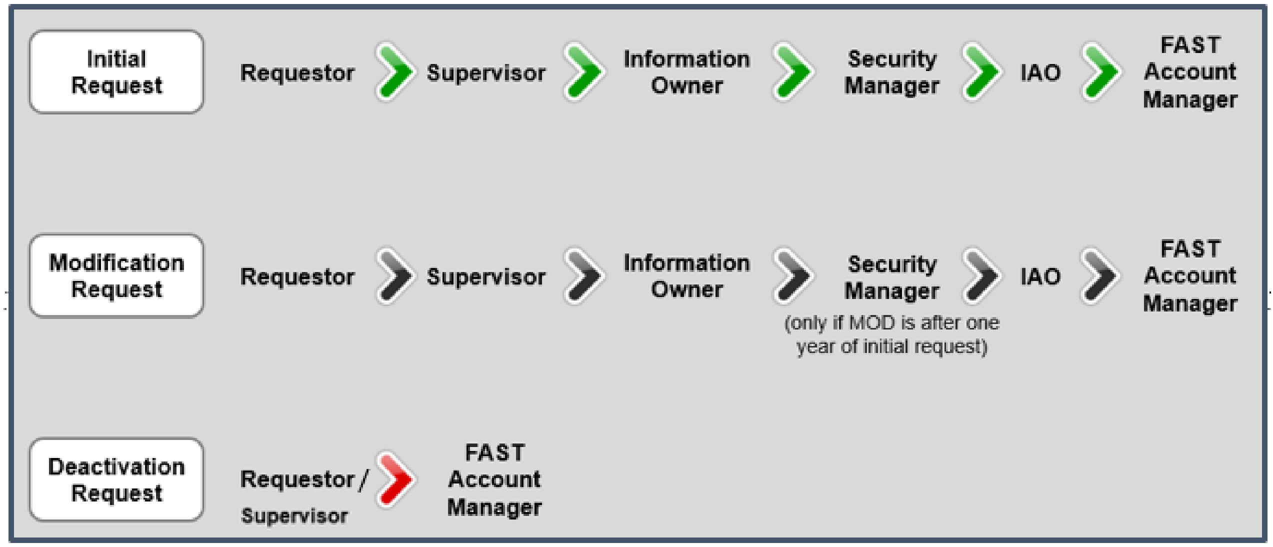
4.3. DCMA DD FORM 2875.

a. DD Form 2875 User Process. All DCMA users who require access to DAI will submit a DD Form 2875 via the DCMA eCapability, eSAAR. The user must only select roles required for their position. Questions on which roles are required for the user's position should be addressed with the employee's supervisor. Refer to the SoD Matrix, Figure 5, for details on restricted roles. Only roles approved on the DD Form 2875 will be granted to the user in DAI. The DD Form 2875 Initial/Modification User Process can be found on the Resource Page.

b. DD Form 2875 Supervisor Process. Supervisors will verify that all requested roles are required for the named employee's job duties. Upon concurrence, the supervisor approves and digitally signs the DD Form 2875. If corrections are required, the supervisor will reject the DD Form 2875 and notify the employee to resubmit with any needed corrections.

c. DD Form 2875 Approval POCs Process. The IO must review the DD Form 2875 for completeness, ensuring both employee and supervisor digital signatures are present and will approve or reject the request accordingly. The Security Manager must review the DD Form 2875 and validate the user's access in accordance with their security clearance by utilizing the appropriate background investigation or security clearance. The IAO must verify Annual IA Training has been completed within the past year. The FAST will perform a Quality Assurance review of the request prior to approving the DD Form 2875. The FAST will also ensure the user has any additional required documentation to support the roles requested, as needed. All DD Form 2875 Approval POCs will approve or reject the completed Form and sign with a digital signature. If a DD Form 2875 is rejected at any point throughout the approval process the user will need to resubmit a new DD Form 2875 as the old request will no longer be valid.

Figure 2. DD Form 2875 Approval Steps



4.4. DAI SELF-REGISTRATION.

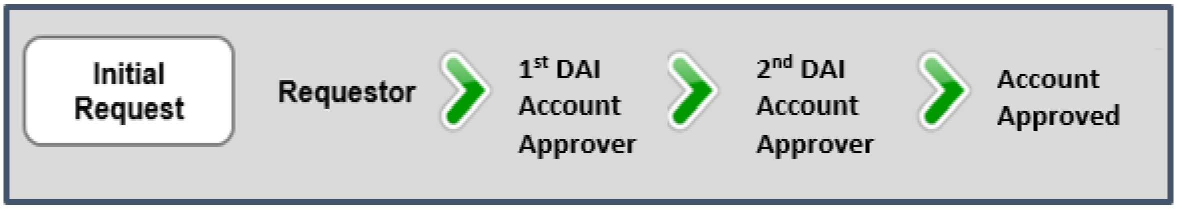
a. DAI Self-Registration User Process Overview. DAI Self-registration is completed after approval of the DD Form 2875. This step is only required for DCMA employees who need initial access to DAI. DAI Self-Registration link will be provided within the DD Form 2875 approval notification email. The DAI Self-Registration User Process can be found on the Resource Page.

(1) Self-Registration Errors. If a user receives an error during the self-registration process, the user will submit a Help Desk ticket to the FBSO to troubleshoot the account creation error. The FBSO will determine if the MRF process for account creation is required and escalate accordingly. When the issue has been resolved, the FBSO will contact the user, inform the user of the resolution, and provide guidance on how to proceed.

(2) Approval Notification. Self-Registration requests will be processed within 1 to 2 business days of submission. Employees will be notified via an email that states, "Your account request has been approved. Use the following link to access the system." The user can click the link that is included in the notification or navigate via the DCMA portal.

b. DAI Self-Registration FBSO Personnel Overview. User account requests submitted through the UMX Self-Registration process are routed to designated approvers. FBSO personnel will ensure that all DAI Account Requestors have an approved DD Form 2875. DCMA will have the option to modify UMX account approvers in the Production environment and delegate approval as required.

Figure 3. DAI Self-Registration Approval Steps



c. MRF Process. This process consists of completing and submitting the MRF. If the UMX self-registration procedure cannot process the user's Common Access Card (CAC) or if the user is unable to access the Access Request page in DAI, an MRF must be completed and submitted to the FBSO.

(1) The FBSO Tier 1 Help Desk will obtain a signed MRF.

(2) After required signatures have been captured, the user or FBSO personnel will create a DAI Help Desk ticket and attach the MRF.

(3) Prior to accepting the ticket for processing, the FBSO Tier 1 Help Desk should ensure that the DD Form 2875 for the user is completed and approved and the action and other details on the MRF are on the approved DD Form 2875.

(4) FBSO Tier 1 Help Desk will work directly with DAI Unit Identification Code (UIC) Team Leads and FBSO Tier 2 to submit the form to the DAI PMO Help Desk Team for processing.

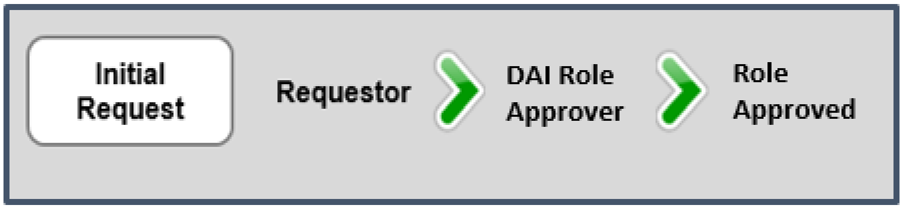
4.5. DAI ROLE REQUEST.

a. DAI Role Request User Process Overview. Personnel must request access to roles in order to perform activities in DAI. Roles granted in DAI will determine the Homepage layout and menu paths for navigation. DAI Role Request process is completed after the DD Form 2875 and DAI Self-Registration processes are complete. Roles requests will not be approved unless the requested role is listed on the user's approved DD Form 2875 and will be processed within 1-2 business days after submission. The DAI Role Request User Process can be found on the Resource Page.

b. Roles with Additional Steps. For Limited Timekeeper DCMA roles, users must submit a DAI Help Desk Ticket to request access to designated Timekeeper Group(s). Users must have the DD Form 2875 approved with the Limited Timekeeper roles approved as well as the role assigned to them in DAI before submitting the DAI Tier 1 Help Desk Ticket. The DAI Tier 2 Help Desk Team will confirm with the Financial Payroll Support Branch (FBSP) to validate that all required training has been completed.

c. DAI Role Request FBSO Personnel Overview. FBSO will ensure that all requested roles are on an approved DD Form 2875 prior to approving the user's request.

Figure 4. DAI Role Request Approval Steps



4.6. DAI ROLE MODIFICATIONS.

a. User Overview. DAI account roles need to be modified in accordance with modifications to an employee's duties. Users should only have roles within DAI that are actively needed to perform work for their mission. This process is coordinated with FBSO Personnel. To initiate the modification:

(1) Submit Modification DD Form 2875 via the Agency system of record.

(2) Submit Role Request in DAI. If a user is adding roles to the DD Form 2875, the user process for requesting modified roles in DAI mirrors the user process described in paragraph 4.4.a.

(3) Removing roles from the DD Form 2875. No action is required by the user in DAI. After all approvals are captured on the DD Form 2875, the FBSO will process the removal request by end dating the indicated DAI roles.

b. FBSO Personnel Responsibilities. Additional steps must be taken by the FAST for role modification requests. The FAST must review the previously approved DD Form 2875 to identify changes to the user's DAI roles. If the user is removing a DAI role from the DD Form 2875, the FAST will end date the role within DAI.

4.7. PROXY DELEGATES.

a. Overview. DAI allows alternate responders to approve notifications on another user's behalf. The original approver must set up these alternate responders in advance. DAI provides two different mechanisms to facilitate this process: Vacation Rule and Manage Proxies. Due to the importance of approving notifications on a timely basis, an Approver must maintain additional approvers who can access their Worklist to process notifications within DAI. These alternate approvers will be referred to within the documentation as "Proxy Delegates".

b. Vacation Rule. Created in advance of the Approver being off duty and will focus on temporary situations, such as when an Approver is on leave.

(1) All approval actions are delegated to another approver with appropriate access for a limited period.

(2) These notification actions will only appear in the Worklist of the Proxy Delegate approver established in the Vacation Rule and not in the original Approver's Worklist.

c. Manage Proxies. Allows the Approver to create a list of Proxy Delegates, who can process notifications on behalf of the Approver at any given time.

(1) Establishes a backup hierarchy. These individuals will have permanent access to the Approver's Worklist.

(2) These Proxy Delegates will login to DAI as themselves and then access the other Approver's Worklist to process any pending notifications.

(3) Prior to out-processing DCMA, DAI users must remove all Proxy Delegates from their accounts by end dating the established proxy rules. This action must be completed prior to DAI account deactivation.

(4) For historical reasons, Proxies can never be deleted. If the name is removed, it affects historical reporting and therefore cannot identify the proxy who may have approved a timecard(s).

4.8. OUT-PROCESSING DAI.

a. Overview. Requests for account deactivation will be coordinated with HC. The employee's supervisor initiates deactivation requests by the deactivation of the user's IWAM account. After the deactivation request is submitted and approved, the user's assigned roles will be end dated and the user Account will be terminated. Account deactivations will be completed within 5-10 business days of receipt. Exceptions to this process will be documented.

b. DAI Account Deactivation. DAI accounts and associated HR Records will be deactivated when employees depart the Agency. Deactivations require 2 points of verification to confirm employee departures. The following methods notify FBSO personnel, and can be used to verify employee departures:

(1) Deactivation DD Form 2875. Results from Supervisors deactivating employee's IWAM accounts.

(2) HC Separation Report. Report shows all employees who have departed the Agency.

(3) HC Personnel Action Report. Report shows all employees who have completed or have pending personnel actions in DCPDS for the current month.

(4) Monthly PMO DCPDS ex-Employee Notification Emails. PMO provided listing of DCMA employees with active DAI accounts whose DCPDS account status is ex-employee.

(5) Employee's HR CSR Profile updates to ex-Employee. Results from HC manually processing HR requests or DAI interfacing with DCPDS.

(6) Military Departure Report provided by DCM. Report shows all assigned and departed military members who are assigned to DCMA.

(7) Help Desk Tickets submitted to the FBSO. Supervisors can submit DAI Help Desk tickets requesting employee's DAI accounts be deactivated.

c. DAI Account Deactivation FBSO Personnel Process Overview. Account deactivations are initiated when one of the above methods are executed. FBSO personnel will acknowledge receipt of the request and employ a second method to confirm the employee's departure. Upon verification, FBSO personnel will execute the processes related to Role End Date and Account Deactivation while applying the rules defined under HR Record.

(1) Role End Date. End date all active DAI roles in the departed employee's user profile. The DAI Role End Date Process can be found on the Resource Page.

(2) Account Deactivation. Deactivate the DAI account and digitally sign the Deactivation DD Form 2875. The DAI Account Deactivation Process can be found on the Resource Page.

(3) HR CSR employee status updates automatically.

(a) Civilian Users. The process to terminate HR records will be updated automatically when DCPDS interfaces with DAI.

(b) Contingent Worker Users. No DCPDS process is required. The UMX Account deactivation process will disable the User account and terminate the HR record as part of the Change request.

SECTION 5: DCMA UMX APPROVALS AND WORKFLOWS

5.1. OVERVIEW. UMX is configured with account approvals and workflows to manage UMX requests.

5.2. AUTHORIZED APPROVERS. FBSO is responsible for designating Agency Approvers. A list of Agency Approvers is maintained in the DAI System and DCMA has the ability to update this list as required. The Approvers are required for the UMX approval processes and are used as part of the UMX key process flows.

a. Agency Account Approvers. Account Approvers process self-registration requests for initial DAI access. DAI requires two levels of approval for account creation. FBSO personnel serve as both the first level and second level Account Approvers for all DCMA DAI accounts, for both civilian and contingent worker users. First Level Approver and Second Level Approver cannot be the same person.

b. Agency Responsibility Approvers. FBSO will provide Responsibility Approvers for all process areas. Responsibility Approvers process DAI role access requests. After the user accounts are approved by the Agency Account Approvers, users can log in to the DAI application and request access to responsibilities (roles) through UMX. Every responsibility is aligned to a process area, and each process has a designated Agency Responsibilities Approver(s).

(1) After Agency approval is granted, responsibility requests will be routed to a final PMO license approver, if applicable.

(2) DCMA has the option to modify UMX Responsibility Approvers, as required.

c. Termination Approvers. DAI utilizes the same Approvers that have been designated as part of the UMX Approvers. If a user has been designated as an Approver for Initial Account Requests, then the same Approver will be selected as a Termination Approver.

5.3. WORKFLOW PROCESSES.

a. Account Request Approval. This workflow is triggered when a user requests a DAI Account and implements the configurations related to Agency Account Approvers to select the approvers and send out multiple action-based notifications. Once all approvals have been completed, DAI will automatically create and activate the DAI account and then send out an FYI notification to the end-user.

b. Role Request Approval. This workflow is initiated when a user requests a role assignment and implements the configurations related to Agency Responsibility Approvers to select the approvers and send out multiple action-based notifications. After all approvals have been satisfied, DAI will automatically assign the requested roles and then send out FYI notifications to the Manual Setup Approver (if required) and the end-user.

c. Change Request Approval. This workflow is triggered when a UMX Proxy User submits a request to deactivate the account and role assignments for a selected user.

(1) UMX Proxy Super User**.** Agencies that utilize the capabilities related to User Maintenance are required to add designation users to the Proxy Manage Group. In addition, the UMX Proxy roles should be assigned based on the functionality that will be performed by these users. The assignment of this privilege is considered restricted, which requires that the MRF process be followed to request the role.

(a) UMX Proxy Manage Group DCMA. This role provides the permissions to be able to assign users to the Proxy User Group.

(b) UMX Proxy User DCMA. This role provides the permissions to be able to submit a request for additional role assignments on behalf of users.

(c) UMX Proxy Limited User DCMA. This role provides the permissions to perform out-processing and reactivation tasks: Deactivate and Reactivate roles and Deactivate accounts.

(2) Deactivate an account. This workflow uses the configuration of Agency Account Approvers to select only the first-level account. The system will send out an action-based notification. This notification is used to capture the approval. When Agency approval is received, the system automatically sends an action-based notification to the DAI PMO Office to capture the final approval before automatically deactivating the account and sending the user an FYI notification that his/her account has been deactivated.

(3) Deactivate roles. This workflow uses the configuration of Agency Responsibility Approvers to select only the Agency designated approver. The system will send out an action-based notification. This notification is used to capture the approval. When Agency approval is received, the system automatically sends an action-based notification to the DAI PMO Office to capture the final approval before automatically deactivating the role assignments and sending the user a FYI notification that his/her role access has been deactivated.

SECTION 6: DAI PROCESS AREAS AND ROLE RESTRICTIONS

6.1. OVERVIEW. The DAI application is segregated into eight process areas. See Table 1, DAI Process Areas.

Table 1. DAI Process Areas

Process Area	Process Description
A2R	Acquire to Retire
B2R	Budget to Report
CA	Cost Accounting
O2C	Order to Cash
P2P	Procure to Pay
OTL	Oracle Time and Labor
UMX	User Management
OBIEE	Reporting

6.2. DAI ROLES AND RESPONSIBILITIES. Reference the Responsibility Description document located on the Resource Page for a complete listing of DCMA Responsibilities and descriptions.

6.3. DAI ROLE RESTRICTIONS. Additional restrictions apply to the following DAI roles to limit system access to PII, Super User roles, sensitive transactions, and supervisory functions.

a. **UMX Restricted Roles.** The following roles are restricted to FBSO personnel only:

(1) User Management DCMA.

(2) UMX Proxy User Limited DCMA.

(3) UMX Proxy User DCMA.

(4) UMX Proxy Manage Group DCMA.

b. **OBIEE Restricted Roles.** The following roles are restricted to FBSO personnel only:

(1) OBIEE Answers Subject Matter Expert (SME) DCMA.

(2) OBIEE Answers HR SME DCMA.

(3) OBIEE Dashboard SME DCMA.

(4) OBIEE Answers HR DCMA. Restricted to users within FBSO, FBSP and HC.

c. **OTL Restricted Roles.** The following roles are restricted to identified users:

(1) Super Timekeeper DCMA. Restricted to users within the FBSO, FBSP, Internal Auditors, FB Executive Director/Comptroller, and FB Deputy Director.

(2) Super Timekeeper DCMA Contingent Worker. Restricted to users within the FBSO, FBSP, Internal Auditors, FB Executive Director/Comptroller, and FB Deputy Director.

(3) Super Timekeeper DCMA Ungraded. Restricted to users within the FBSO, FBSP, Internal Auditors, FB Executive Director/Comptroller, and FB Deputy Director.

(4) OTL CSR DCMA. Restricted to users within the FBSO and FBSP only.

d. HR Restricted Roles. The following roles are restricted to personnel in HC, FBSO, and FBSP:

(1) HR CSR DCMA.

(2) HR Interface Administrator DCMA.

(3) HR Inquiry DCMA.

e. Restricted Financial Roles. The following roles are restricted to identified users:

(1) Projects Budgets All DCMA. Restricted to users within the Financial Business Budget Division (FBB), FBSP, the International and Federal Business Division (FBR) and the FBSO. Contractor personnel are not authorized access to this role.

(2) Projects Finance DCMA. Restricted to users within the Special Programs Directorate, and Planning and Budgeting Center Budgeting Group (FBAB). Contractor personnel are not authorized access to this role.

(3) Federal Administrator (Fed Admin) Budget Manager DCMA. Restricted to users within the FBB Execution Team and FBSO. Contractors are not authorized access to this role.

(4) Fed Admin Budget Analyst DCMA. DCMA users will utilize the Fed Admin Budget Manager DCMA role as authorized above. No additional users will have access to this role.

(5) P2P Cost Distribution DCMA. Restricted to users within the FB.

(6) P2P Maintenance DCMA. Restricted to users within the FBSO.

(7) P2P Supplier Maintenance DCMA. Restricted to users within the FBSO.

(8) O2C CA Project Manager DCMA. Restricted to users within FB.

(9) O2C Maintenance DCMA. Restricted to users within the FBSO.

(10) Projects Interface Submittal DCMA. Restricted to users within the FBSO and FBB.

(11) Projects Budgets Interface Submittal DCMA. Restricted to users within the FBSO and FBB.

(12) Projects Billing Interface Submittal DCMA. Restricted to users within the FBSO and FBB.

f. Supervisor Only Role and Guidelines.

(1) The OTL Supervisor Approver DCMA role is restricted to personnel that are coded as a supervisor in DCPDS.

(2) Temporary Assignments/Detailed Supervisor Restrictions. Detailed supervisors are not coded as supervisors in DCPDS and therefore will not be granted supervisor access in DAI to approve timecards.

(3) Supervisor Proxy Usage. Supervisors should only appoint other individuals designated in DCPDS as supervisors as proxy to approve time cards.

g. Exceptions to Restricted Role Policy. Users who require exception to policy consideration for any role identified as restricted will need to submit a Help Desk ticket to the FBSO for review. The Help Desk ticket shall include the role requested, justification, and supervisor approval. The FBSO will coordinate the appropriate approvals and documentation as required for the requested exception to policy.

SECTION 7: SEGREGATION OF DUTIES

7.1. OVERVIEW. DAI is configured to implement the SoD rules to restrict pre-defined, conflicted roles from being requested via the UMX System but this does not prevent the manual assignments of sensitive roles that can create transactions that are defined as financial risks. The combination of the defined sensitive transactions is what constitutes the risk, and in some cases, a user being assigned to perform specific sensitive transactions can introduce financial risk.

7.2. IMPLEMENTATION. As dictated by DAI PMO, DCMA will implement the SoD rules and User Access monitoring of the User role assignments for DAI system access to mitigate risk.

7.3. SoD MATRIX. Provides a graphical representation of potential conflicts at the role and entitlement levels. This matrix is independent of the DAI system and details the business driver for each transaction that is included as part of a risk statement.

a. Scope. The SoD Matrix provides a programmatic and balanced approach to internal controls.

b. Objective. Identify the methods and tools that will be used as part of the SoD Risk Mitigation Review. This will provide the framework to assist with identifying risks and the appropriate actions needed to remediate those risks.

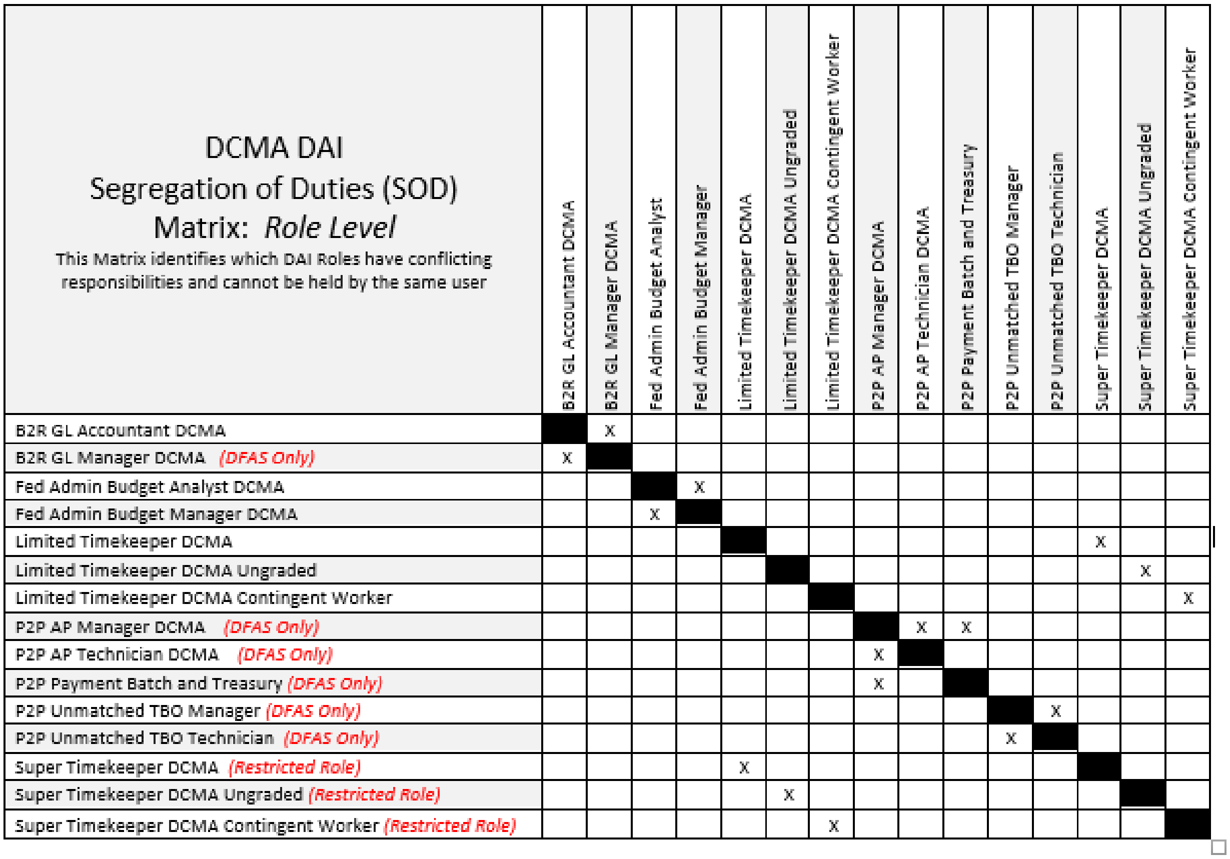
c. Approach. Implement an SoD Standard Operating Procedure (SOP) along with SoD Matrices.

(1) SOP. Provides the framework for business, mitigation, and remediation of the identified risks based on the risk statements that have been documented and set forth by the DAI PMO. The DCMA SoD SOP can be found on the FBSO 360 SharePoint page.

(2) DAI SoD Matrix. Provides a summarized view of the restricted role combination that has been defined by the UMX system. This Matrix is part of the user role request process and compliance review. Restricted role combinations are depicted with an "X" indicating an SoD conflict. See Figure 5, DAI Segregation of Duties Matrix.

(3) DCMA SoD Matrix. Provides a complete matrix that includes the restricted roles and sensitive transactions that are defined in the UMX and Governance Risk and Compliance (GRC) Systems. This matrix is part of the user role request process and compliance review. Refer to the DCMA DAI SoD Matrix SOP for full listing of sensitive transactions at the task level.

Figure 5. DAI Segregation of Duties Matrix



DCMA DAI Segregation of Duties (SOD) Matrix: *Role Level* This Matrix identifies which DAI Roles have conflicting responsibilities and cannot be held by the same user	B2R GL Accountant DCMA	B2R GL Manager DCMA	Fed Admin Budget Analyst	Fed Admin Budget Manager	Limited Timekeeper DCMA	Limited Timekeeper DCMA Ungraded	Limited Timekeeper DCMA Contingent Worker	P2P AP Manager DCMA	P2P AP Technician DCMA	P2P Payment Batch and Treasury	P2P Unmatched TBO Manager	P2P Unmatched TBO Technician	Super Timekeeper DCMA	Super Timekeeper DCMA Ungraded	Super Timekeeper DCMA Contingent Worker
B2R GL Accountant DCMA	■	X													
B2R GL Manager DCMA *(DFAS Only)*	X	■													
Fed Admin Budget Analyst DCMA			■	X											
Fed Admin Budget Manager DCMA			X	■											
Limited Timekeeper DCMA					■								X		
Limited Timekeeper DCMA Ungraded						■								X	
Limited Timekeeper DCMA Contingent Worker							■								X
P2P AP Manager DCMA *(DFAS Only)*								■	X	X					
P2P AP Technician DCMA *(DFAS Only)*								X	■						
P2P Payment Batch and Treasury *(DFAS Only)*								X		■					
P2P Unmatched TBO Manager *(DFAS Only)*											■	X			
P2P Unmatched TBO Technician *(DFAS Only)*											X	■			
Super Timekeeper DCMA *(Restricted Role)*					X								■		
Super Timekeeper DCMA Ungraded *(Restricted Role)*						X								■	
Super Timekeeper DCMA Contingent Worker *(Restricted Role)*							X								■

7.4 REPORTS. The User Management DCMA role provides “User by Responsibility” reports that detail role assignments along with the “UMX Audit Report” which provide details on who is assigned the roles and the approvers. The purpose of these reports is to provide the tools so that reviews can be performed by both the Agency and PMO to determine the state of the granted access.

SECTION 8: PERIODIC REVIEW OF ACCESS

8.1. OVERVIEW. The FBSO will perform periodic audits of DAI User access in accordance with FIAR requirements. This review will actively monitor and verify the appropriateness of users' access to DAI. Periodic reviews will be performed to ensure access is restricted to authorized users and assigned roles align with functional responsibilities.

8.2. ACCESS REVIEW PROCEDURES. The FBSO will provide the following oversight:

a. Frequency. Ensure periodic DAI account reviews are conducted at least annually.

b. Audit Requirements. The following aspects of User Access will be reviewed:

(1) Verify terminated or transferred user accounts have been removed in a timely manner.

(2) Reviews and monitors the effectiveness of the SoD matrix, identifies any users with conflicting roles, and mitigates the risk of users with incompatible privileges on at least an annual basis.

(3) Validates users have an approved DD Form 2875 for system authorization access that has been completed through the Agency system of record.

(4) Validates that the DD Form 577 has been completed for applicable DAI roles.

(5) Reviews DAI User Roles to ensure assigned roles are commensurate with functional responsibilities.

8.3. CORRECTIVE ACTIONS. Based on audit findings, the FBSO will take corrective actions to ensure compliance with FIAR requirements. Any corrective actions or conflicts that cannot be resolved by the FBSO will be submitted to the DAI PMO for action.

8.4. DOCUMENTATION. The FBSO will ensure all audit documentation and results are maintained per FIAR requirement.

GLOSSARY

G.1. ACRONYMS.

AP	Accounts Payable
CA	Cost Accounting
CIO	Chief Information Officer
CSR	Customer Service Representative
DAI	Defense Agencies Initiative
DCM	Military Personnel Office
DCMA-IT	Information Technology Directorate
DCPDS	Defense Civilian Personnel Database System
DD FORM 577	Appointment/Termination – Authorized Signature
DD FORM 2875	System Authorization Access Request
DLA	Defense Logistics Agency
eSAAR	Electronic System Authorization Access Request Form
FAST	Financial Accounting Support Team
FB	Financial and Business Operations Directorate
FBA	DCMA, Financial Business Operations, Planning and Budgeting Center
FBB	DCMA, Financial Business Operations, Budget Division
FBSO	DCMA, Financial Business Operations, Financial Systems Operations Branch
FBSP	DCMA, Financial Business Operations, Financial Payroll Support Branch
Fed Admin	Federal Administrator
FIAR	Financial Improvement and Audit Readiness
FMR	Financial Management Regulation
FYI	For Your Information
GL	General Ledger
HC	Human Capital Directorate
HR	Human Resources
IA	Information Assurance
IAO	Information Assurance Officer
IO	Information Owner
IWAM	Internal Web Access Management
MRF	DAI Manual Responsibility Form
O2C	Order to Cash
OBIEE	Oracle Business Intelligence Enterprise Edition
OTL	Oracle Time and Labor

P2P	Procure to Pay
PII	Personally Identifiable Information
PMO	Program Management Office
POC	Point of Contact
SAAR	System Authorization Access Request
SME	Subject Matter Expert
SoD	Segregation of Duties
SOP	Standard Operating Procedure
TBO	Transactions By Others
UMX	User Management

REFERENCES

DCMA Manual 4401-05, “Cyber Workforce Improvement Management,” TBD
DCMA Manual 4502-13, Privacy and Civil Liberties,” TBD
DCMA Responsibility Description Form November 20, 2017 (as amended)
DoD Directive 5105.64, “Defense Contract Management Agency (DCMA),” January 10, 2013
DoD 7000.14-R Financial Management Regulation (FMR) Vol 1, Chapter 7, November 2017 (as amended)
DoD 7000.14-R Financial Management Regulation (FMR) Vol 5, Chapter 5, November 2017 (as amended)
DoD 7000.14-R Financial Management Regulation (FMR) Vol 13, Chapter 9, November 2017 (as amended)
DoD 7000.14-R Financial Management Regulation (FMR) Vol 14, Chapter 2, November 2017 (as amended)
Federal Information System Controls Audit Manual (FISCAM), February 2, 2009