



DCMA Manual 4201-08

Human Resources Systems and Automated Tools

Office of Primary Responsibility:	Talent Management Capability
Effective:	May 26, 2019
Change 1 Effective:	April 7, 2023
Releasability:	Cleared for public release
Implements:	DCMA Instruction 4201, "Civilian Personnel," July 20, 2018
Internal Control:	Process flow is located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://dod365.sharepoint-mil.us/sites/DCMA-BCF-Talent_Management/SitePages/4201-08r--Human-Resources-Systems-and-Automated-Tools-.aspx
Approved by:	David H. Lewis, VADM, USN, Director
Change 1 Approved by:	David G. Bassett, LTG, USA, Director

Purpose: This issuance is in accordance with the authority in DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," implements policy established in DCMA Instruction 4201, "Civilian Personnel," assigns responsibility and prescribes general principles associated with Human Resources Systems and Automated Tools.

SUMMARY OF CHANGES

This issuance has substantive changes. The most notable are as follows:

- Updated Paragraph 1.2, by revising servicing organization's information
- Updated Paragraph 2.1, by changing Human Capital to Total Force
- Added Paragraph 2.2
- Updated Paragraph 3.1.a, by changing "trigger" to "initiate"
- Updated procedures for processing of request forms in Paragraph 3.2
- Moved Paragraph 3.2.b.(3), to Paragraph 2.1.j, under Responsibilities
- Updated procedures for Change Management Requests in Paragraph 3.5

TABLE OF CONTENTS

SUMMARY OF CHANGES	2
SECTION 1: GENERAL ISSUANCE INFORMATION	4
1.1. Applicability.....	4
1.2. Policy.....	4
SECTION 2: RESPONSIBILITIES	5
2.1. Executive Director, Total Force (TF) Directorate or Designee	5
2.2. Human Resources Office	5
SECTION 3: PROCEDURES	7
3.1. Account Requirements.....	7
3.2. Request Procedures.....	7
3.3. Segregation of Duties.....	9
3.4. Periodic Access Review.....	9
3.5. Change Management	10
GLOSSARY	11
G.1. Definitions.....	11
G.2. Acronyms	12
REFERENCES	13

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to all DCMA activities unless higher-level regulations, policy, guidance, or agreements take precedence.

1.2. POLICY. It is DCMA policy to:

a. Implement policy and establish uniform DCMA-wide procedures and guidelines, delegate authorities and assign responsibilities regarding Human Resources (HR) systems and automated tools access.

b. Assign responsibility for monitoring the appropriateness of accounts as well as the account holder documentation to the servicing Human Resources Office (HRO) and DCMA.

c. Have a documented process to ensure access and privileges are validated as well as maintained per the documented regulations.

d. The guidance within this Manual is applicable to systems directly owned by or licensed to the servicing HRO or when the account administration responsibility has been delegated by the system owner. This includes the Defense Civilian Personnel Data System (DCPDS), electronic Official Personnel Folder, servicing HRO Access Control Lists, Business Objects/Business Intelligence, USA Staffing which includes Onboarding Manager, and all other applications assigned to the servicing HRO for administrative management.

e. Execute this Manual in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBILITIES

2.1. EXECUTIVE DIRECTOR, TOTAL FORCE (TF) DIRECTORATE OR DESIGNEE.

The Executive Director of TF (or designee) will:

- a. Develop and implement HR System Access policy and guidance.
- b. Follow all requirements of the servicing HRO Administered Account Maintenance and recommend updates and corrections where required.
- c. Request account termination when employees no longer require system access or leave the organization.
- d. Respond timely to annual account validation reviews issued by the servicing HRO Systems Helpdesk, Information System Division.
- e. Review requests for accuracy, completeness, and appropriateness of the user roles and organizational access.
- f. Perform quarterly reviews to identify users who have changed positions, moved organizationally, or who are no longer employed and take appropriate steps to extend or terminate/end-date accounts.
- g. Notify supervisors and users to perform annual recertification of accounts.
- h. Follow all requirements of this Manual and recommend updates and corrections where required.
- i. Adjudicate disputes through delegated access to Total Force Business Operations Division (TFB) from the TF Executive Director.
- j. Realignment modifications will be submitted by TFB to the HRO Systems according to the organization's validated realignment crosswalk provided by the Financial and Business Executive Directorate, Manpower and Organization Management Division (FBO).

2.2. HUMAN RESOURCES OFFICE. The servicing HRO will:

- a. Grant system access.
- b. Provide reports and data upon request.
- c. Provide monthly data to complete length of service and retirement certificates for serviced employees.
- d. Provide training on automated tools, systems, upgrades, or applications as requested.

e. Serve as Change Control Board member for all HR Information Technology functional boards.

f. Provide written notes regarding any changes that will be impactful to the agency or employees.

SECTION 3: PROCEDURES

3.1. ACCOUNT REQUIREMENTS. Supervisors must determine which HRO systems are required for positions within their organization, and complete the forms (or request user completion of forms) required to establish, change, or terminate/end-date HRO system accounts. The following actions should initiate a form submission to add, modify, or terminate/end-date an account:

- a. A user is new to the organization.
- b. A user leaves an organization. It is essential account terminations are processed immediately if an account holder leaves the agency.
- c. Account access rights or system roles are expanded or diminished, or new systems are required to meet work assignment changes.
- d. A user's supervisor changed, whether or not the organization was changed.
- e. A user's organization code changed, whether or not the supervisor was changed.
- f. A user legally changes his/her name.

3.2. REQUEST PROCEDURES.

a. Initial Account Request.

(1) When requesting access, user must complete Part I of the DD Form 2875, "System Authorization Access Request (SAAR)," and the servicing HRO Employee User Account Request Form (URF). Refer to the Resource Page in the Templates section. Once completed and signed, the user will send both forms to their supervisor for approval via encrypted email.

(2) The supervisor completes Part II of the DD Form 2875 and the servicing HRO URF, verifying requested user access and authorizing account setup with an electronic signature.

(3) The supervisor must send DD Form 2875 via encrypted email to obtain signatures from the Personnel Security Manager and a DCMA authorized Information System Security Officer or designee for completion of the form. The minimum Personnel Security Investigation requirements for system access is a National Agency Check with requests for information.

(4) Once all signatures are obtained, the supervisor or designee will upload the completed signed forms to the HR System Access Requests site. Refer to the Resource Page in the Points of Contact section for Uniform Resource Locator or computer address.

(5) TFB reviews forms for completeness and accuracy. Forms not completed appropriately will be returned to the sender for correction and resubmission.

(6) TFB will submit the request forms via encrypted email to the HRO Systems Helpdesk. Refer to the Resource Page for the email to HR service processing.

(7) Once the accounts have been established, the servicing HRO or TFB staff will notify the user that access has been granted along with login information and guidance. Refer to the Resource Page for the Access Request Process Flowchart.

b. Modification Account Requests.

(1) If the system name and supervisor have not changed from the original DD Form 2875 and the Information Assurance/Cybersecurity training is dated within the last 12 months, the URF will be accepted for account modifications. Follow same guidance in Paragraph 3.2.a.(1).

(2) If the HRO Systems does not have a valid DD Form 2875 on file, the supervisor changes, or the organization is not the same as what is on the initial DD Form 2875, then the user must complete a new DD Form 2875 and the Employee URF. Follow initial request guidance in Paragraph 3.2.a.(1).

c. Deactivating Account Requests.

(1) Supervisors must complete and sign the first page of the DD Form 2875 and submit to TFB to deactivate accounts. The supervisor will sign the form, but the following signatures are not required: Employee, Individual Systems Security Officer (ISSO) or Personnel Security Manager.

(2) Refer to Resource page, Guidance section for guidance on form completion.

(3) If the servicing HRO has a Separation/Loss Standard Form 50, "Notification of Personnel Action," for the user, all user accounts administered by the servicing HRO will be deactivated.

(4) Email notification and/or the DD Form 2875 from the supervisor will be accepted by TFB to deactivate the account(s) via inbox found in the Requesting HR Systems and Tools Access section on the Resource Page.

d. Access Approval.

(1) Requests for Agency-wide access must be approved by the TF Executive Director with coordination through TFB before access is granted.

(2) For all other requests, TFB has the authority to "Approve" or "Deny" access requests. Approval and level of access is based on the need to access this information to perform one's job responsibilities as provided for in the DoD Directive 5400.11, "DoD Privacy Program."

3.3. SEGREGATION OF DUTIES. TFB is responsible for ensuring sufficient separation of duties for roles with DCPDS responsibilities. Refer to the Resource Page for DCPDS Segregation of Duties Matrix in the References section.

3.4. PERIODIC ACCESS REVIEW.

a. Quarterly Review.

(1) TFB will perform reviews on a quarterly basis to identify users who have changed positions, moved organizations, or are no longer employed by the requesting office.

(a) TFB will submit a servicing HRO Service Portal ticket or send an email to the servicing HRO Systems Helpdesk to terminate/end-date all accounts for users who have separated from DCMA within 10 business days of review completion.

(b) TFB will contact the user if the person has changed positions other than a career promotion or realignment. If there is no response, accounts will be terminate/end-date within 10 business days of requested return date.

b. Annual Review (Recertification).

(1) TFB will prepare a list of all active DCPDS account holders to perform annual recertification of accounts.

(2) TFB will send account lists to the Director, Commander, Deputy, and Mission Support Office or Chief requesting management to identify any accounts requiring termination or change, and verify that any remaining accounts are still active and valid. Management will have 10 business days to respond in writing. If there is no response, accounts will be terminated/end-dated within 10 business days of requested return date.

(3) Upon receipt of management response to the annual review, TFB will submit a request to terminate/end-date accounts as required to the servicing HRO Systems. If account changes are requested, ensure appropriate paperwork is completed, signed, and submitted.

(4) Annual review certification paperwork will be stored for a period of 3 years. Records will identify the information sent to management, management's response, and action taken to resolve account issues. User paperwork and account maintenance records will be annotated to indicate actions taken.

c. Internal Controls.

(1) TFB will ensure evidence of quarterly reviews, to include identification of personnel changes impacting account records and actions taken to update records, if available.

(2) TFB will ensure evidence of annual recertification reviews, to include management responses and actions taken to update records, if available.

3.5. CHANGE MANAGEMENT. Any change request to HR Systems utilized by DCMA must follow the procedures contained within the requirements of the servicing HRO Administered Account Maintenance.

GLOSSARY

G.1. DEFINITIONS.

Change Control Board. A review body with authority for approving changes that are consistent with DCPDS performance requirements, budget costs, and schedule.

DCPDS. The database of records for civilian employees of the DoD. Used to process personnel actions and maintain workforce data. Features: MyBiz+ and MyTeam, Employment Verification, Personnel Actions, Personal Information and Request for Personnel Action Tracker.

Financial & Business Operations Executive Directorate. The Manpower and Organization Management Division is responsible for providing realignment crosswalks.

HRO System Helpdesk. The entity responsible for providing HR systems & tools support.

Individual Systems Security Office. The individual or appointee of the office responsible for approving access to the system being requested.

Mission Support Office. The Administrative staff that provides support to the Director and personnel within an organization.

Personnel Security Manager. Validates the background investigation or clearance information.

Supervisor. Certifies the user requires access as requested.

Uniform Resource Locator. Computer web address.

User. The person requesting the access.

GLOSSARY

G.2. ACRONYMS.

DCPDS	Defense Civilian Personnel Data System
DD Form 2875	System Authorization Access Request (SAAR)
HR	Human Resources
HRO	Human Resources Office
Standard Form 50	Notification of Personnel Action
TF	Total Force
TFB	Total Force Business Operations Division
URF	Employee User Account Request Form

REFERENCES

DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013
DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014