

# DCMA Manual 4201-14

# **Personnel Accountability**

**Office of Primary** 

**Responsibility:** Talent Management Capability

Effective: April 18, 2018

**Releasability:** Cleared for public release

**Implements:** DCMA-INST 4201, "Civilian Personnel"

**Incorporates and Cancels:** DCMA-INST 562, "Personnel Accountability," January 26, 2016

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/TM/SitePages/4201-14r.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)," establishes processes and procedures to implement, within DCMA, the requirements contained in DoD Instruction 3001.02, "Personnel Accountability in Conjunction with Natural or Manmade Disasters."

# TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION	3
1.1. Applicability	3
1.2. Policy	
SECTION 2: RESPONSIBILITIES	4
2.1. Director, DCMA	4
2.2. Component Heads and Contract Management Office (CMO) Commanders/Directors	4
2.3. Director of Security (DCS)	4
2.4. Executive Director, Office of Internal Audit and Inspector General (DM)	5
2.5. Executive Director, Human Capital (HC).	5
2.6. Executive Director, Information Technology (IT) and Chief Information	
Officer (CIO)	5
2.7. PAPM	5
2.8. PAA	6
2.9. Managers and Supervisors	6
2.10. DCMA Employees.	7
SECTION 3: PROCEDURES	8
3.1. General	8
3.2. Preparedness	8
3.3. Conducting and Reporting PA	.10
3.4. Out-processing Requirements	.12
GLOSSARY	.14
G.1. Definitions	.14
G.2. Acronyms	.16
REFERENCES	.17

## **SECTION 1: GENERAL ISSUANCE INFORMATION**

- **1.1. APPLICABILITY.** This Manual applies to all DCMA organizations, facilities, activities, and personnel.
- **1.2. POLICY.** DCMA must establish and maintain Personnel Accountability (PA) programs and procedures at all levels of the organization that facilitate the expeditious accountability of assigned personnel (active duty military, DoD civilian employees, and contractors with a contractual obligation to DCMA outside the continental United States (OCONUS)) in compliance with DoD Instruction (DoDI) 3001.02.
- a. PA is a shared responsibility between and among Commanders/Directors, managers, supervisors, and assigned personnel.
- b. The senior management official at DCMA offices have overall responsible for the accountability of all DCMA personnel assigned to or housed (e.g., mission partners or hotelers) at their DCMA office. Managers and supervisors of employees housed at DCMA offices must fully support the PA program of the host senior management official.
- c. In accordance with (IAW) DoDI 3001.02, the DoD Personnel Accountability Reporting System (PARS) serves as the DoD system of record (SOR) for conducting and reporting PA. Within DCMA, the Fourth Estate Personnel Accountability and Assessment System (FEPAAS) and the various Service accountability systems serve as the authoritative sources for feeding PA information to the DoD PARS.
- d. Employees and responsible management officials will jointly ensure accountability information is accurately recorded and maintained in the various DoD systems that feed the PARS. Such systems include the FEPAAS, the various Service accountability systems, the Defense Civilian Personnel Data System (DCPDS), Trusted Associate Sponsorship System (TASS), and DoD milConnect.
- e. Once PA operations are ordered or initiated, employees and management officials will promptly conduct PA operations to facilitate the timely and accurate reporting of accountability.

#### **SECTION 2: RESPONSIBILITIES**

**2.1. DIRECTOR, DCMA.** The Director, DCMA, must establish and resource a PA Program that complies with the requirements of DoDI 3001.02 and other higher-level guidance.

# **2.2. COMPONENT HEADS AND CONTRACT MANAGEMENT OFFICE (CMO) COMMANDERS/DIRECTORS.** Component Heads and CMO Commanders/Directors must:

- a. Establish organizational PA programs and procedures that facilitate the expeditious accountability of personnel in compliance with this Manual and DoDI 3001.02.
- b. Designate a primary and alternate PA Administrator (PAA) for the organization that will have responsibility for the implementation and maintenance of the organization's PA Program. Report designations to the DCMA Personnel Accountability Program Manager (PAPM).
- c. Establish organizational-specific processes and procedures to rapidly account for DCMA personnel assigned to, housed with, or visiting offices or facilities under their responsibility. Such procedures will include the use of Emergency Recall Rosters (ERRs).
- d. Establish and maintain procedure(s) that ensure accurate PA information is recorded and maintained in the FEPAAS and in the other DoD systems identified in paragraph 1.2.d.
  - e. Ensure personnel are trained and comply with the requirements of this Manual.
- f. Prepare and submit Situation Report (SITREP) IAW DCMA-INST 1002, "Situation Report (SITREP)" at the initiation and completion of PA operations (Region, International, and Special Directorate Commanders/Directors only).
- g. Report deaths of DCMA personnel using the procedures contained in Human Capital Business Practice Number 32 or DoDI 1300.18, "Department of Defense (DoD) Personnel Casualty Matters, Policies, and Procedures," as applicable.
- h. Establish processes and procedures to ensure Personally Identifiable Information (PII) is safeguarded IAW DoD Directive (DoDD) 5400.11, "DoD Privacy Program."

## **2.3. DIRECTOR OF SECURITY (DCS).** The DCS must:

- a. Establish and maintain an Agency PA Program that meets the spirit and intent of DoDI 3001.02 and tailored to the unique DCMA environment.
- b. Appoint, in writing, a PAPM responsible for the day-to-day execution and management of the PA Program.
  - c. Advocate and allocate resources in support of the PA Program.

# 2.4. EXECUTIVE DIRECTOR, OFFICE OF INTERNAL AUDIT AND INSPECTOR GENERAL (DM). The Executive Director, DM must:

- a. In addition to the requirements listed in paragraph 2.2, biennially conduct and document an assessment of the Agency's PA Program as required by DoDI 3001.02, enclosure 2, paragraph 7.
- b. Ensure reports are marked and safeguarded IAW DoD Manual 5200.01, "DoD Information Security Program," Volumes 1 through 4.

# **2.5. EXECUTIVE DIRECTOR, HUMAN CAPITAL (HC).** The Executive Director, HC, must:

- a. In addition to the requirements listed in paragraph 2.2, establish processes and procedures that provides for the accurate recording of accountability-related information (duty location, contact information, etc.) in DCPDS.
- b. Upon request of the PAPM, provide updated personnel lists/reports, by specific criteria, to support PA operations and reporting.

# 2.6. EXECUTIVE DIRECTOR, INFORMATION TECHNOLOGY (IT) AND CHIEF INFORMATION OFFICER (CIO). The Executive Director, IT must:

- a. In addition to the requirements listed in paragraph 2.2, establish and maintain toll free emergency call-in numbers to support rapid accountability.
- b. Provide telecommunications devices to the deaf (TDD) or a TDD line(s) for hearing impaired employees.
- c. Provide IT technical support to ensure communications and connectivity with the FEPAAS.

#### **2.7. PAPM.** The PAPM must:

- a. Establish and maintain Agency-level PA policy and tools.
- b. Provide training and FEPAAS access to designated PAAs.
- c. Schedule, coordinate, and conduct PA exercises on a quarterly basis in selected geographic locations to exercise and test accountability readiness.
- d. Notify Executive Directorates, Regions, and/or CMO headquarters (HQ) when a higher HQ or Agency directed "Order to Account" is initiated; and provide assistance to PAAs in resolving and submitting accountability reports, as applicable.

- e. Report Agency-level PA status to higher HQ elements (OSD and/or the Chairman of the Joint Chiefs of Staff (CJCS)), when directed.
- f. Facilitate the submission of DD Form 2875, "System Authorization Access Request," to the Director, Defense Manpower Data Center (DMDC), to obtain account access to the PARS; and train designated personnel on its use.
- g. Facilitate the posting of emergency call-in numbers on the Military OneSource Website (a link is available on the resource page of this Manual).
- h. Grant FEPAAS system administrator access to Primary Regional PAAs to facilitate PA operations.
  - i. Represent the Agency at higher-level PA forums.
  - j. Identify and report PA resource requirements to the Director of Security.

#### **2.8. PAA.** PAAs must:

- a. Establish and maintain effective organizational PA Programs that ensure the prompt and accurate reporting of accountability IAW this Manual.
- b. Provide FEPAAS "SUPV" access to designated supervisory and managerial personnel, as deemed necessary, to expeditiously conduct PA operations; and train these individuals in its use.
- c. Obtain and maintain access to the DoD PARS (primary Regional PAAs only). Contact the DCMA PAPM for assistance in obtaining PARS access.
- d. Obtain and maintain FEPAAS system administrator access (primary Regional PAAs only). Contact the DCMA PAPM for assistance in obtaining this access.
- e. On order of the DCMA PAPM, assume responsibility of Agency-level PA operations in support of a DCMA HQ continuity event (designated Regional PAAs only).
  - f. Safeguard PII IAW with DoDD 5400.11.

#### **2.9.** MANAGERS AND SUPERVISORS. DCMA Managers and Supervisors must:

- a. Validate the information in blocks 38 and 39 of Standard Form (SF) 50, "Notification of Personnel Action," for assigned personnel to ensure accuracy of the duty geographic location code and duty station location information (city, county, and state).
  - b. Ensure PA data in the various systems identified in paragraph 1.2.d. remains accurate.

- c. With employees housed with other DCMA organizations (i.e., missions partners/hotelers), report employee names, organizational code(s), and non-duty contact information quarterly to the host PAA and ensure this information remains accurate
- d. Validate, on a monthly basis, that assigned DCMA civilian employees are in the FEPAAS and any departed employees have been removed. Report discrepancies to the responsible Region PAA or Agency PAPM for corrective action.
- e. When directed, expeditiously account for assigned personnel using the guidance issued in this Manual and by the local Commander/Director, and report results to the responsible PAA.
- f. Create, maintain, and terminate Internal Web Access Management (IWAM) accounts for assigned employees IAW DCMA-INST 632, "Onboarding Process," and the IWAM User Manual. Ensure duty and non-duty contact information remains accurate and is identical to that information in their employee's "My Info" tab in the FEPAAS.
  - g. Safeguard PII IAW DoDD 5400.11.

## **2.10. DCMA EMPLOYEES.** DCMA employees must:

- a. Validate and/or update current residence and work address, with contact information (duty and non-duty telephone number and email address) using the DoD milConnect and FEPAAS Web sites at least during the periods of March through April and September through October or when there is a change in information (links are located on the resource page).
- b. When directed or following a disaster, promptly report personal accountability status using the FEPAAS (link is located in the resource page). If employees lack the capability to access FEPAAS, employees must promptly report their accountability status to the responsible manager, supervisor, senior representative, or commander/director.
- c. Provide duty and non-duty telephone number to the responsible manager, supervisor, senior representative, and/or PAA; and update information as necessary.

## **SECTION 3: PROCEDURES**

#### 3.1. GENERAL.

- a. DoDI 3001.02 establishes the requirements for the execution of the DoD PA Program. This reference clearly defines PA as a joint responsibility of management and employees.
- b. The DoD PARS is the DoD definitive source for reporting accountability within DoD. Information within the DoD PARS is populated by a variety of feeder systems. The most efficient way for personnel to update their personal information in the DoD PARS is through use of the DoD milConnect website (the link is available on the resource page of this Manual).
- c. Within DCMA, the FEPAAS and the various Services Personnel Accountability and Assessment System (PAAS) serve as the authoritative sources for feeding PA information to the DoD PARS. The FEPAAS and the various Services PAAS, provide an automated means for personnel to self-report accountability using an internet based capability accessible from any computer or smart phone. These PAAS automatically record accountability status in the DoD PARS. As such, it is imperative that employees ensure their contact and work information in the various PAAS remains current.
- d. PII used in connection with PA operations and reporting must be safeguarded IAW DoDD 5400.11.
- e. Unless otherwise directed, DCMA activities OCONUS follow the PA policies and procedures of the responsible Combatant Commander (COCOM) and/or local host DoD installation when conducting PA operations.

## 3.2. PREPAREDNESS.

- a. PA begins on the first day an employee is assigned to DCMA and runs through the full lifecycle of one's assignment/employment. Success in PA operations lies in preparation. As such, this paragraph addresses the preparation actions required to ensure effective and efficient accountability operations. Refer to the Personnel Accountability Quick Reference Guide, located on the resource page of this Manual, for additional preparation actions.
  - b. Information Readiness.
- (1) DoD Civilian and OCONUS Contractor Personnel. When PA information changes or at least during the periods of March through April and September through October, annually, DoD civilian employees and OCONUS contractors (with a contractual obligation to DCMA) must update/validate their accountability information using the "My Info" tab in the FEPAAS and in the "Update Personal Contact Info" link on the DoD milConnect website.
- (a) FEPAAS Update. During the periods identified in paragraph 2.10.a., using the "My Info Contact Information" tab in FEPAAS, employees must validate their data by selecting the "Verify Info as Current" button or edit their data using the "Edit Contact Info" button.

- (b) DoD milConnect Update. During the periods identified in paragraph 2.10.a., using the "Update Personal Contact Info" link on the DoD milConnect website, personnel must validate/update their data under the "Personal" and "CIV" tabs and then select submit.
- (2) Service Members. Military service members must update/validate their accountability information in the appropriate Service PAAS and on the DoD milConnect Web site.
- (3) To ensure accomplishment of the requirements in paragraph 3.2.b.(1), managers/supervisors and/or senior representatives must confirm employees have updated their information via the "My Info Contact Information" and "Recall Roster Reports" tabs in the FEPAAS.
- c. To ensure preparedness and familiarity with PA operations, Commanders/Directors will conduct a PA exercise annually, not later than the end of April, and report completion of the exercise to the Regional PAA and DCMA PAPM using the following email address: personnelaccountability@dcma.mil. The format for reporting completion of PA exercises is located on the resource page of this Manual.
- d. Within 72 to 120 hours (3 to 5 days) of a known potential incident for which accountability operations may be initiated (example: hurricane, flood, snowstorm, etc.), the following essential preparatory actions must be taken.

#### (1) PAAs must:

- (a) Upon the completion of the requirements in 3.2.b., print a "Recall Roster Report" from the FEPAAS.
- (b) Issue managers, supervisors, and/or senior representatives detailed guidance on when and how personnel are to report their accountability status following the event.
  - (2) Managers, supervisors, and senior representatives must:
- (a) Direct all DCMA personnel for which they are responsible for accountability to update/validate their accountability information IAW paragraph 3.2.b.
- (b) Provide employees with phone numbers (duty and non-duty) and email addresses of the responsible managerial chain (supervisor, manager, senior representative, PAA, commander/director, etc.) to support accountability efforts.
- (c) Provide detailed guidance to employees on when and how to report their accountability status.

#### 3.3. CONDUCTING AND REPORTING PA.

a. Within DCMA, PA operations may be initiated as a result of an "Order to Account" issued by higher authority or as a result of a localized incident (natural or man-made disasters, incidents of severe weather, decisions to initiate Continuity of Operations (COOP) plans, etc.). Contained within this paragraph are the procedures and reporting requirements associated with conducting and reporting PA.

#### b. Order To Account.

- (1) The initiation of PA operations based on an "Order To Account" may be issued by the responsible OSD element, CJCS, the responsible COCOM, the DCMA Director, or a host Installation Commander. Such an order may be issued Agency-wide, may be organizational-specific, or may be issued for a specific country, state, and/or county affected by a disaster.
- (2) When a higher HQ or Agency-level "Order To Account" is issued, the following actions will be accomplished:
- (a) The Agency PAPM (or designated representative) will disseminate the order to the affected HQ Component(s) and/or Region(s) HQ.
- (b) Upon receipt of an "Order To Account," the responsible Component Head(s) and the Region Commander(s) (or designated representative) will ensure prompt dissemination of the order to applicable commands/organizations. Region Commanders will also submit initial SITREP to HQ validating receipt of the "Order to Account" and affirming accountability efforts have begun.
- (c) Commanders/Directors issued an "Order To Account" will promptly direct managers, supervisors, senior representatives, etc., to initiate PA operations and continue those efforts until positive accountability is validated for all DCMA personnel for which they (Commander/Director) are responsible for accountability. Here are the categories of personnel for which positive accountability must be established under an "Order To Account":
  - 1. Active duty military and their family members.
  - 2. DoD civilian employees.
- <u>3</u>. Family members of OCONUS DoD civilian employees and DCMA-affiliated contractors receiving benefits associated with being evacuated to an authorized safe haven.
- <u>4</u>. OCONUS DCMA-affiliated contractors (those with a contractual obligation to DCMA).
- (d) During the conduct of PA operations, these are the acceptable means for validating positive accountability:

- $\underline{1}$ . DoD civilian and OCONUS DCMA-affiliated contractor personnel may account for themselves by logging into the FEPAAS.
- <u>2</u>. Military personnel may account for themselves by logging into the applicable Service PAAS/protocol to report accountability.
- $\underline{3}$ . If internet access is not available, managers/supervisors may manually account for their employees when:
  - a. An employee(s) is in the presence of the manager/supervisor.
- $\underline{\mathbf{b}}$ . Notification is made to the manager/supervisor by an employee via telephone, text message, or email.
  - (e) Non-Accountability.
- <u>1</u>. Military Personnel. When DCMA military personnel cannot be accounted for, the responsible official(s) (manager, supervisor, organizational PAA, etc.) will notify the DCMA HQ Military Personnel Office (DCMA-DCM) of the situation. DCMA personnel will ensure coordination with the respective military service to further address the situation.
- <u>2</u>. DoD Civilian Employees and OCONUS Contractors. When DoD civilian employees and/or OCONUS contractors (with contractual obligation to DCMA) cannot be accounted for, the responsible official(s) (manager, supervisor, organizational PAA, etc.) will record the status of the specific employee(s) in the FEPAAS using one of the following categories:
  - Deceased (due to event)
  - Deceased (not by event)
  - Deployed
  - Transferred
  - Separated/Retired
  - Deserter
  - Other
  - (3) Reporting Accountability.
- (a) Once 100 percent accountability is obtained and validated by the Region PAAs and/or the Agency PAPM, the responsible Region Commander (or designated representative) will submit a final SITREP officially notifying the Agency HQ of the closure of accountability operations. SITREPs are not required for HQ Components as accountability reporting progress is monitored and reported by the PAPM.
- (b) In the event 100 percent accountability cannot be obtained within 8 hours of the initial order to account, the applicable Region Commander(s) will submit an updated SITREP

daily, not later than 1600 hours (local), reflecting the progress and challenges of accountability operations.

- (4) Reporting Deaths. During the course of conducting accountability, should it be determined that a DCMA employee(s) has died, report the death IAW the following guidance:
- (a) DoD Civilian Employee. Follow the guidance in DCMA Human Capital Business Practices Number 32.
- (b) Active Duty Military Personnel or their Family Member(s). Follow the guidance in DoDI 1300.18.

#### c. Localized Incidents.

- (1) When localized incidents occur which warrant the initiation of accountability operations, DCMA Commanders/Directors may order the initiation of such operations for personnel and operations for which they are assigned PA responsibility. Such incidents might include but are not limited to natural or man-made disasters, incidents of severe weather, decisions to initiate COOP plans, terrorist threats, etc.
- (2) When a DCMA Commander/Director initiates PA operations at the local level, the following must be accomplished:
- (a) If the FEPAAS is to be used during the local PA operation, contact the Region PAA or Agency PAPM so an event can be initiated.
- (b) Promptly notify the next higher HQ of the initiation of PA operations, along with the specific details of the situation.
- (c) Once 100 percent accountability is obtained, report the closure of accountability operations to the next higher HQ. If 100 percent accountability cannot be obtained, report results to the next higher HQ for further action and reporting.
- (d) Region HQ will report accountability operations IAW the guidance contained in paragraph 3.3.b.(3).
- **3.4. OUT-PROCESSING REQUIREMENTS.** Commanders/Directors must establish procedures that ensure personnel out-processing the organization are removed from the various authoritative databases that support PA operations. This paragraph discusses the appropriate out-processing requirements relative to the PA Program.
- a. Military Personnel. Managers/supervisors of DCMA military personnel must ensure accomplishment of the requirements of DCMA-INST 1028, "Military In-processing and Outprocessing."

- b. DoD Civilian Employees. Managers/supervisors of DoD civilian employee must ensure accomplishment of the following out-processing requirements:
  - (1) Ensure employees out-process the organization IAW existing DCMA guidance.
- (2) Coordinate with the DCMA Human Capital Directorate to ensure an appropriate final SF 50 is initiated and processed for employees departing from or transferring within the organization.
- (3) Contact the Regional PAA or Agency PAPM to ensure the affected employee(s) have been transferred out of their Org ID in the FEPAAS.
  - c. DCMA Affiliated Contractor Personnel.
- (1) Contracting Officer Representatives (CORs) must notify the responsible trusted agent (TA) of all contractor departures from DCMA.
  - (2) The TA must ensure the contractor is deactivated in the TASS.
- (3) CORs must ensure the departing contractor's assigned equipment, Common Access Card (CAC), security badge(s), and other information and/or materials are collected. All departing contractors are required to visit their security office prior to departure for any required debriefings.
  - (4) CORs must ensure the contractor's IWAM account is deleted.

## **GLOSSARY**

#### **G.1. DEFINITIONS.**

**Accounted For.** A person's status and whereabouts have been confirmed by a commander and/or supervisor. Family members of a person in a desertion status will not be accounted for and will be reconciled off the DMDC baseline. A DoD Component must consider its personnel accounted for when:

- The person is physically present
- The person has been contacted or has made contact (i.e., by telephone or other means)
- The person is in an official status of unauthorized absence, desertion, deceased, or missing
- The person will not be physically accounted for and will be reconciled off the PARS baseline
- The employee or military member indicates his or her family members are accounted for or accountability is verified through other means

**Civilian Employee.** Appropriated fund (DoD civilian employees) and nonappropriated fund employees. This does not include foreign national employees in OCONUS.

**Contractor.** An employee of a firm, corporation, partnership, association, or other legal non-Federal entity who enters into a contract directly with the DoD to furnish services, supplies, or construction and working in and/or on a DoD facility, including commercial facilities. Foreign governments, representatives of foreign governments, or foreign corporations wholly owned by foreign governments that have entered into contracts with the DoD are not defense contractors.

**DCMA Employees, DCMA Persons, or DCMA Personnel.** These terms includes military, DoD civilian, and OCONUS contractor personnel with a contractual obligation to DCMA.

**Geographical Area of Coverage.** An area established by the CJCS, in conjunction with the Federal Emergency Management Agency (FEMA), when applicable, in which DoD-affiliated PA will be accomplished, using the PARS, upon the occurrence of a natural or manmade disaster.

**Hoteling/Mission Partners.** Employees who are not assigned to the current CMO and have been assigned to a vacant desk.

**Incident.** An occurrence or event, natural or manmade, that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wild land and urban fires, floods, hazardous material (HAZMAT) spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war-related disasters, medical and public health emergencies, and other occurrences requiring an emergency response.

**Military OneSource.** A confidential DoD-funded program providing comprehensive information on every aspect of military life at no cost to active duty, National Guard, and

Reserve members, and their families. Information includes, but is not limited to, deployment, reunion, relationships, grief, spouse employment and education, parenting and childhood services. It is a virtual extension to installation services.

**OCONUS.** Locations outside the continental United States, including the States of Hawaii and Alaska, the Commonwealth of Puerto Rico, Guam, the Commonwealth of the Northern Mariana Islands, and U.S. territories.

**Order To Account.** An official order requiring execution of PA reporting procedures.

**Personal Information**. Information about an individual that identifies, links, relates, or is unique to, or describes him or her; e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information.

**Personally Identifiable Information (PII).** Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual.

**Personnel Accountability (PA)**. The process of determining the status and whereabouts of all assigned or attached personnel at the social security number level of detail.

**Residence Address**. This is the location where the employee is dwelling while employed by the Agency and can be located in case of any manmade or natural disaster. This is not the employees Home of Record, domicile, nor tax address.

## **GLOSSARY**

#### G.2. ACRONYMS.

CJCS Chairman of the Joint Chiefs of Staff

CMO Contracting Management Office

COCOM Combatant Commander COOP Continuity of Operations

COR Contracting Officer Representative

DCPDS Defense Civilian Personnel Data System

DCS Director of Security

DM Office of Internal Audit and Inspector General

DMDC Defense Manpower Data Center

DoDD DoD Directive
DoDI DoD Instruction

FEPAAS Fourth Estate Personnel Accountability and Assessment System

HC Human Capital HQ Headquarter

IAW In Accordance With IT Information Technology

IWAM Internal Web Access Management

OCONUS Outside the continental United States

PA Personnel Accountability

PAA Personnel Accountability Administrator

PAAS Personnel Accountability and Assessment System

PAPM Personnel Accountability Program Manager PARS Personnel Accountability Reporting System

PII Personally Identifiable Information

SF Standard Form

SF 50 Notification of Personnel Action

SITREP Situation Report

TA Trusted Agent

TASS Trusted Association Sponsorship System
TDD Telecommunications device for the deaf

#### REFERENCES

- DCMA Instruction 632, "Onboarding Process," December 19, 2013, as amended
- DCMA Instruction 1002, "Situation Report (SITREP)," May 14, 2014
- DCMA Instruction 1028, "Military In-Processing and Out-Processing," May 14, 2013
- DCMA "Internal Web Access Management (IWAM) User Manual," Version 3.2, February 2014
- DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013
- DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
- DoD Instruction 1300.18, "Department of Defense (DoD) Personnel Casualty Matters, Policies, and Procedures," January 8, 2008, as amended
- DoD Instruction 3001.02, "Personnel Accountability in Conjunction With Natural or Manmade Disasters," May 3, 2010
- DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012
- DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information," February 24, 2012, as amended
- DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
- DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012
- Human Capital Business Practice Number 32, "Reporting the Death of a Civilian Employee," June 4, 2015

References 17