

information on quantities that can be supplied and the time necessary to fill an order, as well as any relevant information on past production.

Complete comments, including any attachments and submissions containing confidential business information (CBI), must be received no later than May 24, 2024.

Interested persons are invited to submit comments not containing CBI electronically to the Chairman of the Committee for the Implementation of Textile Agreements at [OTEXA.USMCA@trade.gov](mailto:OTEXA.USMCA@trade.gov). If interested persons are unable to submit comments electronically, please contact Laurie Mease at [Laurie.Mease@trade.gov](mailto:Laurie.Mease@trade.gov) or 202-482-2043 for instructions on other means of submission.

For those seeking to submit comments with CBI for government use only, please clearly mark such submissions as CBI and submit an accompanying version redacting the CBI to be made public. Submissions containing CBI may be submitted electronically through the Department of Commerce's secure online file sharing tool. Access to the secure electronic system will be by invitation only. Interested persons planning to file a submission containing CBI should contact Laurie Mease at [Laurie.Mease@trade.gov](mailto:Laurie.Mease@trade.gov) for instructions before submitting any documents (either public or confidential versions) to CITA.

CITA will protect any information that is marked business confidential from disclosure to the full extent permitted by law. Information marked as business confidential will be shared with OTEXA staff tasked with reviewing responses to this request for comment, and may be shared with CITA members, at the request of the CITA member, as they consider making a recommendation with respect to a modification of the USMCA rules of origin. CBI will not be shared with representatives of the Governments of Canada and Mexico during consultation among the Parties as they consider whether to modify the USMCA rules of origin, as discussed above.

Public versions of all comments received will be posted on OTEXA's website for commercial availability proceedings under the USMCA: <https://www.trade.gov/fta-commercial-availability-usmca>.

**Jennifer Knight,**

*Chairman, Committee for the Implementation of Textile Agreements.*

[FR Doc. 2024-08691 Filed 4-23-24; 8:45 am]

**BILLING CODE 3510-DR-P**

## DEPARTMENT OF DEFENSE

### Office of the Secretary

[Docket ID: DoD-2024-OS-0040]

### Privacy Act of 1974; System of Records

**AGENCY:** Defense Contract Audit Agency, Department of Defense (DoD).

**ACTION:** Notice of a modified system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the DoD is modifying and reissuing a current system of records titled, "DCAA Management Information System (DMIS), RDCAA 590.8." This system of records was originally established by the Defense Contract Audit Agency (DCAA) to collect and maintain records on audit requirements, programs, and performance and to provide timekeepers with access to time and attendance records. This system of records notice (SORN) is being updated to change the SORN title from "DCAA Management Information System (DMIS)" to "DCAA Portfolio Management System Records." The DoD is also modifying various other sections within the SORN to improve clarity or update information that has changed.

**DATES:** This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before May 24, 2024. The Routine Uses are effective at the close of the comment period.

**ADDRESSES:** You may submit comments, identified by docket number and title, by either of the following methods:

\* *Federal Rulemaking Portal:* <https://www.regulations.gov>. Follow the instructions for submitting comments.

\* *Mail:* Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

*Instructions:* All submissions received must include the agency name and docket number for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

#### FOR FURTHER INFORMATION CONTACT:

Keith Mastromichalis, FOIA, Privacy, and Civil Liberties Officer, Defense

Contract Audit Agency, 8725 John J. Kingman Road, Suite 2135, Fort Belvoir, VA 22060-6219, [keith.o.mastromichalis.civ@mail.mil](mailto:keith.o.mastromichalis.civ@mail.mil), (571) 448-3153.

#### SUPPLEMENTARY INFORMATION:

##### I. Background

The DCAA Management Information System is used to collect and maintain records on audit requirements, programs, and performance as well as to plan, perform, and oversee non-audit projects supporting Agency mission and initiatives. This system of records name is changing from "DCAA Management Information System" to "DCAA Portfolio Management System Records." Subject to public comment, the DoD is updating this SORN to add the standard DoD routine uses (A through J). Additionally, the following sections of this SORN are being modified as follows: (1) to the System Manager and System Location sections to update system name and Location to reflect the cloud environment; (2) to the Authority for Maintenance of the System to update citations and add additional authorities; (3) to the Purpose of the System section to clarify the scope of the system; (4) to the Categories of Records in the System to add additional categories and to remove Social Security Number; (5) to the Purpose to provide clarity on the scope of collection; (6) to the Records Source Categories to add additional sources; (7) to the Records Storage Section to update storage medium in which records are maintained; to Retrievability to reduce the identifiers listed for records retrieval; (8) to the Record Access, Notification, and Contesting Record Procedures section, to reflect the need for individuals to identify the appropriate DoD office and/or component to direct their request and to update the appropriate citation for contesting records. and (9) to the Record Source Categories to list the appropriate Federal information systems.

DoD SORNs have been published in the **Federal Register** and are available from the address in **FOR FURTHER INFORMATION CONTACT** or at the Privacy and Civil Liberties Directorate website at <https://dpcl.d.defense.gov>.

##### II. Privacy Act

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, OATSD (PCLT) has provided a report of this system of records to the OMB and to Congress.

Dated: April 19, 2024.

**Aaron T. Siegel,**

*Alternate OSD Federal Register Liaison Officer, Department of Defense.*

**SYSTEM NAME AND NUMBER:**

DCAA Portfolio Management System Records, RDCAA 590.8.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

**SYSTEM MANAGER(S):**

The system manager is Chief Digital and AI Office, Defense Contract Audit Agency, 8725 John J. Kingman Road, Suite 2135, Fort Belvoir, VA 22060-6219.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

DoDD 5105.36, Defense Contract Audit Agency, and DoDI 7640.02, Policy for Follow-Up on Contract Audit Reports.

**PURPOSE(S) OF THE SYSTEM:**

To provide managers, supervisors, and team members with timely, online information regarding audit requirements, programs, and performance as well as to plan, perform, and oversee non-audit projects supporting Agency mission and initiatives.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Defense Contract Audit Agency (DCAA) employees.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Records relating to audit work performed in terms of hours expended by individual employees, dollar amounts audited, exceptions reported, audit activity codes, and net savings to the government as a result of those exceptions; records containing employee data; name, DOD ID Number, position/title, rank/grade, work email address, official duty telephone number, time and attendance, and work

schedule; and records containing office information, *e.g.*, duty station address, office symbol and telephone number.

**RECORD SOURCE CATEGORIES:**

Records and information stored in this system of records are obtained from: Individuals; existing DoD information systems, such as Defense Civilian Personnel Data System (DCPDS), Defense Agencies Initiative (DAI), Learning Management System (LMS), and System for Award Management (SAM); Procurement Integrated Enterprise Environment (PIEE); audit reports and working papers.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:**

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when

the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or other review as authorized by the Inspector General Act.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:**

Records may be stored electronically or on magnetic disc, tape, or digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:**

Records may be retrieved by individuals' name and DoD ID number.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

Records Schedule DAA-0372-2024-0001 is being reviewed by NARA pending approval. NARA appraiser had some recommended changes which we are re-submitting for review and approval. Records will be maintained as

permanent until NARA approves the retention and disposition of these records.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:**

The DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, the DoD established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. The DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in Agency facilities.

**RECORD ACCESS PROCEDURES:**

Individuals seeking access to their records should address written inquiries to the Defense Contract Audit Agency, FOIA Requester Service Center, 8725 John J. Kingman Road, Suite 2135, Fort Belvoir, VA 22060-6219. Signed written requests should contain the name and number of this system of records notice along with full name, current address, and email address of the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the

foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

**CONTESTING RECORD PROCEDURES:**

The DoD rules for accessing records, contesting contents, and appealing initial Component determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

**NOTIFICATION PROCEDURES:**

Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:**

None.

**HISTORY:**

November 9, 2005, 70 FR 67995.

[FR Doc. 2024-08760 Filed 4-23-24; 8:45 am]

**BILLING CODE 6001-FR-P**

**DEPARTMENT OF DEFENSE**

**Office of the Secretary**

[Docket ID: DoD-2024-OS-0041]

**Privacy Act of 1974; System of Records**

**AGENCY:** Defense Finance and Accounting Service (DFAS), Department of Defense (DoD).

**ACTION:** Notice of a modified system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the DoD is modifying and reissuing a current system of records titled, "MyPay System," T7336. This system of records was originally established by the DFAS to collect and maintain records on individual payroll accounts. This system of records notice (SORN) is being updated to expand the 'Categories of Individuals Covered' section to cover non-appropriate personnel, and to add the standard DoD routine uses (routine uses A through J). The DoD is also modifying various other sections within the SORN to improve clarity or update information that has changed.

**DATES:** This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before May 24, 2024. The Routine Uses are effective at the close of the comment period.

**ADDRESSES:** You may submit comments, identified by docket number and title, by either of the following methods:

\* *Federal Rulemaking Portal:* <https://www.regulations.gov>. Follow the instructions for submitting comments.

\* *Mail:* Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

Comments should be sent electronically to the docket listed above.

*Instructions:* All submissions received must include the agency name and docket number for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

**FOR FURTHER INFORMATION CONTACT:** Mr. Gregory L. Outlaw, Defense Finance and Accounting Service, Freedom of Information/Privacy Act Program Manager, Corporate Communications, DFAS-ZCF/N, 8899 E 56th Street, Indianapolis, IN 46249-0150 or by phone at (317) 212-4591.

**SUPPLEMENTARY INFORMATION:**

**I. Background**

The MyPay system of records is used to track and allow authorized individuals the ability to retrieve, review, and update payroll information. It is an innovative, automated system that puts the authorized individual in control of processing certain discretionary pay items without using paper forms. Subject to public comment, the DoD is adding the standard DoD routine uses (routine uses A through J). Additionally, the following sections of this SORN are being modified as follows: (1) to the System Manager and System Location sections to update the addresses and office names; (2) to the Authority for Maintenance of the System section to add additional authorities; (3) to the Purpose of the System section to clarify the scope of the system; (4) to the Categories of Individuals to expand the individuals covered; (5) to the Categories of Records in the System to add additional categories; (6) to the Records Source Categories to add additional sources; (7) to the Records Storage Section to update storage medium in which records are maintained; (8) to the Administrative, Technical, and Physical Safeguards to