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 clarity 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

update the individual safeguards protecting the personal information; (9) to the Record Access, Contesting, and Notification 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. Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

DoD SORNs have been published in the **Federal Register** and are available from the address in **FOR FURTHER INFORMATION CONTACT** or at the Office of the Assistant to the Secretary for Privacy and Civil Liberties Directorate website at *https://dpcld.defense.gov/privacy.*

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:

MyPay System, T7336.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

A. Defense Finance and Accounting Service—Indianapolis, 8899 East 56th St., Indianapolis, IN 46249.

B. Office of Personnel Management, 4685 Log Cabin Drive, Macon, GA 31204–6317.

SYSTEM MANAGER(S):

MyPay System Manager, Defense Finance and Accounting Service—Indianapolis, (DFAS–IN/ZTBD), 8899 East 56th Street, Indianapolis, IN 46249, *dfas.foia@mail.mil.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. Chapter 53, Pay Rates and Systems; 5 U.S.C. Chapter 55, Pay Administration; 5 U.S.C. Chapter 81, Compensation For Work Injuries; 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. Chapter 11, Reserve Components; 10 U.S.C. Chapter 61, Retirement Or Separation For Physical Disability; 10 U.S.C. Chapter 63, Retirement For Age; 10 U.S.C. Chapter 65, Retirement Of Warrant Officers For Length Of Service; 10 U.S.C. Chapter 67, Retired Pay for Non-Regular Service; 10 U.S.C Chapter 69, Retired Grade; 10 U.S.C. Chapter 71, Computation Of Retired Pay; 10 U.S.C. Chapter 73, Annuities Based on Retired or Retainer Pay; 37 U.S.C., sections 101–1015, Pay And Allowances Of The Uniformed Services; and E.O. 9397 (SSN) as amended.

PURPOSE(S) OF THE SYSTEM:

To track and allow authorized individuals the ability to retrieve, review and update payroll information from their specific payroll system(s). Records are also used for extraction or compilation of data and reports for management studies and statistical analyses for use internally or externally as required by DoD or other government agencies.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. Active Duty and Reserve military personnel, Military service academy cadets, Naval Reserve Officer Training Corps students; Reserve/National Guard retiree not yet eligible for retired pay, Armed Forces Health Professions Scholarship Program (AFHPSP) students.

B. DoD Civilian employees, to include Non-Appropriated Funds (NAF) employees.

C. Military retirees, their former spouses (Former Spouse Protection Act (FSPA) Claimants), and annuitants.

D. Other Federal agencies employees, to include Executive Office of the President employees, Department of Health and Human Services, Department of Energy, Department of Veterans Affairs, and United States Agency for Global Media.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal Information, to include name, Social Security Number (SSN), DoD ID number, military branch of service, employment status (as appropriate), pay plan/grade/step, and home address and email.

B. Financial Information, to include pay, wage, benefits, earnings, and allowances; additional pay (bonuses, special and incentive pays); allotments and other withholdings, such as taxes withheld/paid, debts, and retirement contributions; banking information; leave balances and leave history.

C. Transaction Information, to include records of transactions initiated by the individual using the MyPay system, such as mailing address, allotments, tax withholdings, direct deposit, and health savings account.

RECORD SOURCE CATEGORIES:

Records and information stored in this system of records are obtained from: Individual; Defense Joint Military Pay System (DJMS), Defense Civilian Pay System (DCPS), Defense Manpower Data Center (DMDC), Health and Human Services (HHS), Veteran Affairs (VA), Executive Office of the President, Department of Energy and United States Agency for Global Media.

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 some 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 in secure facilities in a locked drawer behind a locked door. The records may be stored 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 name and SSN.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records may be temporary in nature and destroyed when actions are completed, they are superseded, obsolete, or no longer needed. Other records may be cut off at the end of the payroll year, destroyed up to 6 years and 3 months after cutoff.

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 DoD facilities.

RECORD ACCESS PROCEDURES:

Individuals seeking access to their records should address written inquiries to the Defense Finance and Accounting, Freedom of Information/Privacy Act Program Manager, Corporate Communications, DFAS–ZCF/IN, 8899 E 56th Street, Indianapolis, IN 46249–0150. Signed written requests should contain the name and number of this system of records notice along with full name, SSN for verification, 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:

June 16, 2006, 71 FR 34898.

[FR Doc. 2024–08762 Filed 4–23–24; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF EDUCATION

Applications for New Awards; Expanding Opportunity Through Quality Charter Schools Program (CSP)—State Charter School Facilities Incentive Grant (SFIG) Program

AGENCY: Office of Elementary and Secondary Education, Department of Education.

ACTION: Notice.

SUMMARY: The Department of Education (Department) is issuing a notice inviting applications for fiscal year (FY) 2024 for the SFIG Program, Assistance Listing Number (ALN) number 84.282D. This notice relates to the approved information collection under OMB control number 1855–0012.

DATES:

Applications Available: April 24, 2024.

Notice of Intent to Apply: Applicants are strongly encouraged but not required to submit a notice of intent to apply by June 24, 2024. Applicants who do not meet this deadline may still apply.

Deadline for Transmittal of Applications: July 23, 2024.

Deadline for Intergovernmental Review: September 23, 2024.

Pre-Application Webinar Information: The SFIG Program intends to hold a webinar designed to provide technical