BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2020-OS-0001]

Privacy Act of 1974; System of Records

AGENCY: Office of the Under Secretary of Defense (Comptroller) (OUSD(C)), Department of Defense (DoD).

ACTION: Notice of a modified System of Records.

SUMMARY: The OUSD(C) is modifying an existing System of Records titled, "Forms and Account Management Service (FAMS)," DCFO 01. FAMS will be the sole, web-based platform for the appointment and termination of Department Accountable Officials, appointment and termination of Key Signatories of financial documentation, and access management to a portfolio of information systems. During Financial Improvement and Audit Readiness (FIAR) audits of Department of Defense (DoD) Information Technology (IT) processes, numerous notices of findings and recommendations were issued related to vulnerabilities in managing Defense systems account access and appointment of accountable official positions. Findings identified gaps in properly handling and managing accounts for access and authority to act. Improper account management presents information security risks that could result in unauthorized access. Historically, many of these functions were performed in a decentralized manner and conducted manually without effective checks and balances on accuracy. Introduction of the new web-based platform will reduce and eliminate the use of paper forms as it will automate the request and approval processes and enable periodic validation and reconciliation of account records against actual account permissions.

DATES: This notice is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

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

* Federal Rulemaking Portal: https://www.regulations.gov.

Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Chief Management Officer, Directorate for Oversight and Compliance, 4800 Mark Center Drive, 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: Ms. Cynthia B. Stanley, Department of Defense, Office of the Chief Management Officer, Directorate for Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700, or by phone at (703) 571-0070.

SUPPLEMENTARY INFORMATION: Office of Management and Budget (OMB) Circular No. A-123 defines management's responsibility for internal control in Federal agencies. A re-examination of the existing internal control requirements for Federal agencies was initiated in

light of the new internal control requirements for publicly-traded companies contained in the Sarbanes-Oxley Act of 2002. Circular A-123 and the statute it implements, the Federal Managers' Financial Integrity Act of 1982, are at the center of the existing Federal requirements to improve internal control.

This circular reflects policy recommendations developed by a joint committee of representatives from the Chief Financial Officer Council (CFOC) and the President's Council on Integrity and Efficiency. The policy changes in this circular are intended to strengthen the requirements for conducting management's assessment of internal control over financial reporting. OUSD(C) is responsible for developing and maintaining effective internal controls for the DoD to provide assurance significant weaknesses in the design or operation of internal control, such as unauthorized access to Defense business systems, which could adversely affect the Department's ability to meet its objectives, are prevented or detected in a timely manner. FAMS enables the DoD to track and manage the appointment of qualified personnel (Departmental Accountable Officials and Financial Signatories) to key positions and control Defense business system access to appropriately cleared and authenticated employees, thereby meeting the requirements of OMB A-123.

The OSD notices for Systems of Records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the Federal Register and are available from the address provided in the FOR FURTHER INFORMATION CONTACT paragraph or are available via the Defense Privacy, Civil Liberties, and Transparency Division website at https://dpcld.defense.gov.

The proposed systems reports, as required by the Privacy Act, as amended, were submitted on November 26, 2019 to the House Committee on Oversight and Reform, the Senate

Committee on Homeland Security and Governmental Affairs, and the OMB pursuant to Section 6 of OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," revised December 23, 2016 (December 23, 2016, 81 FR 94424).

Dated: January 8, 2020.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Forms and Account Management Service (FAMS), DCFO-01

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: Air Force Life Cycle Management Center, 9 Eglin Street, Building 1606, Hanscom Air Force Base, MA 01731.

SYSTEM MANAGER(S): Program Manager, OUSD(C), 1500 West Perimeter Road, Suite 3130, Joint Base Andrews NAF, MD 20762-6604, telephone contact numbers: (240) 612-5307, (202) 320-2372, and (240) 612-5199.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 31 U.S.C. § 902, Authority and Functions of Agency Chief Financial Officers, as amended; 31 U.S.C. § 3325, Vouchers; 31 U.S.C. § 3528, Responsibilities and Relief from Liability of Certifying Officials; Chief Financial Officers Act of 1990, 31 U.S.C., chapters 5, 9, 11, and 35; also 5 U.S.C. § 5313-5315, 38 U.S.C. § 201 and 42 U.S.C. § 3533; Government Management Reform Act of 1994, Pub. L. No. 103-356; Federal Financial Management Improvement Act of 1996, Pub. L. No. 104-208, Title VIII; 44 U.S.C. § 3541, Federal Information Security Modernization Act of 2014; Executive Order

10450, Security Requirements for Government Employment; DoD Financial Management Regulation 7000.14-R, Vol. 5.

PURPOSE(S) OF THE SYSTEM: FAMS is a secure, cloud-based set of tools and services established to automate key Financial Management Forms, workflow, and reporting processes (audit materials). FAMS optimizes the use of information technology and streamlines the financial management processes by eliminating paper form routing and physical storage requirements and closing the associated access control audit finding performance gaps. The data acquired and updated from each record source is used not only for identity validation, but is also stored and revalidated for subsequent workflow actions.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Within the DoD: Active Duty service members, Reserve service members, National Guard Bureau service members, Presidential Appointees, Civilians, Military Academy Cadets, and Contractors. Also includes Foreign Military Members and Foreign Civilian hire employees.

CATEGORIES OF RECORDS IN THE SYSTEM: Name, Electronic Data Interchange Personal Identifier Number (EDIPI), also referred to as the DoD ID number, current rank/grade, current organization, current duty location, security clearance level, security clearance completion date, Active/Reserve/Guard designation, specialty codes used by the military branches to identify a specific job, hire date, hire location, separation/retirement date, and date of death.

RECORD SOURCE CATEGORIES: Individuals; DoD databases accessed through Defense Manpower Data Center (DMDC) Identity Web Services - Personal Identity Data and DMDC Information System for Security - Personal Security Clearance Data.

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, these records contained therein 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. This routine use complies with 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 has confirmed that the security or confidentiality of the information in the System of Records has been compromised; (2) the DoD has determined that 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored on electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Individual's full name and EDIPI / DoD ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Destroy 10 years after cancellation or revocation of the order, provided there are no outstanding discrepancies for which corrective action has been prescribed.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Role-based access control restricts the system access to authorized users with a need-to-know. Network encryption protects data transmitted over the network while disk encryption secures the disks storing data. Key management services safeguards encryption keys.

RECORD ACCESS PROCEDURES: Individuals seeking to determine whether this System of Records contains information on themselves should address written inquiries to the Director, Chief Financial Officer - Data Transformation Office, OUSD-C/DCFO/CDTO, 1100 Defense Pentagon, Washington D.C. 20301-1100, (703) 571-1396. For verification purposes, individuals should provide their full name, EDIPI / DoD ID number from their Common Access Card (CAC), office or organization where currently assigned, if applicable, and current address and telephone number. 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 following 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 rule for accessing, contesting and appealing agency determinations by the individual concerned are published 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 should address written inquiries to the Director, Chief Financial Officer - Data Transformation Office, OUSD-C/DCFO/CDTO, 1100 Defense Pentagon, Washington D.C. 20301-1100. For verification purposes, individuals should provide full name, EDIPI / DoD ID number from CAC, office or organization where currently assigned, if applicable, and current address and telephone number. 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 following 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)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: October 9, 2019, 84 FR 54125.

[FR Doc. 2020-00365 Filed: 1/13/2020 8:45 am; Publication Date: 1/14/2020]