BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2020-OS-0031]

Privacy Act of 1974; System of Records

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

ACTION: Notice of a new System of Records.

SUMMARY: The Office of the Under Secretary of Defense (Comptroller) proposes to add a System of Records titled, "Defense Repository for Common Enterprise Data (DRCED)," DUSDC 01. This system will automate financial and business transactions, perform cost-management analysis, produce oversight and audit reports, and provide critical data linking to improve performance of mission objectives. Congress mandated the creation of this system through the National Defense Authorization Act of 2018 and then codified it by statute as "Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management." The DRCED's purpose is to improve the Department's defense business enterprise by synchronizing and normalizing data for affordability, performance, and mission readiness. To achieve this, the DRCED will optimize technology to provide an enterprise solution for integrating and analyzing targeted data from existing Department systems to develop timely, actionable, and insightful conclusions in support of national strategies. Also, DRCED is capable of creating predictive analytic models based upon specific data streams to equip decision makers with critical data necessary for execution of fiscal and operational requirements.

DATES: This new System of Records 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: DRCED is a single authoritative repository for DoD Common Enterprise Data (CED) to provide decision-makers greater insight into financial auditability, business processes, and operational combat/mission readiness. CED is defined as

automatically accessible data from business operations or management records provided in a usable format to authorized DoD personnel or DoD components. DRCED will extract records from relevant Department systems, synchronize and normalize CED from those systems to facilitate and streamline enterprise-wide analysis and management of business processes. DRCED capabilities include: robust auditing to recognize fraudulent budget, programming, and fiscal transactions; linking of data from multiple systems (such as personnel, financial, and medical systems) to specific operations and missions for visibility and traceability of expenditures and resource allocation; producing reports for individual transaction processing for each stage of the budgetary life cycle; assessment tools for decision-makers charged with overseeing costs for specific missions or functions (e.g., equipment, training, personnel); and applying predictive analysis to identify common operational factors for readiness and unit deploy ability.

The DoD notices for Systems of Records subject to the Privacy Act of 1974, as amended, have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at https://dpcld.defense.gov.

The proposed systems reports, as required by of the Privacy Act, as amended, were submitted on January 24, 2020, to the House Committee on Oversight and Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to Section 6 to 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: March 12, 2020.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer,

Department of Defense.

SYSTEM NAME AND NUMBER: Defense Repository for Common Enterprise Data (DRCED), DUSDC 01.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Marine Corps Information Technology Center (MCITC), 2306 East Bannister Road, Kansas City, MO 64131-3088. Amazon Web Services (AWS), 12900 Worldgate Drive, Suite 800, Herndon, VA 20170-6040.

SYSTEM MANAGER(S): Director, Business Integration Office, OUSD Comptroller, 1100 Defense Pentagon, Washington, DC 20301-1100; e-mail: osd.pentagon.ousd-c.mbx.audit-helpdesk@mail.mil; Phone: (703) 614-8575.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. § 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; 31 U.S.C. § 902, Authority and Functions of Agency Chief Financial Officers, as amended; 31 U.S.C. § 6101, Digital Accountability and Transparency Act of 2006, as amended in 2014; 31 U.S.C. 3512(b), Executive Agency Accounting and Other Financial Management Reports and Plans; 10 U.S.C. § 117, Readiness Reporting System; DoD Directive 7045.14, The Planning, Programming, Budgeting, and Execution (PPBE) Process; DoD Instruction 8320.02, Data Sharing in a Net-Centric Department of Defense; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: This system establishes a single authoritative repository for DoD CED providing decision-makers an integrated system for data processing and the production of reports for auditability, business operations, cost performance, and combat/mission readiness. As a single system repository of department-wide CED, the DRCED will maintain information retrieved from several systems of record within the Department. As a shared data environment DRCED will make information more easily accessible, standardized, efficiently processed, and useful for customers across the DoD.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: All armed services personnel, including National Guard and Reserve components; former members, and retirees of the armed services; dependent family members of armed services members; DoD "affiliated" individuals (e.g. non-appropriated fund employees, Red Cross volunteers, United Services Organization (USO) staff, Congressional staff members, etc.), presidential appointees, civilian employees, contractors, or individuals (and their surviving beneficiaries) accorded benefits, rights, privileges, or immunities associated with DoD as provided by U.S. law.

CATEGORIES OF RECORDS IN THE SYSTEM: Personal Information: Name; DoD ID number; Social Security Number (SSN); address; e-mail address(es); date of birth; gender; branch of service; citizenship; Defense Enrollment Eligibility Reporting System benefit number; sponsorship and beneficiary information; race and ethnic origin;

Employment Information: employment status; duty position; leave balances and history; work schedules; individual personnel records; time and attendance records; retirement records, sponsor duty location, unit of assignment; occupation; rank; skill specialty; security clearance information.

Personal Financial Information: Pay, wage, earnings information; separation information; financial benefit records; income tax withholding records; accounting records.

Medical Readiness and Deployment Information: Inpatient and outpatient medical records; pharmacy records; immunization records; Medical and Physical Evaluation Board records; neuropsychological functioning and cognitive testing data; periodic and deployment-related health assessments.

RECORD SOURCE CATEGORIES: Individuals; all DoD databases flowing into or accessed through the following integrated data systems, environments, applications, and tools: Defense Finance and Accounting Services financial business feeder systems, Procurement Integrated Enterprise Environment, Defense Manpower Data Center including the Defense Eligibility Enrollment System, Defense Readiness Reporting System (DRRS) enterprise (including DRRS-Strategic and DRRS-Army Database), Defense Medical Logistics - Enterprise Solution, Digital Training Management System; Defense Occupational and Environmental Health Readiness System, Global Force Management Data Initiative, Medical Operations Data System, Force Risk Reduction, Medical Readiness Reporting System, the Medical Data Repository, Army National Guard Human/Personnel, Resource, and Manpower, and commensurate data from National Guard Bureau systems. The following standalone systems and datasets: Drug and Alcohol Management Information System; Physical Disability Case Processing System; Personnel Tempo; TRANSCOM Patient Regulating Command & Control Evaluation System, Substance Abuse Program, DoD Suicide Event Report System, Unit Risk Inventory, Global Assessment Tool, Defense Organizational Climate Survey: Military, Learning Management System, Total Human Resource Managers Information System, Navy Manpower Program and Budget System, and Army Training Requirements and Resources System.

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, the records 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.

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

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records will be typically retrieved by individual's full name, key words and/or DoD ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Permanent. Cut off when canceled or superseded. Transfer to NARA 25 years after cutoff.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Multifactor log-in authentication including CAC authentication and password; SIPR token as required. Access controls enforce need-to-know policies so only authorized users have access to PII. Additionally, security audit and accountability policies and procedures directly support privacy and accountability procedures. Network encryption protects data transmitted over the network while disk encryption secures the disks storing data. Key management services safeguards encryption keys. Sensitive data is identified and masked as practicable. All individuals granted access to this System of Records must complete requisite training to include Information Assurance and Privacy Act training. Sensitive data will be identified, properly marked with access by only those with a need to know, and safeguarded as appropriate. Physical access to servers are controlled at building access points utilizing detection systems other electronic alert systems. Electronic intrusion detection systems are installed within the facilities to monitor, detect, and automatically alert appropriate personnel of security incidents. Access to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should address written inquiries to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Requester Service Center, 1155 Defense Pentagon, Washington, D.C. 20301-1155. Signed written requests should contain the name and number of this System of Records Notice along with the full name, identifier (i.e., DoD ID Number or Defense Benefits Number), date of birth, current address, and telephone number 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 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 rules for accessing records, contesting contents, and appealing initial agency 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 should address written inquiries to the Director, Business Integration Office, OUSD Comptroller, 1100 Defense Pentagon, Washington, DC 20301-1100; e-mail: osd.pentagon.ousd-c.mbx.audit-helpdesk@mail.mil; Phone: (703) 614-8575. Signed written requests should contain the full name, identifier (i.e. DoD ID Number or DoD Benefits Number), date of birth, and current address and telephone number 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 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: None.

[FR Doc. 2020-05504 Filed: 3/16/2020 8:45 am; Publication Date: 3/17/2020]